**Dziennik Uniwersytetu warszawskiego**

RADY DYDAKTYCZNE

**Dziennik Uniwersytetu warszawskiego**

RADY DYDAKTYCZNE DLA KIERUNKÓW STUDIÓW

**UCHWAŁA NR 7/2023**

**RADY DYDAKTYCZNEJ DLA KIERUNKÓW STUDIÓW BEZPIECZEŃSTWO WEWNĘTRZNE, EUROPEISTYKA – INTEGRACJA EUROPEJSKA, ORGANIZOWANIE RYNKU PRACY, POLITOLOGIA, POLITYKA SPOŁECZNA, STOSUNKI MIĘDZYNARODOWE, STUDIA EUROAZJATYCKIE**

z dnia 26 stycznia 2023 r.

**w sprawie wniosku o utworzenie kierunku studiów:
*cyberbezpieczeństwo,* II stopień, studia stacjonarne**

Na podstawie § 143 pkt 1 uchwały nr 443 Senatu Uniwersytetu Warszawskiego
z dnia 26 czerwca 2019 r. w sprawie uchwalenia Statutu Uniwersytetu Warszawskiego (Monitor UW 26.06.2019 poz. 190) Rada Dydaktyczna postanawia, co następuje:

§ 1

 Pozytywnie opiniuje wniosek o utworzenie kierunku studiów: *cyberbezpieczeństwo,* II stopień, studia stacjonarne, stanowiący załącznik do uchwały nr 1.

§ 2

Uchwała wchodzi w życie z dniem podjęcia.

Przewodniczący Rady Dydaktycznej: *M. Raś*

Załącznik nr 1

z dnia 26/01//2023 do uchwały nr 7/2023 Rady Dydaktycznej dla kierunków

Bezpieczeństwo wewnętrzne, Europeistyka – integracja europejska,

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

Studia euroazjatyckie

**WNIOSEK O UTWORZENIE KIERUNKU STUDIÓW**

**CZĘŚĆ I**

**PROGRAM STUDIÓW**

|  |  |
| --- | --- |
| nazwa kierunku studiów | Cyberbezpieczeństwo |
| nazwa kierunku studiów w języku angielskim /w języku wykładowym | Cybersecurity |
| język wykładowy | język polski |
| poziom kształcenia | studia drugiego stopnia |
| poziom PRK | 7 |
| profil studiów | profil ogólnoakademicki |
| liczba semestrów | 4 |
| liczba punktów ECTS konieczna do ukończenia studiów | 120 |
| forma studiów | studia stacjonarne |
| tytuł zawodowy nadawany absolwentom (nazwa kwalifikacji w oryginalnym brzmieniu, poziom PRK) | magister |
| liczba punktów ECTS, jaką student musi uzyskać w ramach zajęć prowadzonych z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia | 120 |
| liczba punktów ECTS w ramach zajęć z dziedziny nauk humanistycznych lub nauk społecznych (nie mniej niż 5 ECTS) | 5 |

**Przyporządkowanie kierunku studiów do dziedzin nauki i dyscyplin naukowych, w których prowadzony jest kierunek studiów**

|  |  |  |  |
| --- | --- | --- | --- |
| **Dziedzina nauki** | **Dyscyplina naukowa** | **Procentowy udział dyscyplin** | **Dyscyplina wiodąca****(ponad połowa efektów uczenia się)** |
| dziedzina nauk społecznych | nauki o bezpieczeństwie | 70% | nauki o bezpieczeństwie |
|  | informatyka  | 20% |  |
|  | nauki o polityce i administracji  | 10% |  |
| **Razem:** | - | 100% | - |

**Efekty uczenia się zdefiniowane dla programu studiów odniesione do charakterystyk drugiego stopnia Polskiej Ramy Kwalifikacji dla kwalifikacji na poziomach 6-7 uzyskiwanych w ramach systemu szkolnictwa wyższego i nauki po uzyskaniu kwalifikacji pełnej na poziomie 4**

|  |  |  |
| --- | --- | --- |
| **Symbol efektów uczenia się dla programu studiów** | **Efekty uczenia się** | **Odniesienie do charakterystyk drugiego stopnia PRK**  |
| **Wiedza: absolwent zna i rozumie** |
| **K\_W01** | istotę, miejsce i znaczenie cyberbezpieczeństwa oraz jego relacje (przedmiotowe i metodologiczne) z innymi obszarami nauk  | P7S\_WG  |
| **K\_W02** | metody i techniki badawcze oraz narzędzia opisu stosowane w obszarze cyberbezpieczeństwa, dysponuje poszerzoną i pogłębioną wiedzą na ten temat | P7S\_WG |
| **K\_W03** | zachowania wpływające na bezpieczeństwo w cyberprzestrzeni, ze szczególnym uwzględnieniem tych zachowań, które mają znaczenie dla bezpieczeństwa społeczeństwa, w którym funkcjonuje i ma wiedzę o działalności człowieka mającej na celu zapewnienie bezpiecznego korzystania z narzędzi i rozwiązań oferowanych przez technologie informatyczne | P7S\_WG  |
| **K\_W04** | rozwiązania organizacyjne, ekonomiczne i techniczne dotyczące kształtowania polityki cyberbezpieczeństwa na poziomie firmy, kraju i UE | P7S\_WK  |
| **K\_W05** | metody diagnozowania, analizy, oceny i ryzyka występowania sytuacji stanowiących zagrożenie w cyberprzestrzeni, na jakie narażone są organizacje, państwa i ich obywatele | P7S\_WK |
| **K\_W06** | polityki i plany bezpieczeństwa informacji, w tym kontroli fizycznych, oprogramowania i sieci oraz monitoring i zabezpieczenia baz danych przed naruszeniem ich poufności, integralności i dostępności, sposoby ochrony danych, systemów zarządzania bazami danych i aplikacji, które uzyskują dostęp do danych i korzystają z nich | P7S\_WK |
| **K\_W07** | techniki i technologie zapewniające cyberbezpieczeństwo systemów i infrastruktur IT, sposoby identyfikowania obecności luk w projektowaniu i wdrażaniu systemów, uniemożliwiające wprowadzenie lub pomyślne zakończenie ataków, ograniczanie szkód ponoszonych przez ataki oraz strategie odzyskiwania po złamaniu systemu | P7S\_WK |
| **K\_W08** | wpływ rozwoju nowych technologii i Internetu na rozwój dezinformacji, sposoby i narzędzia manipulacji informacją w cyberprzestrzeni, zagrożenia i wyzwania związane z rozwojem serwisów internetowych i Web 2.0 | P7S\_WK |
| **K\_W09** | strategie wdrażania kontroli bezpieczeństwa, przeprowadzania oceny ryzyka, obsługi wykrywania i reagowania na incydenty w środowiskach opartych na chmurze i zagrożenia związane z wdrażaniem nowych usług sieciowych, np. IoT | P7S\_WK |
| **K\_W10** | znaczenie sztucznej inteligencji w ograniczaniu ryzyka występowania cyberzagrożeń i ich zapobieganiu | P7S\_WK |
| **K\_W11** | rolę kryminalistyki cyfrowej jako kluczowego elementu ochrony sieciowych systemów teleinformatycznych, procesy odkrywania i interpretowania danych elektronicznych, techniki kryminalistyczne w reagowaniu na incydenty | P7S\_WK |
| **K\_W12** | pojęcia i zasady z zakresu ochrony własności przemysłowej i prawa autorskiego oraz rozumie konieczność zarządzania zasobami własności intelektualnej | P7S\_WK |
| **K\_W13** | podstawy tworzenia i rozwoju przedsiębiorczości indywidualnej z wykorzystaniem wiedzy w zakresie organizacyjnych i technicznych rozwiązań dotyczących kształtowania polityki cyberbezpieczeństwa | P7S\_WK |
| **Umiejętności: absolwent potrafi** |
| **K\_U01** | wykorzystywać zdobytą wiedzę do samodzielnego tworzenia i wprowadzania w życie polityki cyberbezpieczeństwa w organizacjach oraz kształtowania polityki cyberbezpieczeństwa kraju, ze świadomością potrzeby stałego dostosowywania się do zmieniających się procedur i technologii | P7S\_UK |
| **K\_U02** | analizować sytuacje stwarzające ryzyko występowania cyberzagrożeń i wykorzystywać zdobytą wiedzę do zarządzania ryzykiem i wdrażania strategii zapobiegawczych w celu zapewnienia bezpieczeństwa przedsiębiorstw i instytucji państwa | P7S\_UK |
| **K\_U03** | samodzielnie wyjaśniać i wykorzystywać podstawowe techniki i technologie w celu zapewnienia cyberbezpieczeństwa systemów i infrastruktur IT, definiować podstawowe elementy zarówno sprzętowych, jak i programowych systemów komputerowych z punktu widzenia niezawodnego działania i cyberbezpieczeństwa  | P7S\_UK |
| **K\_U04** | tworzyć i stosować etyczne i prawne zasady pracy z danymi m.in. poufnymi danymi biznesowymi, danymi zastrzeżonymi i danymi osobowymi | P7S\_UK |
| **K\_U05** | formułować samodzielnie, wyjaśniać i stosować podstawowe zasady analizy, projektowania, wdrażania i kontroli jakości systemów komputerowych | P7S\_UK |
| **K\_U06** | wykorzystywać narzędzia do przeciwdziałania zagrożeniom i destrukcyjnemu oddziaływaniu na informację i systemy informatyczne | P7S\_UK |
| **K\_U07** | rozpoznawać szanse i zagrożenia związane z inteligentnymi systemami, a także zagrożenia cyberbezpieczeństwa wewnątrz organizacji i w państwie  | P7S\_UK |
| **K\_U08** | przygotowywać wystąpienia publiczne i prowadzić debatę związaną z problematyką cyberbezpieczeństwa i powiązanymi obszarami nauk | P7S\_UK |
| **K\_U09** | posługiwać się językiem obcym, zgodnie z wymaganiami przewidzianymi dla poziomu B2+ESOKJ, wykazywać się znajomością terminologii i słownictwa z zakresu cyberbezpieczeństwa | P6(7)S\_UK |
| **K\_U10** | pracować w zespołach powołanych w celu wykrywania i przeciwdziałania cyberincydentom i podejmować samodzielnie decyzje  | P7S\_UO |
| **K\_U11** | kierować zespołem, być osobą odpowiedzialną za organizację pracy, podział zadań i efekty działań zespołu | P7S\_UO |
| **K\_U12** | samodzielnie pogłębiać wiedzę i kierować rozwojem swoich umiejętności, w szczególności być przygotowanym do dalszego kształcenia się w obszarze cyberbezpieczeństwa na studiach podyplomowych i propagowania potrzeby kształcenia się w tym zakresie | P7S\_UU |

