



**Profil ogólnoakademicki**

# **Raport zespołu oceniającego Polskiej Komisji Akredytacyjnej**

---

Nazwa kierunku studiów: cyberbezpieczeństwo

Nazwa i siedziba uczelni prowadzącej kierunek: Politechnika  
Warszawska

Data przeprowadzenia wizytacji: 3-4 kwietnia 2025 r.

**Warszawa, 2025**

## Spis treści

---

|                                                                                                                                                                                                                         |          |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|
| <b>1. Informacja o wizytacji i jej przebiegu</b>                                                                                                                                                                        | <b>3</b> |
| 1.1. Skład zespołu oceniającego Polskiej Komisji Akredytacyjnej                                                                                                                                                         | 3        |
| 1.2. Informacja o przebiegu oceny                                                                                                                                                                                       | 3        |
| <b>2. Podstawowe informacje o ocenianym kierunku i programie studiów</b>                                                                                                                                                | <b>4</b> |
| <b>3. Propozycja oceny stopnia spełnienia szczegółowych kryteriów oceny programowej określona przez zespół oceniający PKA</b>                                                                                           | <b>6</b> |
| <b>4. Opis spełnienia szczegółowych kryteriów oceny programowej i standardów jakości kształcenia</b>                                                                                                                    | <b>7</b> |
| Kryterium 1. Konstrukcja programu studiów: koncepcja, cele kształcenia i efekty uczenia się                                                                                                                             | 7        |
| Kryterium 2. Realizacja programu studiów: treści programowe, harmonogram realizacji programu studiów oraz formy i organizacja zajęć, metody kształcenia, praktyki zawodowe, organizacja procesu nauczania i uczenia się | 16       |
| Kryterium 3. Przyjęcie na studia, weryfikacja osiągnięcia przez studentów efektów uczenia się, zaliczanie poszczególnych semestrów i lat oraz dyplomowanie                                                              | 26       |
| Kryterium 4. Kompetencje, doświadczenie, kwalifikacje i liczebność kadry prowadzącej kształcenie oraz rozwój i doskonalenie kadry                                                                                       | 33       |
| Kryterium 5. Infrastruktura i zasoby edukacyjne wykorzystywane w realizacji programu studiów oraz ich doskonalenie                                                                                                      | 38       |
| Kryterium 6. Współpraca z otoczeniem społeczno-gospodarczym w konstruowaniu, realizacji i doskonaleniu programu studiów oraz jej wpływ na rozwój kierunku                                                               | 45       |
| Kryterium 7. Warunki i sposoby podnoszenia stopnia umiędzynarodowienia procesu kształcenia na kierunku                                                                                                                  | 47       |
| Kryterium 8. Wsparcie studentów w uczeniu się, rozwoju społecznym, naukowym lub zawodowym i wejściu na rynek pracy oraz rozwój i doskonalenie form wsparcia                                                             | 49       |
| Kryterium 9. Publiczny dostęp do informacji o programie studiów, warunkach jego realizacji i osiągniętych rezultatach                                                                                                   | 53       |
| Kryterium 10. Polityka jakości, projektowanie, zatwierdzanie, monitorowanie, przegląd i doskonalenie programu studiów                                                                                                   | 56       |

## 1. Informacja o wizytacji i jej przebiegu

### 1.1. Skład zespołu oceniającego Polskiej Komisji Akredytacyjnej

Przewodniczący: dr hab. Inż. Jacek Kucharski, członek PKA

#### **członkowie:**

1. dr inż. Anna Pławiak-Mowna, ekspert PKA
2. dr hab. inż. Izabela Rojek, ekspert PKA
3. mgr inż. Zbigniew Rudnicki, ekspert PKA ds. pracodawców
4. Kamila Kowalczyk, ekspert PKA ds. studenckich
5. mgr Agnieszka Kozera, sekretarz zespołu oceniającego

### 1.2. Informacja o przebiegu oceny

Ocena jakości kształcenia na kierunku cyberbezpieczeństwo prowadzonym na Politechnice Warszawskiej, została przeprowadzona z inicjatywy Polskiej Komisji Akredytacyjnej w ramach harmonogramu prac określonych przez Komisję na rok akademicki 2024/2025. Wizytacja została zrealizowana zgodnie z obowiązującą procedurą oceny programowej przeprowadzanej stacjonarnie z wykorzystaniem narzędzi komunikowania się na odległość. PKA po raz pierwszy oceniała jakość kształcenia na wizytowanym kierunku.