|  |
| --- |
| **Kompetencje społeczne: absolwent jest gotów do** |
| **K\_K01** | propagowania potrzeby ograniczania ryzyka zagrożeń i kształtowania odpowiedzialnych postaw dotyczących korzystania z cyberprzestrzeni, rozpowszechniania znaczenia wiedzy w krytycznym odnoszeniu się do problemów bezpieczeństwa IT w życiu społecznym i gospodarczym | P7S\_KK |
| **K\_K02** | zachowywania profesjonalnej, odpowiedzialnej i etycznej postawy w wykonywaniu obowiązków zawodowych  | P7S\_KR |
| **K\_K03** | wykorzystania zdobytej wiedzy w kształtowaniu odpowiedzialnych postaw w społeczeństwie dotyczących korzystania z cyberprzestrzeni | P7S\_KR |
| **K\_K04** | współpracy na rzecz projektów społecznych z obszaru cyberbezpieczeństwa i wspólnego rozwiązywania problemów mających na celu interes publiczny | P7S\_KO |
| **K\_K05** | przedsiębiorczej postawy w zakresie samodzielnego zdobywania wiedzy, kierowania rozwojem swoich umiejętności i prowadzenia działań w ramach własnej działalności gospodarczej | P7S\_KO |

OBJAŚNIENIA

Symbol efektu uczenia się dla programu studiów tworzą:

* litera K – dla wyróżnienia, że chodzi o efekty uczenia się dla programu studiów,
* znak \_ (podkreślnik),
* jedna z liter W, U lub K – dla oznaczenia kategorii efektów (W – wiedza, U – umiejętności, K – kompetencje społeczne),
* numer efektu w obrębie danej kategorii, zapisany w postaci dwóch cyfr (numery 1-9 należy poprzedzić cyfrą 0).

**Zajęcia lub grupy zajęć przypisane do danego etapu studiów**

**Rok studiów:** pierwszy

**Semestr studiów:** pierwszy

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Nazwa przedmiotu** | **Forma zajęć – liczba godzin** | **Razem: liczba** **godzin zajęć** | **Razem:****punkty ECTS** | **Symbole efektów uczenia się dla programu studiów** | **Dyscyplina / dyscypliny, do których odnosi się przedmiot** |
| **Wykład** | **Konwersatorium** | **Seminarium** | **Ćwiczenia** | **Laboratorium** | **Warsztaty** | **Projekt** | **Inne** |
| Podstawy cyberbezpieczeństwa (O) | 15 |  |  | 15 |  |  |  |  | 30 | 3 | K\_W01K\_W02K\_W03K\_W06K\_W12K\_U01K\_U03K\_K01 | nauki o bezpieczeństwie |
| **Treści programowe**  | Przedmiot obejmuje zagadnienia:Wykład:* wprowadzenie do cyberbezpieczeństwa, obejmujące m.in. kluczowe podstawowe pojęcia, definicje, normy, wytyczne, dobre praktyki,
* regulacje i akty prawne dotyczące cyberbezpieczeństwa,
* organizacje i instytucje zajmujące się bezpieczeństwem teleinformatycznym,
* rodzaje informacji, jawne, niejawne, klauzule tajności, odpowiedzialność karna,
* główne zasady ochrony informacji.

Ćwiczenia:* cyberbezpieczeństwo – podstawowe pojęcia z zakresu bezpieczeństwa informacji, kontroli dostępu,
* gospodarka cyfrowa i jej wyzwania bezpieczeństwa,
* wyzwania związane z praktycznym zapewnieniem cyberbezpieczeństwa w przedsiębiorstwie,
* zarządzanie ryzykiem w cyberbezpieczeństwie,
* przetwarzanie w chmurze – wyzwania bezpieczeństwa,
* Internet rzeczy – wyzwania bezpieczeństwa,
* zasady cyberbezpieczeństwa w organizacji,
* etyka w cyberbezpieczeństwie.
 |
| **Sposoby weryfikacji efektów uczenia się** | test, zadania, case-study, prezentacje |
| Państwo i społeczeństwo ryzyka (O) | 15 |  |  |  |  |  |  |  | 15 | 2 | K\_W01K\_W02K\_W03K\_W04K\_U01K\_K01K\_K03 | nauki o polityce i administracji |
| **Treści programowe**  | Przedmiot obejmuje zagadnienia:* fenomen państwa jako organizacji porządku i bezpieczeństwa,
* społeczeństwo ryzyka w erze globalizacji,
* sekurytyzacja dziedzin życia społecznego,
* prawa i wolności w kontekście współczesnych zagrożeń,
* wojny współczesne i ich konsekwencje,
* rola państwa w zagwarantowaniu cyberbezpieczeństwa.
 |
| **Sposoby weryfikacji efektów uczenia się** | egzamin pisemny |
| Analiza, ocena i zarządzanie ryzykiem występowania cyberzagrożeń (O) | 15 | 15 |  |  |  |  |  |  | 30 | 3 | K\_W03K\_W05K\_U02K\_K01K\_K02K\_K03 | nauki o bezpieczeństwie |
| **Treści programowe**  | Przedmiot obejmuje zagadnienia:Wykład:* zagrożenia występujące w cyberprzestrzeni,
* przegląd i analiza potencjalnych wektorów ataku,
* metody przeciwdziałania cyberzagrożeniom,
* ochrona zasobów cyfrowych w szczególności plików, baz danych, systemów teleinformatycznych,
* usługi w chmurze i on premise z perspektywy cyberzagrożeń,
* zasady tworzenia systemów teleinformatycznych spełniających najwyższe standardy bezpieczeństwa (skala mikro i makro),
* zapewnienie ciągłość działania systemów teleinformatycznych,
* rodzaje zagrożeń i podatności IoT – klasyfikacje,
* e-usługi i usługi publiczne,
* audyt bezpieczeństwa teleinformatycznego,
* ochrona informacji i urządzeń np. ochrona elektromagnetyczna, sygnalizacja zagrożeń, systemy kontroli dostępu, zabezpieczenia mechaniczne, macierz szacowania ryzyka, procedury bezpiecznej eksploatacji.

Ćwiczenia:* zarządzanie ryzykiem w przedsiębiorstwie a cyberbezpieczeństwo,
* metody wykorzystywane w ocenie cyberbezpieczeństwa,
* analizy przypadków – lessons learned.
 |
| **Sposoby weryfikacji efektów uczenia się** | test, zadania, case-study, prezentacje |
| Bezpieczeństwo zasobów cyfrowych (O) |  | 15 |  |  |  |  |  |  | 15 | 2 | K\_W01K\_W02K\_W06K\_W12K\_U01K\_U03K\_K01 | nauki o bezpieczeństwie |
| **Treści programowe**  | Przedmiot obejmuje zagadnienia:* problematyka bezpieczeństwa zasobów cyfrowych,
* treści szkodliwe, niepożądane, nielegalne publikowane w Internecie np. przemoc, pornografia, sekty, popularyzacja faszyzmu, werbunek do org. Terrorystycznych,
* cyberprzemoc, nękanie, straszenie, szantażowanie z użyciem sieci,
* publikowanie lub rozsyłanie ośmieszających, kompromitujących informacji, zdjęć, filmów z użyciem sieci oraz podszywanie się w sieci pod kogoś wbrew jego woli,
* naruszenia prywatności dotyczące nieodpowiedniego lub niezgodnego z prawem wykorzystania danych osobowych lub wizerunku,
* łamanie prawa autorskiego, ryzyko poniesienia odpowiedzialności cywilnej lub karnej z tytułu naruszenia prawa autorskiego albo negatywnych skutków pochopnego spełnienia nieuzasadnionych roszczeń (tzw. copyright trolling).
 |
| **Sposoby weryfikacji efektów uczenia się** | egzamin ustny |
| Ekonomia informacji (O) | 30 |  |  |  |  |  |  |  | 30 | 3 | K\_W01K\_W02K\_W06K\_U01K\_U03K\_U11K\_K02K\_K03K\_K05 | informatyka |
| **Treści programowe**  | Przedmiot obejmuje zagadnienia:* informacja jako kategoria ekonomiczna,
* przedmiot zainteresowania ekonomii informacji,
* system informacyjny jako system ekonomiczny,
* rynek informacji i jego regulacje,
* asymetria informacji, zarządzanie informacją,
* zastosowanie metod i mierników opracowanych przez ekonomikę informacji do oceny sytuacji ekonomicznej podmiotów gospodarczych,
* elementy ekonomiki informacji w zarządzaniu informacją,
* informacja i jej wpływ na procesy gospodarcze i społeczne,
* koszt i wartość informacji.
 |
| **Sposoby weryfikacji efektów uczenia się** | projekt |
| Podstawy programowania w języku Python (O) |  | 30 |  |  |  |  |  |  | 30 | 3 | K\_W05K\_W10K\_U02K\_U06K\_K03  | informatyka |
| **Treści programowe**  | Przedmiot obejmuje zagadnienia:* wartości, zmienne i ich typy w języku Python,
* operatory w języku Python (logiczne, arytmetyczne, porównania itp),
* podstawowe struktury danych: lista, krotka, słownik, zbiór,
* importowanie i wykorzystanie modułów,
* funkcje i funkcje anonimowe,
* klasy i obiekty,
* wyrażenia regularne,
* czas i data w języku Python,
* obsługa baz danych w Pythonie,
* scraping i rafinacja danych w Pythonie.
 |
| **Sposoby weryfikacji efektów uczenia się** | projekt |
| Polityka cyberbezpieczeństwa w organizacji (O) |  | 30 |  |  |  |  |  |  | 30 | 3 | K\_W01K\_W02K\_W04K\_W06K\_W12K\_U01K\_U03K\_U04K\_U07K\_U11K\_K04 | nauki o polityce i administracji |
| **Treści programowe**  | Celem przedmiotu jest:- poznanie struktur bezpieczeństwa w biznesie,- poznanie procedur i możliwości firm w zakresie realizacji zadań z cyberbezpieczeństwa,- zapoznanie z aspektami prawnymi funkcjonowania firm w zakresie KSC i cyberbezpieczeństwa,- przedstawienie procedur w zakresie reagowania na incydenty. |
| **Sposoby weryfikacji efektów uczenia się** | projekt |
| Bezpieczeństwo wewnętrzne i cyberbezpieczeństwo RP (O) | 15 |  |  |  |  |  |  |  | 15 | 2 | K\_W01K\_W02K\_W04K\_W06K\_U01K\_U04K\_U07K\_K04 | nauki o bezpieczeństwie |
| **Treści programowe**  | Przedmiot obejmuje zagadnienia:* organizacja krajowego systemu cyberbezpieczeństwa oraz zadania i obowiązki podmiotów wchodzących w skład tego systemu,
* zakres strategii cyberbezpieczeństwa Rzeczypospolitej Polskiej,
* kluczowe obszary ryzyka dla systemów wykorzystywanych przez podmioty odpowiedzialne za bezpieczeństwo wewnętrzne w Polsce,
* podstawowe zasady oceny wiarygodności informacji przez funkcjonariuszy publicznych,
* cyberbezpieczeństwo Rzeczypospolitej Polskiej w ramach struktur sojuszniczych NATO,
* analiza przypadków zagrożeń w obszarze cyberbezpieczeństwa dla Rzeczypospolitej Polskiej w ujęciu globalnym.
 |
| **Sposoby weryfikacji efektów uczenia się** | egzamin pisemny |
| Metody analizy danych (O) |  | 15 |  |  |  |  |  |  | 15 | 2 | K\_W05K\_U02K\_K01 | nauki o zarządzaniu i jakości |
| **Treści programowe**  | Przedmiot obejmuje zagadnienia:* podstawowe funkcje statystyczne w R,
* graficzna analiza danych,
* regresja liniowa,
* korelacja i inne parametry statystyczne zbiorów danych,
* testowanie hipotez,
* przykłady analizy danych.
 |
| **Sposoby weryfikacji efektów uczenia się** | projekt |
| OSINT 2.0 – praktyczne wprowadzenie do technik białego wywiadu w Internecie (O) |  | 15 |  |  |  |  |  |  | 15 | 2 | K\_W03K\_W05K\_U02K\_K02K\_K03 | nauki o bezpieczeństwie |
| **Treści programowe**  | Celem przedmiotu jest przekazanie usystematyzowanej wiedzy na temat metod, technik, taktyk i sposobów pozyskiwania informacji w Internecie ze źródeł otwartych i legalnych.Szczegółowe cele przedmiotu: * przyswojenie niezbędnej wiedzy o źródłach danych jawnych i ukrytych w Internecie, ich wiarygodności i zasobności,
* praktyczne opanowanie wybranego oprogramowania (głównie niekomercyjnego, typu Open Source) służącego do pozyskiwania informacji w Internecie,
* przekazanie użytkownikom autorskiego oprogramowania do wyszukiwania informacji w Internecie.
 |
| **Sposoby weryfikacji efektów uczenia się** | projekt |
| Przedmiot swobodnego wyboru z obszaru nauk humanistycznych (z oferowanych zajęć ogólnouniwersyteckich) (SW) |  |  |  |  |  |  |  |  | minimum 30 | 5 |  |  |
| **Treści programowe**  | zgodnie z sylabusem |
| **Sposoby weryfikacji efektów uczenia się** | zgodnie z sylabusem |