Wizytację poprzedzono zapoznaniem się zespołu oceniającego PKA z raportem samooceny przekazanym przez władze Uczelni. Zespół odbył także spotkania organizacyjne w celu omówienia kwestii w nim przedstawionych, spraw wymagających wyjaśnienia z władzami Uczelni oraz szczegółowego harmonogramu przebiegu wizytacji.

Wizytacja rozpoczęła się od spotkania z kierownictwem Uczelni. W trakcie wizytacji odbyły się spotkania ze studentami, z przedstawicielami Samorządu Studenckiego i studenckiego ruchu naukowego, nauczycielami akademickimi prowadzącymi kształcenie na ocenianym kierunku, z osobami odpowiedzialnymi za doskonalenie jakości kształcenia, funkcjonowanie wewnętrznego systemu zapewnienia jakości kształcenia, publiczny dostęp do informacji oraz z przedstawicielami otoczenia społeczno-gospodarczego. Ponadto dokonano przeglądu wybranych prac dyplomowych i etapowych, przeprowadzono hospitację zajęć oraz dokonano przeglądu bazy dydaktycznej, wykorzystywanej w procesie dydaktycznym. Przed zakończeniem wizytacji dokonano oceny stopnia spełnienia kryteriów, sformułowano uwagi, o których przewodniczący zespołu oraz eksperci poinformowali władze Uczelni na spotkaniu podsumowującym.

Podstawa prawna oceny została określona w załączniku nr 1, a szczegółowy harmonogram wizytacji, uwzględniający podział zadań pomiędzy członków zespołu oceniającego, w załączniku nr 2.

## 2. Podstawowe informacje o ocenianym kierunku i programie studiów

|                                                                                                                                                                                               |                                          |                              |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------|------------------------------|
| Nazwa kierunku studiów                                                                                                                                                                        | cyberbezpieczeństwo                      |                              |
| Poziom studiów<br>(studia pierwszego stopnia/studia drugiego stopnia/jednolite studia magisterskie)                                                                                           | pierwszy poziom studiów                  |                              |
| Profil studiów                                                                                                                                                                                | ogólnoakademicki                         |                              |
| Forma studiów (stacjonarne/niestacjonarne)                                                                                                                                                    | stacjonarne                              |                              |
| Nazwa dyscypliny, do której został przyporządkowany kierunek <sup>1,2</sup>                                                                                                                   | informatyka techniczna i telekomunikacja |                              |
| Liczba semestrów i liczba punktów ECTS konieczna do ukończenia studiów na danym poziomie określona w programie studiów                                                                        | 7 semestrów, 210 ECTS                    |                              |
| Wymiar praktyk zawodowych <sup>3</sup> /liczba punktów ECTS przyporządkowanych praktykom zawodowym (jeżeli program studiów przewiduje praktyki)                                               | 160/4 ECTS                               |                              |
| Specjalności / specjalizacje realizowane w ramach kierunku studiów                                                                                                                            | -                                        |                              |
| Tytuł zawodowy nadawany absolwentom                                                                                                                                                           | inżynier                                 |                              |
|                                                                                                                                                                                               | <b>Studia stacjonarne</b>                | <b>Studia niestacjonarne</b> |
| Liczba studentów kierunku                                                                                                                                                                     | 183                                      | -                            |
| Liczba godzin zajęć z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia i studentów <sup>4</sup>                                                            | 2709                                     | -                            |
| Liczba punktów ECTS objętych programem studiów uzyskiwana w ramach zajęć z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia i studentów                    | 108                                      |                              |
| Łączna liczba punktów ECTS przyporządkowana zajęciom związanym z prowadzoną w uczelni działalnością naukową w dyscyplinie lub dyscyplinach, do których przyporządkowany jest kierunek studiów | 135                                      |                              |
| Liczba punktów ECTS objętych programem studiów uzyskiwana w ramach zajęć do wyboru                                                                                                            | 74                                       |                              |

<sup>1</sup> W przypadku przyporządkowania kierunku studiów do więcej niż 1 dyscypliny - nazwa dyscypliny wiodącej, w ramach której uzyskiwana jest ponad połowa efektów uczenia się oraz nazwy pozostałych dyscyplin wraz z określeniem procentowego udziału liczby punktów ECTS dla dyscypliny wiodącej oraz pozostałych dyscyplin w ogólnej liczbie punktów ECTS wymaganej do ukończenia studiów na kierunku

<sup>2</sup> Nazwy dyscyplin należy podać zgodnie z rozporządzeniem MEiN z dnia 11 października 2022 r. w sprawie dziedzin nauki i dyscyplin naukowych oraz dyscyplin artystycznych (Dz.U. 2022 poz. 2202).

<sup>3</sup> Proszę podać wymiar praktyk w miesiącach oraz w godzinach dydaktycznych.

<sup>4</sup> Liczbę godzin zajęć z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia i studentów należy podać bez uwzględnienia liczby godzin praktyk zawodowych.

|                                                                                                                                                                                                      |                                          |                              |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------|------------------------------|
| <b>Nazwa kierunku studiów</b>                                                                                                                                                                        | cyberbezpieczeństwo                      |                              |
| <b>Poziom studiów<br/>(studia pierwszego stopnia/studia drugiego stopnia/jednolite studia magisterskie)</b>                                                                                          | drugi poziom studiów                     |                              |
| <b>Profil studiów</b>                                                                                                                                                                                | ogólnoakademicki                         |                              |
| <b>Forma studiów (stacjonarne/niestacjonarne)</b>                                                                                                                                                    | stacjonarne                              |                              |
| <b>Nazwa dyscypliny, do której został przyporządkowany kierunek<sup>5,6</sup></b>                                                                                                                    | informatyka techniczna i telekomunikacja |                              |
| <b>Liczba semestrów i liczba punktów ECTS konieczna do ukończenia studiów na danym poziomie określona w programie studiów</b>                                                                        | 3 semestry, 90 ECTS                      |                              |
| <b>Wymiar praktyk zawodowych<sup>7</sup> /liczba punktów ECTS przyporządkowanych praktykom zawodowym (jeżeli program studiów przewiduje praktyki)</b>                                                | -                                        |                              |
| <b>Specjalności / specjalizacje realizowane w ramach kierunku studiów</b>                                                                                                                            | -                                        |                              |
| <b>Tytuł zawodowy nadawany absolwentom</b>                                                                                                                                                           | magister inżynier                        |                              |
|                                                                                                                                                                                                      | <b>Studia stacjonarne</b>                | <b>Studia niestacjonarne</b> |
| <b>Liczba studentów kierunku</b>                                                                                                                                                                     | 32                                       |                              |
| <b>Liczba godzin zajęć z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia i studentów<sup>8</sup></b>                                                             | 900                                      |                              |
| <b>Liczba punktów ECTS objętych programem studiów uzyskiwana w ramach zajęć z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia i studentów</b>                    | 46                                       |                              |
| <b>Łączna liczba punktów ECTS przyporządkowana zajęciom związanym z prowadzoną w uczelni działalnością naukową w dyscyplinie lub dyscyplinach, do których przyporządkowany jest kierunek studiów</b> | 71                                       |                              |

<sup>5</sup> W przypadku przyporządkowania kierunku studiów do więcej niż 1 dyscypliny - nazwa dyscypliny wiodącej, w ramach której uzyskiwana jest ponad połowa efektów uczenia się oraz nazwy pozostałych dyscyplin wraz z określeniem procentowego udziału liczby punktów ECTS dla dyscypliny wiodącej oraz pozostałych dyscyplin w ogólnej liczbie punktów ECTS wymaganej do ukończenia studiów na kierunku

<sup>6</sup> Nazwy dyscyplin należy podać zgodnie z rozporządzeniem MEiN z dnia 11 października 2022 r. w sprawie dziedzin nauki i dyscyplin naukowych oraz dyscyplin artystycznych (Dz.U. 2022 poz. 2202).

<sup>7</sup> Proszę podać wymiar praktyk w miesiącach oraz w godzinach dydaktycznych.

<sup>8</sup> Liczbę godzin zajęć z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia i studentów należy podać bez uwzględnienia liczby godzin praktyk zawodowych.

|                                                                                    |    |  |
|------------------------------------------------------------------------------------|----|--|
| Liczba punktów ECTS objętych programem studiów uzyskiwana w ramach zajęć do wyboru | 40 |  |
|------------------------------------------------------------------------------------|----|--|