**Łączna liczba punktów ECTS** (w roku/semestrze): **30**

**Łączna liczba godzin zajęć** (w roku/semestrze): **255**

**Łączna liczba godzin zajęć określona w programie studiów dla danego kierunku, poziomu i profilu** (dla całego cyklu): **960**

**Rok studiów:** pierwszy

**Semestr studiów:** drugi

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Nazwa przedmiotu** | **Forma zajęć – liczba godzin** | **Razem: liczba** **godzin zajęć** | **Razem:****punkty ECTS** | **Symbole efektów uczenia się dla programu studiów** | **Dyscyplina / dyscypliny, do których odnosi się przedmiot** |
| **Wykład** | **Konwersatorium** | **Seminarium** | **Ćwiczenia** | **Laboratorium** | **Warsztaty** | **Projekt** | **Inne** |
| Infrastruktura krytyczna i bezpieczeństwo przemysłowe (O) | 15 | 15 |  |  |  |  |  |  | 30 | 3 | K\_W04K\_W06K\_W12K\_U03K\_K01K\_K02K\_K03 | nauki o bezpieczeństwie |
| **Treści programowe**  | Celem przedmiotu jest:* poznanie struktur (jednostek administracyjnych, służb państwowych, inspekcji, instytutów badawczych) zajmujących się̨ monitorowaniem zagrożeń́ wymienionych w Krajowym Planie Zarzadzania Kryzysowego,
* przyswojenie wybranych metod, modeli, technik i narzędzi identyfikacji, analizy i oceny rzeczonych zagrożeń́.
 |
| **Sposoby weryfikacji efektów uczenia się** | projekt |
| Polityka cyberbezpieczeństwa UE (O) | 15 |  |  |  |  |  |  |  | 15 | 2 | K\_W01K\_W02K\_W04K\_U01K\_U04K\_K01K\_K04 | nauki o polityce i administracji |
| **Treści programowe**  | Problematyka przedmiotu skupia się wokół standardów cyberbezpieczeństwa w UE, sposobów ich przyjmowania i stosowania w praktyce. Przedmiot obejmuje zagadnienia:* podstawowe koncepcje i środowisko cyberbezpieczeństwa UE,
* prawne i polityczne aspekty cyberbezpieczeństwa w UE: unijne dyrektywy, wytyczne, rozporządzenia, inicjatywy,
* zarządzanie cyberbezpieczeństwem w UE: zaangażowane organy, procesy i zasady zarządzania ryzykiem związanym z cyberbezpieczeństwem,
* wyzwania nietechniczne – ludzie.
 |
| **Sposoby weryfikacji efektów uczenia się** | egzamin pisemny |
| Technologie budowy i zabezpieczeń serwisów internetowych (O) |  |  |  | 30 |  |  |  |  | 30 | 3 | K\_W07K\_W08K\_U03K\_K01 | informatyka |
| **Treści programowe**  | Przedmiot obejmuje zagadnienia:* rozróżnienie pojęć front-end i back-end,
* technologie tworzenia front-endu i back-endu,
* podatność serwisów internetowych na zagrożenia,
* wektory ataku na serwisy internetowe,
* typowe zagrożenia serwisów i metody ochrony przed nimi.
 |
| **Sposoby weryfikacji efektów uczenia się** | projekt |
| Analiza danych w języku Python (O) |  |  |  | 30 |  |  |  |  | 30 | 3 | K\_W05K\_W10K\_U02K\_U06K\_K03 | informatyka |
| **Treści programowe**  | Przedmiot obejmuje zagadnienia:* wirtualne środowisko Pythona,
* biblioteki służące do analizy danych,
* zależności pomiędzy bibliotekami,
* wymagania bibliotek,
* akwizycja i rafinacja danych,
* przykłady analizy danych.
 |
| **Sposoby weryfikacji efektów uczenia się** | projekt |
| Systemy baz danych (O) |  | 30 |  |  |  |  |  |  | 30 | 3 | K\_W06K\_U03K\_K01 | informatyka |
| **Treści programowe**  | Zajęcia praktyczne ukierunkowane na poznanie funkcjonalności baz danych: relacyjnych oraz NoSQL. Przedmiot obejmuje zagadnienia:* wprowadzenie w problematykę baz danych - właściwości i funkcje baz danych, modele danych,
* relacyjne bazy danych - elementy i właściwości modelu relacyjnego,
* podstawy projektowania relacyjnych baz danych - tworzenie tabel, relacji, modyfikacja schematu,
* podstawy języka SQL – składnia języka SQL, definicja danych, typy danych,
* wyszukiwanie danych – SELECT,
* funkcje i operacje na typach danych,
* grupowanie danych i funkcje agregujące,
* podzapytania i instrukcje zagnieżdżone,
* konstrukcja zapytań złożonych – łączenie instrukcji,
* nieustrukturyzowane przetwarzanie i analiza danych - praca z bazami danych NoSQL.
 |
| **Sposoby weryfikacji efektów uczenia się** | test |
| Kryminalistyka cyfrowa (O) | 15 | 30 |  |  |  |  |  |  | 45 | 4 | K\_W05K\_W11K\_U02K\_K03 | nauki o bezpieczeństwie |
| **Treści programowe**  | Przedmiot obejmuje zagadnienia:* zbieranie dowodów, ich udokumentowanie i zabezpieczenie,
* rola sprzętu komputerowego, urządzeń mobilnych, systemów operacyjnych, systemów plików, oprogramowania narzędziowego w zbieraniu dowodów,
* internet jako źródło danych i dowodów,
* analiza incydentów,
* analiza śledcza w zakresie sprzętu, oprogramowania, danych cyfrowych etc.,
* analiza wybranych studiów przypadków.
 |
| **Sposoby weryfikacji efektów uczenia się** | egzamin pisemny |
| Normy bezpieczeństwa i ciągłości działania (O) |  | 30 |  |  |  |  |  |  | 30 | 3 | K\_W05K\_W06K\_U02K\_U03K\_K03 | nauki o bezpieczeństwie |
| **Treści programowe**  | Przedmiot obejmuje zagadnienia:* normy ISO - zapoznanie się z normami przydatnymi do audytu,
* norma ISO 22301 i 27001 - podejście do zarządzania jakością i bezpieczeństwem informacji oraz ciągłości działania,
* proces certyfikacji i ciągłości działania,
* metody i techniki prowadzenia audytu i raportowanie niezgodności,
* sporządzanie raportów z audytu,
* etyka pracy audytora.
 |
| **Sposoby weryfikacji efektów uczenia się** | test |
| Badania nad cyberbezpieczeństwem I (projekt) (OW) |  |  |  |  |  |  | 30 |  | 30 | 3 | K\_W01K\_W02K\_W03K\_W05K\_U01K\_U02K\_K01K\_K03 | nauki o bezpieczeństwienauki o polityce i administracjiinformatyka |
| **Treści programowe**  | Przedmiot obejmuje zagadnienia:* przygotowanie projektu pod kierunkiem prowadzącego zajęcia,
* identyfikacja i analiza problemu badawczego z zakresu cyberbezpieczeństwa,
* projekt przejściowy obejmuje podstawowe elementy w tym: wybór zagadnienia badawczego, przygotowanie założeń, pytań badawczych, celu i hipotezy badawczej,
* metody i techniki badawcze niezbędne do realizacji projektu,
* w ramach projektu, studenci mogą opracować własne narzędzia lub skorzystać z dostępnych narzędzi.