### 3. Propozycja oceny stopnia spełnienia szczegółowych kryteriów oceny programowej określona przez zespół oceniający PKA

| Szczegółowe kryterium oceny programowej                                                                                                                                                                                 | Propozycja oceny stopnia spełnienia kryterium określona przez zespół oceniający PKA <sup>9</sup><br>kryterium spełnione/<br>kryterium spełnione częściowo/<br>kryterium niespełnione |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Kryterium 1. konstrukcja programu studiów: koncepcja, cele kształcenia i efekty uczenia się                                                                                                                             | kryterium spełnione                                                                                                                                                                  |
| Kryterium 2. realizacja programu studiów: treści programowe, harmonogram realizacji programu studiów oraz formy i organizacja zajęć, metody kształcenia, praktyki zawodowe, organizacja procesu nauczania i uczenia się | kryterium spełnione                                                                                                                                                                  |
| Kryterium 3. przyjęcie na studia, weryfikacja osiągnięcia przez studentów efektów uczenia się, zaliczanie poszczególnych semestrów i lat oraz dyplomowanie                                                              | kryterium spełnione                                                                                                                                                                  |
| Kryterium 4. kompetencje, doświadczenie, kwalifikacje i liczebność kadry prowadzącej kształcenie oraz rozwój i doskonalenie kadry                                                                                       | kryterium spełnione                                                                                                                                                                  |
| Kryterium 5. infrastruktura i zasoby edukacyjne wykorzystywane w realizacji programu studiów oraz ich doskonalenie                                                                                                      | kryterium spełnione                                                                                                                                                                  |
| Kryterium 6. współpraca z otoczeniem społeczno-gospodarczym w konstruowaniu, realizacji i doskonaleniu programu studiów oraz jej wpływ na rozwój kierunku                                                               | kryterium spełnione                                                                                                                                                                  |
| Kryterium 7. warunki i sposoby podnoszenia stopnia umiędzynarodowienia procesu kształcenia na kierunku                                                                                                                  | kryterium spełnione                                                                                                                                                                  |

<sup>9</sup> W przypadku gdy oceny dla poszczególnych poziomów studiów różnią się, należy wpisać ocenę dla każdego poziomu odrębnie.

|                                                                                                                                                             |                     |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| Kryterium 8. wsparcie studentów w uczeniu się, rozwoju społecznym, naukowym lub zawodowym i wejściu na rynek pracy oraz rozwój i doskonalenie form wsparcia | kryterium spełnione |
| Kryterium 9. publiczny dostęp do informacji o programie studiów, warunkach jego realizacji i osiągniętych rezultatach                                       | kryterium spełnione |
| Kryterium 10. polityka jakości, projektowanie, zatwierdzanie, monitorowanie, przegląd i doskonalenie programu studiów                                       | kryterium spełnione |

#### 4. Opis spełnienia szczegółowych kryteriów oceny programowej i standardów jakości kształcenia

##### Kryterium 1. Konstrukcja programu studiów: koncepcja, cele kształcenia i efekty uczenia się

##### Analiza stanu faktycznego i ocena spełnienia kryterium 1

Kierunek cyberbezpieczeństwo na poziomie studiów I i II stopnia prowadzony jest na Politechnice Warszawskiej w formie stacjonarnej. Jednostką odpowiedzialną za realizację kształcenia na ocenianym kierunku jest Wydział Elektroniki i Technik Informacyjnych.

Celem kształcenia na kierunku jest przygotowanie absolwentów do projektowania, realizowania, testowania oraz utrzymywania sprawności sprzętu i oprogramowania, które służą zapewnieniu bezpieczeństwa systemów teleinformatycznych. Ponadto absolwenci przygotowani są do reagowania i przeciwdziałania w sposób minimalizujący skutki (spodziewanym i zainicjowanym) atakom, które stwarzają zagrożenie dla bezpieczeństwa dla sieci i systemów teleinformatycznych. Identyfikowanie i analizowanie cyberzagrożeń w odniesieniu do danych, systemów informacyjnych oraz sieci komputerowych jest przeprowadzane na podstawie informacji, które pochodzą z różnych źródeł. Koncepcja programu na kierunku cyberbezpieczeństwo zarówno w odniesieniu do studiów I jak i II stopnia wynika również ze zmieniających się wymagań, m.in. natury organizacyjno-prawnej w kontekście zabezpieczenia rozwiązań oraz rozpoznawania i przeciwdziałania incydentom, czy też minimalizowania ich skutków. Przed absolwentami tego kierunku, który przypisany jest do dyscypliny informatyka techniczna i telekomunikacja, w porównaniu do oczekiwań otoczenia społeczno-gospodarczego sprzed kilku lat stawiane są nowe wymagania. Stąd nie tylko aspekty związane z posiadaniem umiejętności w zakresie na przykład projektowania i wykonania, testowania czy wdrożenia systemu czy sieci teleinformatycznych, ale również w zakresie szeroko rozumianych aspektów zabezpieczania tych rozwiązań oraz rozpoznawania zagrożeń, przeprowadzenia ich analizy (również w kontekście rozpoznania potencjalnych ataków) oraz minimalizowanie skutków cyberataków, są kluczowe dla specjalistów z zakresu cyberbezpieczeństwa.

Absolwent studiów I stopnia na kierunku cyberbezpieczeństwo posiada wiedzę i umiejętności, m.in.: z zakresu matematyki, informatyki, teleinformatyki, telekomunikacji i techniki cyfrowej, oprogramowania systemów komputerowych i sieci teleinformatycznych, które są niezbędne do kształtowania specjalistycznych kompetencji w obszarze cyberbezpieczeństwa. Jak również są kluczowe dla rozwoju i uzupełniania tych kompetencji w zmieniających się uwarunkowaniach

otoczenia społeczno-gospodarczego oraz w świetle postępu technologicznego. Nabytą wiedzę absolwenci wykorzystują przede wszystkim do identyfikowania i rozwiązywania problemów z obszaru bezpiecznego funkcjonowania wystawionych na zagrożenia systemów komputerowych i sieci teleinformatycznych; co jest realizowane dzięki umiejętnościom takim jak: wykorzystywanie informacji pozyskiwanych z różnych źródeł na potrzeby identyfikowania i analizowania zagrożeń bezpieczeństwa dla ww. systemów oraz danych, projektowanie, realizowanie, testowanie i utrzymywanie sprzętu i oprogramowania dedykowanego do zapewnienia bezpieczeństwa systemów informacyjnych i sieci teleinformatycznych oraz adekwatne reagowanie w sytuacjach zagrożenia. Ponadto absolwent studiów ma świadomość pozatechnicznych aspektów działalności inżynierskiej, działania na rzecz interesu publicznego oraz myślenia w sposób przedsiębiorczy.

Absolwent studiów II stopnia na kierunku cyberbezpieczeństwo posiada wiedzę i umiejętności m.in. w zakresie: procesów zachodzących w systemach teleinformatycznych istotnych dla zapewnienia ich bezpiecznego funkcjonowania, prowadzenia prac o charakterze badawczym w szczególności związanych z badaniami z zakresu cyberbezpieczeństwa oraz zaawansowanych narzędzi informatycznych niezbędnych do analizy wyników badań. Ponadto absolwent posiada wiedzę i umiejętności m.in. z zakresu matematyki, analizy danych, zabezpieczenia rozwiązań sprzętowych i komunikacji opartej na najnowszych standardach sieci bezprzewodowych. Zna systemy Internetu Rzeczy (IoT) w kontekście cyberbezpieczeństwa, które stosuje na potrzeby identyfikowania problemów i ich rozwiązywania z wykorzystaniem właściwie dobranych metod i narzędzi, wprowadzając elementy innowacyjności oraz weryfikując poprawność opracowanych rozwiązań. Student, który ukończył studia cyberbezpieczeństwo na drugim stopniu zna główne tendencje rozwojowe informatyki technicznej i telekomunikacji oraz rozumie aspekty tworzenia i rozwoju różnych form indywidualnej przedsiębiorczości (również w formie start-up). Uzyskuje także metodologiczne podstawy prowadzenia prac badawczych właściwych dla dyscypliny informatyka techniczna i telekomunikacja.

Misja i wizja rozwoju Politechniki Warszawskiej została przyjęta Uchwałą Nr 159/L/2021 Senatu Politechniki Warszawskiej z dnia 22 grudnia 2021 roku. W dokumencie Strategia Rozwoju Politechniki Warszawskiej do roku 2030 wskazano, że misja Uczelni postrzegana jest jako kreatywny udział w kształtowaniu przyszłości, co realizowane jest poprzez badania, które tworzą nową wiedzę i technologie przyszłości, jak również poprzez kształtowanie następnych pokoleń. Ponadto w strategii określono, że misja wpisuje się w zakres działań koncentrujących się na badaniach związanych z największymi wyzwaniami cywilizacyjnymi. Wizja Politechniki Warszawskiej to pozycja uznanej i rozpoznawalnej technicznej uczelni badawczej, która jest atrakcyjnym ośrodkiem naukowo-dydaktycznym, w którym prowadzone są badania naukowe i kształcenie na światowym poziomie. Ponadto doprecyzowano, że wizja Uczelni wpisuje się w działania obejmujące przede wszystkim kształtowanie trendów rozwoju technologii, dostarczanie wiedzy i rozwiązań dla krajowego i światowego przemysłu, co pozostaje w bezpośrednim związku z kształceniem kompetentnej kadry naukowej oraz wspierającej przemysł przyszłości. Koncepcja kształcenia na ocenianym kierunku studiów jest zgodna z misją i strategią rozwoju Uczelni. Kształcenie studentów na ocenianym kierunku cyberbezpieczeństwo wpisuje się w tworzenie „wykwalifikowanej, kompetentnej kadry naukowej i kadry wspierającej przemysł przyszłości”. Dodatkowo, w ślad za zdefiniowanym dla Uczelni katalogiem strategicznych obszarów (jej) działalności badawczej i dydaktycznej wyrażonych w Strategicznych Polach Oddziaływania, kierunek cyberbezpieczeństwo wpisuje się ich zakres. Na przykład w odniesieniu do pola „Informacja i otoczenie cyfrowe” dla którego wskazano między innymi aspekty rozwoju opartego na danych w kontekście poszczególnych sektorów gospodarki jak na