Przedmiot prowadzony będzie przez kilku specjalistów z różnych obszarów związanych z cyberbezpieczeństwem (do wyboru w zależności od tematyki projektu). |
| **Sposoby weryfikacji efektów uczenia się** | projekt |
| Proseminarium (OW) |  |  | 30 |  |  |  |  |  | 30 | 6 | K\_W01K\_W02K\_W03K\_W05K\_U01K\_U02K\_K01K\_K02K\_K03 | nauki o bezpieczeństwienauki o polityce i administracjiinformatyka |
| **Treści programowe**  | Przedmiot obejmuje:* wybór tematyki, opracowanie złożeń i identyfikacja problemu badawczego,
* przygotowanie konspektu pracy magisterskiej pod kierunkiem promotora,
* dobór metod i technik badawczych do realizacji założeń pracy.
 |
| **Sposoby weryfikacji efektów uczenia się** | praca pisemna |

**Łączna liczba punktów ECTS** (w roku/semestrze): **30**

**Łączna liczba godzin zajęć** (w roku/semestrze): **270**

**Łączna liczba godzin zajęć określona w programie studiów dla danego kierunku, poziomu i profilu** (dla całego cyklu): **960**

**Rok studiów:** drugi

**Semestr studiów:** trzeci

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Nazwa przedmiotu** | **Forma zajęć – liczba godzin** | **Razem: liczba** **godzin zajęć** | **Razem:****punkty ECTS** | **Symbole efektów uczenia się dla programu studiów** | **Dyscyplina / dyscypliny, do których odnosi się przedmiot** |
| **Wykład** | **Konwersatorium** | **Seminarium** | **Ćwiczenia** | **Laboratorium** | **Warsztaty** | **Projekt** | **Inne** |
| Bezpieczeństwo systemów bazodanowych i pracy w chmurze (O) |  | 30 |  |  |  |  |  |  | 30 | 3 | K\_W03K\_W06K\_W09K\_U03K\_K01 | nauki o bezpieczeństwieinformatyka |
| **Treści programowe**  | Przedmiot obejmuje zagadnienia:* specyfika rozwiązań chmurowych,
* przegląd systemów bazodanowych,
* typowe zagrożenia dla systemów bazodanowych,
* metody zabezpieczenia baz danych.
 |
| **Sposoby weryfikacji efektów uczenia się** | projekt |
| Przetwarzanie języka naturalnego i sztuczna inteligencja (O) |  |  |  | 30 |  |  |  |  | 30 | 3 | K\_W05K\_W10K\_U03K\_K01 | informatyka |
| **Treści programowe**  | Przedmiot obejmuje zagadnienia:* podstawy przetwarzania języka naturalnego,
* podstawowe problemy techniczne związane z kodowaniem tekstu,
* wstępne przygotowanie danych tekstowych do dalszej analizy,
* modele językowe,
* ekstrakcja słów kluczowych z tekstów,
* detekcja tematów.
 |
| **Sposoby weryfikacji efektów uczenia się** | projekt |
| Wprowadzenie do bezpieczeństwa IoT (O) | 15 |  |  |  |  |  |  |  | 15 | 2 | K\_W03K\_W07K\_W09K\_U03K\_K01 | nauki o bezpieczeństwieinformatyka |
| **Treści programowe**  | Przedmiot obejmuje zagadnienia:* klasyfikacja urządzeń IoT i obszary zastosowań,
* aspekty bezpieczeństwa internetu rzeczy i nowych technologii,
* obszary zastosowania IoT, od urządzeń personalnych do przemysłowych,
* problematyka podatności IoT na zagrożenia cyberbezpieczeństwa (np. wektor ataku na inne aktywne urządzenia sieci za pośrednictwem IoT),
* aspekty prywatności w urządzeniach IoT,
* przyszłe wyzwania w zakresie bezpieczeństwa związane z urządzeniami IoT,
* zabezpieczanie urządzeń IoT, problematyka ciągłości działania etc.,
* zagrożenia informatyczne, macierz szacowania ryzyka.
 |
| **Sposoby weryfikacji efektów uczenia się** | egzamin pisemny |
| Bezpieczeństwo systemów (O) |  |  |  | 15 |  |  |  |  | 15 | 2 | K\_W06K\_W07K\_W12K\_U03K\_K01 | nauki o bezpieczeństwieinformatyka |
| **Treści programowe**  | Przedmiot obejmuje zagadnienia:* system i bezpieczeństwo – definicje, pojęcia systemu oraz bezpieczeństwa wg różnych kryteriów,
* bezpieczeństwo systemu a jego stabilność,
* inżynieria bezpieczeństwa,
* analiza Big Data zdarzeń w systemie jako narzędzie do jego optymalizacji,
* studium przypadku w obszarze systemów MIS.
 |
| **Sposoby weryfikacji efektów uczenia się** | projekt |
| Web 2.0 i media społecznościowe (O) | 15 |  |  |  |  |  |  |  | 15 | 2 | K\_W03K\_W08K\_U01K\_K01 | nauki o komunikacji społecznej i mediach |
| **Treści programowe**  | Przedmiot obejmuje zagadnienia:* ograniczenie ryzyka cyberataków,
* cyfrowy ślad,
* phishing,
* bezpieczeństwo haseł,
* stosowanie podwójnej weryfikacji,
* bezpieczne korzystanie z mediów społecznościowych (Facebook, Twitter, Instagram, YouTube, LinkedIn, Snapchat),
* bezpieczne korzystanie z komunikatorów,
* zabezpieczenia konta w serwisie społecznościowym.
 |
| **Sposoby weryfikacji efektów uczenia się** | test |
| Ochrona danych i prywatności w Internecie (O) | 15 |  |  |  |  |  |  |  | 15 | 2 | K\_W03K\_W06K\_W12K\_U03K\_K02 | nauki o bezpieczeństwie |
| **Treści programowe**  | Przedmiot obejmuje zagadnienia:* metody bezpiecznego transferu danych,
* ochrona prywatności,
* ochrona danych osobowych,
* dane wrażliwe i ich bezpieczeństwo.
 |
| **Sposoby weryfikacji efektów uczenia się** | projekt |
| Badania nad cyberbezpieczeństwem II (projekt) (OW) |  |  |  |  |  |  | 30 |  | 30 | 3 | K\_W01K\_W02K\_W03K\_W05K\_U01K\_U02K\_K01K\_K03 | nauki o bezpieczeństwienauki o polityce i administracjiinformatyka |
| **Treści programowe**  | Przedmiot obejmuje zagadnienia:* przygotowanie projektu pod kierunkiem prowadzącego zajęcia,
* identyfikacja i analiza problemu badawczego z zakresu cyberbezpieczeństwa,
* projekt przejściowy obejmuje podstawowe elementy w tym: wybór zagadnienia badawczego, przygotowanie założeń, pytań badawczych, celu i hipotezy badawczej,
* metody i techniki badawcze niezbędne do realizacji projektu,
* w ramach projektu, studenci mogą opracować własne narzędzia lub skorzystać z dostępnych narzędzi.