przykład inteligentnych rozwiązań dla miast, administracji państwowej, sektora finansowego i telekomunikacji czy przedsiębiorstw przemysłu 4.0. W takim ujęciu aspekty bezpieczeństwa i ochrony danych oraz zapewnienie infrastruktury sprzętowej i programowej na potrzeby cyfrowego bezpieczeństwa, jak również umiejętność identyfikacji ryzyka i przeciwdziałanie incydentom oraz minimalizowanie skutków cyberataków bezpośrednio wpisują się w cele i koncepcję kształcenia na kierunku cyberbezpieczeństwo, a absolwenci przygotowani są do wdrożenia i zaprojektowania skutecznych rozwiązań we wskazanym wyżej zakresie. W Strategii Uczelni w kontekście cyfrowej transformacji wliczono cyberbezpieczeństwo. W konstrukcji programu kształcenia na kierunku cyberbezpieczeństwo został położony znaczny nacisk na bezpieczeństwo danych i otoczenie cyfrowe, które wiążą się z cyfryzacją społeczeństw. Stąd można sformułować wniosek, że koncepcja kształcenia kierunku cyberbezpieczeństwo i wymagania przed jakimi stawiani są absolwenci kierunku korelują z misją i strategią przyjętą w Uczelni. Polityka jakości kształcenia została sformułowana i wskazana w Księdze Jakości Kształcenia Politechniki Warszawskiej przyjętej Uchwałą Nr 16/LI/2024 Senatu Politechniki Warszawskiej z dnia 25 września 2024 r. Wskazuje się tam między innymi, że proces rozwoju i doskonalenia jakości kształcenia realizowany jest w powiązaniu z prowadzonymi badaniami naukowymi oraz z uwzględnieniem zmieniających się warunków otoczenia społeczno-gospodarczego. Oceniany kierunek jest skorelowany badaniami naukowymi prowadzonymi w dyscyplinie informatyka techniczna i telekomunikacja, do której został przyporządkowany, a koncepcja i monitorowanie programu kształcenia, które realizowane jest przy udziale partnerów z otoczenia społeczno-gospodarczego oraz z wykorzystaniem szeroko zakrojonych analiz zarówno w obszarze zmian na rynku cyberbezpieczeństwa oraz w obszarze potrzeb i losów absolwentów.

Zatem koncepcja i cele kształcenia na kierunku cyberbezpieczeństwo na studiach I i II stopnia są zgodne ze strategią Politechniki Warszawskiej. Przypisanie ocenianego kierunku studiów I i II stopnia w 100% do dyscypliny informatyka techniczna i telekomunikacja, w kontekście opisanej wyżej koncepcji kształcenia, jest prawidłowe.

Na Uczelni prowadzona jest działalność naukowa w dyscyplinie informatyka techniczna i telekomunikacja, do której przyporządkowany jest oceniany kierunek studiów. W wyniku ewaluacji działalności naukowej za lata 2017-2021 dyscyplina ta uzyskała ocenę A, co świadczy o wysokiej jakości prowadzonych badań naukowych. W dyscyplinie informatyka techniczna i telekomunikacja prowadzone są badania naukowe między innymi w zakresie: rozwoju metod optymalizacji, systemów transmisyjnych i przetwarzania sygnałów, metod uczenia maszynowego, sieci nowych generacji i nowych technik sieciowych oraz cyberbezpieczeństwa. W odniesieniu do badań w zakresie cyberbezpieczeństwa obejmują obszary jak na przykład: kryminalistyka cyfrowa, kryptoanaliza, Cyber Threat Intelligence, Threat Hunting, detekcja anomalii z wykorzystaniem AI, reagowanie na incydenty bezpieczeństwa i zarządzanie nimi, optymalizacja systemów cyberbezpieczeństwa, bezpieczeństwo sieci 5G+/6G, zaufane środowisko wykonawcze do realizacji mechanizmów cyberbezpieczeństwa w rozwiązaniach SmartCity, Industry 4.0 oraz aspekty związane z białym wywiadem, bezpieczeństwem operacyjnym czy w ujęciu interdyscyplinarnym – cyberbiobezpieczeństwo. Aktywnie realizowana jest współpraca o charakterze badawczym i rozwojowym z ośrodkami międzynarodowymi. Powyższe aktywności składają się na wysokiej jakości kompleksowy charakter działalności badawczej, która odpowiada koncepcji i celom kształcenia na ocenianym kierunku