Przedmiot prowadzony będzie przez kilku specjalistów z różnych obszarów związanych z cyberbezpieczeństwem (do wyboru w zależności od tematyki projektu). |
| **Sposoby weryfikacji efektów uczenia się** | projekt |
| Nowoczesne trendy zarządzania przedsiębiorstwem -konwersatorium językowe poziom B2+ (O) |  | 30 |  |  |  |  |  |  | 30 | 3 | K\_W01K\_W02K\_W03K\_W04K\_U08K\_U09K\_K01K\_K03K\_W13 | nauki o zarządzaniu i jakości |
| **Treści programowe**  | Przedmiot obejmuje zagadnienia:* nowoczesne trendy zarządzania przedsiębiorstwem,
* gospodarka cyfrowa, Internet of Things i organizacja przyszłości,
* sztuczna inteligencja wyzwania dla HR,
* grywalizacja i innowacyjne metody motywacji pracowników,
* studium przypadku od klasycznego zarządzania firmą do kryzysu wizerunku i cyberataków.
 |
| **Sposoby weryfikacji efektów uczenia się** | case-study, prezentacje |
| Wykład ogólnouniwersytecki OGUN (SW) | 30 |  |  |  |  |  |  |  | 30 | 4 |  |  |
| **Treści programowe**  | zgodnie z sylabusem |
| **Sposoby weryfikacji efektów uczenia się** | zgodnie z sylabusem |
| Seminarium magisterskie (OW) |  |  | 30 |  |  |  |  |  | 30 | 6 | K\_W01K\_W02K\_W03K\_W05K\_U01K\_U02K\_K01K\_K02K\_K03 | nauki o bezpieczeństwienauki o polityce i administracjiinformatyka |
| **Treści programowe**  | Przedmiot obejmuje:* wybór tematyki, opracowanie złożeń i identyfikacja problemu badawczego,
* przygotowanie konspektu pracy magisterskiej pod kierunkiem promotora,
* dobór metod i technik badawczych do realizacji założeń pracy,
* weryfikację założeń przy wykorzystaniu wybranych metod i technik.
 |
| **Sposoby weryfikacji efektów uczenia się** | praca pisemna |

**Łączna liczba punktów ECTS** (w roku/semestrze): **30**

**Łączna liczba godzin zajęć** (w roku/semestrze): **240**

**Łączna liczba godzin zajęć określona w programie studiów dla danego kierunku, poziomu i profilu** (dla całego cyklu): **960**

**Rok studiów:** drugi

**Semestr studiów:** czwarty

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Nazwa przedmiotu** | **Forma zajęć – liczba godzin** | **Razem: liczba** **godzin zajęć** | **Razem:****punkty ECTS** | **Symbole efektów uczenia się dla programu studiów** | **Dyscyplina / dyscypliny, do których odnosi się przedmiot** |
| **Wykład** | **Konwersatorium** | **Seminarium** | **Ćwiczenia** | **Laboratorium** | **Warsztaty** | **Projekt** | **Inne** |
| Symulacje cyberataków (O) |  |  |  |  |  | 30 |  |  | 30 | 3 | K\_W05K\_W07K\_U02K\_K01 | nauki o bezpieczeństwieinformatyka |
| **Treści programowe**  | Przedmiot obejmuje zagadnienia:* kategorie cyberataków,
* Ethical Hacking,
* Killchain model,
* budowa środowiska wirtualnego,
* Kali Linux - podstawy (instalacja, konfiguracja, narzędzia),
* przeprowadzenie ataków w kontrolowanym środowisku,
* testy bezpieczeństwa.
 |
| **Sposoby weryfikacji efektów uczenia się** | test |
| Analiza Big Data w cyberbezpieczeństwie (O) | 15 |  |  | 15 |  |  |  |  | 30 | 3 | K\_W05K\_W10K\_U02K\_K01 | nauki o bezpieczeństwieinformatyka |
| **Treści programowe**  | Przedmiot obejmuje zagadnienia:* rafinacja informacji cyfrowej w zakresie cyberbezpieczeństwa,
* analiza logów,
* źródła informacji cyfrowej wytworzonej przez urządzenia i ludzi,
* algorytmy analizy dużych zbiorów danych cyfrowych,
* narzędzia analizy dużych zbiorów danych,
* metody kolekcjonowania danych cyfrowych,
* bazy podatności sprzętu i oprogramowania.
 |
| **Sposoby weryfikacji efektów uczenia się** | egzamin pisemny |
| Psychomanipulacja w cyberprzestrzeni (O) |  | 15 |  |  |  |  |  |  | 15 | 2 | K\_W03K\_W05K\_U02K\_K01K\_K02K\_K03 | nauki o bezpieczeństwie |
| **Treści programowe**  | Przedmiot obejmuje zagadnienia:* zakres i rozwój cyberzagrożeń,
* poziom świadomości funkcjonowania w cyberprzestrzeni,
* rozwiązania prawne i społeczne w edukacji,
* jakość życia, komunikacji czy prowadzenia polityki informacyjnej.
 |
| **Sposoby weryfikacji efektów uczenia się** | egzamin ustny |
| Ochrona danych osobowych i informacji niejawnych (O) |  | 30 |  |  |  |  |  |  | 30 | 3 | K\_W03K\_W05K\_W12K\_U02K\_K01K\_K02K\_K03 | nauki o bezpieczeństwie |
| **Treści programowe**  | W trakcie zajęć omawiane są zagadnienia z zakresu wymagań formalno-prawnych i standardów ochrony danych osobowych oraz informacji niejawnych.Studenci mają wiedzę z zakresu funkcjonowania instytucji bezpieczeństwa państwa. Omawiane są:* zagadnienia z zakresu wymagań i standardów ochrony danych osobowych oraz informacji niejawnych,
* zakres podmiotowy i przedmiotowy ustaw, obowiązki podmiotów przetwarzających dane osobowe lub informacje stanowiące tajemnicę służbową i państwową,
* zagadnienia związane z zarządzaniem ochroną danych chronionych w podmiotach publicznych i prywatnych.
 |
| **Sposoby weryfikacji efektów uczenia się** | egzamin ustny |
| Nowoczesne trendy zarządzania przedsiębiorstwem -konwersatorium językowe poziom B2+ (O) |  | 30 |  |  |  |  |  |  | 30 | 3 | K\_W01K\_W02K\_W03K\_W04K\_U08K\_U09K\_K01K\_K03K\_W13 | nauki o zarządzaniu i jakości |
| **Treści programowe**  | Przedmiot obejmuje zagadnienia:* nowoczesne trendy zarządzania przedsiębiorstwem,
* gospodarka cyfrowa, Internet of Things i organizacja przyszłości,
* sztuczna inteligencja wyzwania dla HR,
* grywalizacja i innowacyjne metody motywacji pracowników,
* studium przypadku od klasycznego zarządzania firmą do kryzysu wizerunku i cyberataków.
 |
| **Sposoby weryfikacji efektów uczenia się** | case-study, prezentacje |
| Wykład ogólnouniwersytecki OGUN (SW) | 30 |  |  |  |  |  |  |  | 30 | 4 |  |  |
| **Treści programowe**  | zgodnie z sylabusem |
| **Sposoby weryfikacji efektów uczenia się** | zgodnie z sylabusem |
| Seminarium magisterskie (OW) |  |  | 30 |  |  |  |  |  | 30 | 12 | K\_W01K\_W02K\_W03K\_W05K\_U01K\_U02K\_K01K\_K02K\_K03 | nauki o bezpieczeństwienauki o polityce i administracjiinformatyka |
| **Treści programowe**  | Przedmiot obejmuje:* wybór tematyki, opracowanie złożeń i identyfikacja problemu badawczego,
* przygotowanie konspektu pracy magisterskiej pod kierunkiem promotora,
* dobór metod i technik badawczych do realizacji założeń pracy,
* weryfikację założeń przy wykorzystaniu wybranych metod i technik,
* przygotowanie pracy magisterskiej gotowej do obrony.
 |
| **Sposoby weryfikacji efektów uczenia się** | praca magisterska |