Koncepcja i cele kształcenia pozostają w ścisłej korelacji z zawodowym rynkiem pracy i są zorientowane na potrzeby otoczenia społeczno-gospodarczego. W Uczelni realizowane są w ww. szczegółowe analizy, których wyniki publikowane są w formie raportów. Analizy, jak na przykład „Pracodawca dla

inżyniera 2023”, „Absolwenci Wydziału Elektroniki i Technik Informacyjnych Politechniki Warszawskiej”, czy „Rynek pracy na Mazowszu w kontekście kształcenia na uczelni technicznej 2019-2022” to zasoby, które pozwalają na skuteczne wyrobienie sobie opinii w zakresie zapotrzebowania i wymagań rynku pracy. Należy podkreślić, że w Uczelni przyjęte zostały wytyczne w zakresie badań społecznych realizowanych na potrzeby identyfikacji potrzeb otoczenia społeczno-gospodarczego (publikacja „Potrzeby otoczenia społeczno-gospodarczego Uczelni – czym są i jak je badać?”). Ponadto w jednostce poddaje się analizie raporty i doniesienia powiązane z ocenianym kierunkiem między innymi przedstawiany na Światowym Forum Ekonomicznym raport Global Cybersecurity Outlook 2025, czy też 2024 ISC2 Cybersecurity Workforce Global Cybersecurity Workforce Prepares for an AI-Driven World oraz Strategic Cybersecurity Talent Framework (2024). Wskazane publikacje pozwalają na śledzenie potrzeb w kontekście kształcenia specjalistów cyberbezpieczeństwa. W ramach kierunku kształceni są specjaliści, którzy przygotowani są do pracy w firmach, w których tworzone są rozwiązania informatyczne zarówno w kontekście sprzętu jak i oprogramowania z uwzględnieniem właściwych poziomów bezpieczeństwa, jak i w firmach, w których opracowywane są specjalistyczne rozwiązania na potrzeby zapewnienia bezpieczeństwa systemów i sieci teleinformatycznych. Ponadto studenci, którzy zakończyli kształcenie na kierunku są przygotowani do podjęcia pracy w instytucjach i przedsiębiorstwach, w których systemy informatyczne są stosowane, a aspekty bezpieczeństwa cyfrowego sprzętu i oprogramowania są kluczowe (jak na przykład operatorzy telekomunikacji, banki czy urzędy administracji publicznej). Absolwenci mogą podjąć pracę również w: instytucjach, które zajmują się różnorodnymi aspektami cyberbezpieczeństwa państwa oraz firmach, w których realizowane są konsultacje, integracje bądź wdrożenia rozwiązań informatycznych. Osoby, które ukończyły kształcenie na kierunku są przygotowane do pojęcia własnej działalności gospodarczej.