**Łączna liczba punktów ECTS** (w roku/semestrze): **30**

**Łączna liczba godzin zajęć** (w roku/semestrze): **195**

**Łączna liczba godzin zajęć określona w programie studiów dla danego kierunku, poziomu i profilu** (dla całego cyklu): **960**

**Procentowy udział liczby punktów ECTS w łącznej liczbie punktów ECTS dla każdej z dyscyplin, do których przyporządkowano kierunek studiów.**

|  |  |  |
| --- | --- | --- |
| **Dziedzina nauki** | **Dyscyplina naukowa** | **Procentowy udział liczby punktów ECTS w łącznej liczbie punktów ECTS dla każdej z dyscyplin** |
| dziedzina nauk społecznych | nauki o bezpieczeństwie | **60,00%** |
| dziedzina nauk ścisłych i przyrodniczych | informatyka | **15,0%** |
| dziedzina nauk społecznych | nauki o polityce i administracji | **5,83%** |

**CZĘŚĆ II**

|  |
| --- |
| **informacje dodatkowe o kierunku studiów** |
| limit przyjęć | **30** |
| liczba kandydatów wymagana do uruchomienia studiów | **18** |
| wymagania stawiane kandydatom | dyplom licencjata, magistra, inżyniera lub równoważny na dowolnym kierunku studiów. |
| kryteria przyjęcia na studia | Planowany proces kwalifikacji obejmuje dwa etapy:* punkty ze ocenę na dyplomie (z wagą 30%),
* punkty za egzamin pisemny – test wielokrotnego wyboru(z wagą 70%).
 |
| przedstawiciele otoczenia społeczno-gospodarczego współpracujący przy projektowaniu programu studiów | * dr Paweł Ciszek - Wojska Obrony Cyberprzestrzeni,
* insp. Przemysław Więcław, Dyrektor Biura Łączności i Informatyki, Komenda Główna Policji,
* Dariusz Binkowski, Dyrektor Departamentu Informatyzacji, Ministerstwo Klimatu i Środowiska,
* Wojciech Pawlak, Dyrektor NASK - Państwowy Instytut Badawczy.
 |
| przykład uwzględnienia w programie studiów opinii otoczenia społeczno-gospodarczego | Na podstawie rekomendacji Departamentu Informatyzacji, Ministerstwo Klimatu i Środowiska: „ważnym aspektem jest również cyberbezpieczeństwo automatyki przemysłowej (ang. operational technology – OT)” w programie studiów uwzględniono zagadnienia związane z infrastrukturą krytyczną i bezpieczeństwem przemysłowym. Przy tworzeniu programu wykorzystano również sugestie innych podmiotów, z którymi współpracowano podczas tworzenia opisu koncepcji kształcenia (szczegóły zawarte są w dokumencie: opis koncepcji kształcenia).Innym przykładem uwzględnienia w programie studiów opinii otoczenia społeczno-gospodarczego jest analiza wpisów w serwisie Twitter zawierających słowo „cybersecurity”[[1]](#footnote-1), którą przeprowadzono w celu znalezienia obszarów cyberbezpieczeństwa, o których mowa w opinii publicznej. W oparciu o wyniki analizy w programie studiów zamieszczono takie zagadnienia jak: ochrona danych i informacji, sztuczna inteligencja, praca w chmurze, IoT, język Python i inne. Wyniki analizy zawiera Załącznik 1.Program studiów został opracowany z wykorzystaniem wyników analizy programów studiów z zakresu cyberbezpieczeństwa uczelni polskich i zagranicznych (dokument: opis koncepcji kształcenia). Uwzględniono również liczne rekomendacje zawarte w publikacjach na temat tworzenia nowych kierunków studiów z zakresu cyberbezpieczeństwa oraz rozwoju umiejętności w zakresie cyberbezpieczeństwa, np.* wytyczne programowe dla programów kształcenia na poziomie ponadlicealnym w zakresie cyberbezpieczeństwa[[2]](#footnote-2),

<https://cyberpolicy.nask.pl/wp-content/uploads/2020/04/ENISA-Report-Cybersecurity-Skills-Development-in-the-EU.pdf>* raport na temat rozwoju umiejętności w zakresie cyberbezpieczeństwa w UE (Cybersecurity Skills Development in the EU[[3]](#footnote-3),

[file:///C:/UW/CYBERBEZPIECZE%C5%83STWO/Cybersecurity-Curricula-2017.pdf](file:///C%3A/UW/CYBERBEZPIECZE%C5%83STWO/Cybersecurity-Curricula-2017.pdf) |
| przykład uwzględnienia w programie studiów opinii studentów | Projekt programu studiów skonsultowano ze studentami studiów licencjackich WNPiSM. Celem badania było pozyskanie informacji na temat dalszych planów kształcenia się studentów oraz preferencji i oczekiwań w zakresie programu nauczania na nowym kierunku studiów - Cyberbezpieczeństwo[[4]](#footnote-4). Wśród respondentów, którzy zadeklarowali, że planują kontynuować naukę na studiach magisterskich, znaczna część - 96,1% zamierza pozostać na WNPiSM i wybrać studia z oferty wydziału. 76,1% badanych zamierza wybrać studia dzienne a 23,8% studia zaoczne. Wyniki ankiety wskazują na zasadność tworzenia nowego kierunku na studiach dziennych.Osoby które wiedzą już, który kierunek zamierzają studiować na WNPiSM, wybierają najczęściej: Stosunki międzynarodowe – 41,9% i (na drugim miejscu) nowo tworzony kierunek studiów – Cyberbezpieczeństwo – 30,2%.Wszystkie proponowane w programie nowego kierunku tematy zostały ocenione przez studentów jako bardzo ważne. Szczególną uwagę ankietowani zwrócili na znaczenie: bezpieczeństwa zasobów cyfrowych i informacji, bezpieczeństwa systemów oraz ochronę danych i prywatności w Internecie. Za najważniejsze obszary cyberbezpieczeństwa ankietowani uznali bezpieczeństwo wewnętrzne i cyberbezpieczeństwo RP.Z uwagi na fakt, że nowy kierunek Cyberbezpieczeństwo tworzony jest na WNPiSM, na którym wiodące dyscypliny naukowe należą do nauk społecznych oraz na to, że jedną z dyscyplin naukowych, przypisanych do nowego kierunku jest informatyka (20%) – dziedzina nauk ścisłychi przyrodniczych, zapytano respondentów o chęć poznania zagadnień z informatyki. Większość ankietowanych wyraziła chęć poznania obszarów IT, istotnych w tworzeniu polityki cyberbezpieczeństwa, zwłaszcza zagadnień dotyczących sztucznej inteligencji, baz danych oraz Big Data. Wyniki ankiety potwierdzają słuszność zamieszczenia w nowym programie studiów zagadnień IT i przypisanie nowego kierunku do dziedziny informatyka.Respondenci zostali również poproszeni o wypisanie zagadnień, które ich zdaniem powinny być zamieszczone w programie. Wśród odpowiedzi znalazły się:* analiza oprogramowania pod względem bezpieczeństwa danych itp.,
* cyberbezpieczeństwo stron internetowych,
* cyberbezpieczeństwo w służbach mundurowych,
* etyczne hakowanie, Python i SQL w Cybersec,
* języki programowania: JavaScript oraz C/C++/C#,
* język Python oraz cyberbezpieczeństwo w firmach,
* manipulacja, fake news, manipulowanie informacjami,
* metody łamania cyberbezpieczeństwa, sposoby na rozwiązywanie takich problemów i ich zapobieganie,
* moralny hacking,
* ochrona i zabezpieczanie danych osobowych,
* OSINT,
* przestępstwa w przestrzeni internetowej,
* psychomanipulacja w cyberprzestrzeni, sztuczna inteligencja, Big Data oraz rozwiązania chmurowe,
* sztuczna inteligencja,
* wielkie oszustwa internetowe - pod względem jak do nich doszło, skutki na ludzi, skutki w dalszej perspektywie,

 zabezpieczenie danych.Wszystkie z ww. zagadnień, z wyjątkiem języków programowania: JavaScript oraz C/C++/C#, zawarte są w projekcie programu studiów.Jedno z pytań ankiety dotyczyło preferencji dotyczących rodzaju zajęć w programie, czy mają być to zajęcia praktyczne przy komputerze, czy też nie. Prawie połowa – 49,2% respondentów wyraziła opinię, że 50% zajęć na nowym kierunku powinna być zajęciami prowadzonymi w laboratorium komputerowym.Ww. opinia respondentów zostanie uwzględniona w nowo tworzonym programie studiów. Szczegółowe wyniki ankiety zawarte są w Załączniku 2. |
| kod ISCED |  |

|  |
| --- |
| **Przedmioty do wyboru** |
| **Przedmiot** (zajęcia lub grupa zajęć) | **Liczba punktów ECTS** |
| Przedmiot swobodnego wyboru z obszaru nauk humanistycznych (z oferowanych zajęć ogólnouniwersyteckich) | **5** |
| Badania nad cyberbezpieczeństwem (projekt) | **6** |
| Wykład ogólnouniwersytecki OGUN | **8** |
| Proseminarium | **6** |
| Seminarium magisterskie | **18** |
| **Łączna liczba punktów ECTS obejmująca zajęcia do wyboru:**  | **43** |

|  |
| --- |
| **Przedmioty związane z prowadzoną w uczelni działalnością naukową w dyscyplinie lub dyscyplinach****– studia o profilu ogólnoakademickim** |
| **Przedmiot** (zajęcia lub grupa zajęć) | **Liczba punktów ECTS** |
| Podstawy cyberbezpieczeństwa | 3 |
| Państwo i społeczeństwo ryzyka | 2 |
| Analiza, ocena i zarządzanie ryzykiem występowania cyberzagrożeń | 3 |
| Bezpieczeństwo zasobów cyfrowych | 2 |
| OSINT | 2 |
| Systemy zarządzania bezpieczeństwem informacji | 3 |
| Polityka cyberbezpieczeństwa w organizacji | 3 |
| Podstawy programowania w języku Python | 3 |
| Analiza danych w języku Python | 3 |
| Bezpieczeństwo wewnętrzne i cyberbezpieczeństwo RP | 2 |
| Infrastruktura krytyczna i bezpieczeństwo przemysłowe | 3 |
| Polityka cyberbezpieczeństwa UE | 2 |
| Kryminalistyka cyfrowa | 4 |
| Normy bezpieczeństwa i ciągłości działania | 3 |
| Badania nad cyberbezpieczeństwem (projekt) | 6 |
| Bezpieczeństwo systemów bazodanowych i pracy w chmurze | 1 |
| Przetwarzanie języka naturalnego i sztuczna inteligencja | 3 |
| Bezpieczeństwo systemów | 2 |
| Ochrona danych i prywatności w Internecie | 2 |
| Symulacje cyberataków | 3 |
| Analiza Big Data w cyberbezpieczeństwie | 3 |
| Psychomanipulacja w cyberprzestrzeni | 2 |
| Ochrona danych osobowych i informacji niejawnych | 3 |
| Proseminarium | 6 |
| Seminarium magisterskie | 24 |
| **Łączna liczba punktów ECTS obejmująca przedmioty związane z prowadzoną w uczelni działalnością naukową w dyscyplinie / dyscyplinach:** | **93** |

…..…………………………….

(data i podpis Wnioskodawcy)

1. Przedmiotem analizy było 2 221 737 wpisów w serwisie Twitter zawierających słowo „cybersecurity”, opublikowanych w dniach 1.11.2021- 31.10.2022. [↑](#footnote-ref-1)
2. Dokument opracowany w 2017 roku przez grupę roboczą składająca się z największych międzynarodowych stowarzyszeń komputerowych. [↑](#footnote-ref-2)
3. Dokument opublikowany 26 marca 2020 roku przez ENISA. [↑](#footnote-ref-3)
4. Badanie zostało przeprowadzone w dniach 15-23 grudnia 2022 r. Prośba o wypełnienie ankiety została wysłana dwukrotnie za pośrednictwem Sekcji Spraw Studenckich WNPiSM. W ankiecie wzięło udział 129 osób. [↑](#footnote-ref-4)