W przygotowywaniu koncepcji kształcenia brali udział interesariusze zewnątrzni i wewnątrzni. W badaniu poprzedzającym przygotowanie studiów wzięli udział przedstawiciele potencjalnych pracodawców, firm jak na przykład: Asseco, Centralne Laboratorium Kryminalistyczne Policji, CERT Polska, Cryptomage, IBM, KPMG, Narodowe Centrum Kryptologii, Orange, PKO BP, Play, T-Mobile, VT Cyber, WB Electronics. Wyniki badań ankietowych w odniesieniu do oczekiwanych kompetencji absolwenta kierunku zostały opracowane i poddane analizie. Opracowane wyniki wpłynęły na kształt ostatecznej wersji programu na przykład w wyniku podjętych konsultacji większy nacisk położono na aspekty bezpieczeństwa systemów informatycznych i ochrony danych osobowych, testowania oprogramowania oraz projektowania złożonych systemów informatycznych. Należy podkreślić, że również studenci Wydziału mieli czynny udział w określeniu koncepcji kształcenia kierunku. Postulowali oni np. konieczność wprowadzenia na początku cyklu kształcenia przedmiotu, którego zakres tematyczny obejmowałby wprowadzenie do obszaru cyberbezpieczeństwa. Doświadczenie wysokiej klasy ekspertów z obszaru cyberbezpieczeństwa (np. dyrektor departamentu Cyberbezpieczeństwa w Ministerstwie Cyfryzacji, wiceprezes zarządu ComCERT SA czy zastępca dyrektora NASK do Spraw Naukowych) oraz pracowników Wydziału również stanowiło cenny wkład w przygotowanie koncepcji kształcenia. W wyniku konsultacji z ww. ekspertami dokonano między innymi działań: wprowadzenie treści kształcenia np. aspektów w zakresie kill chain, analizy malware, pentesting i digital forensics, bezpiecznych chmur obliczeniowych; zmiana umiejscowienia przedmiotów w semestrach (np. przeniesienie przedmiotu Chmury i sieci); doprecyzowanie nazewnictwa przedmiotów (np. sieci mobilne i sieci internetu rzeczy). Dokumentacja odnosząca się do przebiegu współpracy przedstawiona ZO pozwala sformułować wniosek, że koncepcja i cele kształcenia zostały określone we współpracy z interesariuszami wewnętrznymi i zewnętrznymi.

Koncepcja kształcenia nie uwzględnia nauczania z wykorzystaniem metod i technik kształcenia na odległość.

W programie studiów I stopnia kierunek cyberbezpieczeństwo określono 12 kierunkowych efektów uczenia się z zakresu wiedzy, 13 z zakresu umiejętności oraz 5 z zakresu kompetencji społecznych. W odniesieniu do II stopnia studiów kierunek cyberbezpieczeństwo określonych zostało 13 kierunkowych efektów uczenia się z zakresu wiedzy, 14 z zakresu umiejętności oraz 4 z zakresu kompetencji społecznych.

W odniesieniu do I stopnia studiów kierunku cyberbezpieczeństw do kluczowych efektów uczenia się jednostka zalicza:

- absolwent ma wiedzę w zakresie matematyki, obejmującą logikę, teorię mnogości, analizę, algebrę, rachunek prawdopodobieństwa i statystykę matematyczną opisu i analizy działania systemów przesyłania, która to wiedza daje podstawy do opisu i analizy: przetwarzania i gromadzenia informacji, sygnałów, komponentów systemów i sieci teleinformatycznych, projektowania rozwiązań związanych z zapewnieniem cyberbezpieczeństwa systemów informacyjnych i sieci teleinformatycznych; ma wiedzę w zakresie fizyki umożliwiającą zrozumienie zjawisk fizycznych występujących w komponentach systemów i sieci teleinformatycznych oraz mechanizmów ataków na ich warstwę fizyczną, przeciwdziałania atakom oraz analizę i projektowanie nowych metod ochrony informacji; ma wiedzę w zakresie elektroniki i telekomunikacji oraz także teorii systemów, która tworzy podstawy do identyfikowania problemów i formułowania specyfikacji oraz rozwiązywania złożonych zadań inżynierskich i problemów badawczych; ma wiedzę w zakresie techniki cyfrowej i sprzętowych komponentów systemów komputerowych i sieci teleinformatycznych na potrzeby projektowania i zabezpieczania warstwy sprzętowej systemów teleinformatycznych; ma wiedzę w zakresie oprogramowania systemów komputerowych i sieci teleinformatycznych do projektowania i zabezpieczania warstwy programowej systemów teleinformatycznych; ma wiedzę w zakresie teleinformatyki na potrzeby projektowania komponentów sieci teleinformatycznych; ma wiedzę w zakresie cyberbezpieczeństwa niezbędną do projektowania rozwiązań związanych z zapewnieniem bezpieczeństwa systemów informacyjnych i sieci teleinformatycznych,
- przy identyfikowaniu problemów i formułowaniu rozwiązania zadań inżynierskich oraz problemów badawczych (również zadań i problemów złożonych i nietypowych w kontekście zapewnienia cyberbezpieczeństwa) absolwent potrafi: wykorzystywać wiedzę z zakresu nauk podstawowych oraz nauk technicznych, pozyskiwać uzupełniające informacje, dokonać ich selekcji, interpretacji oraz krytycznej oceny, integrować informacje, wyciągać wnioski jak również formułować i uzasadniać opinie; potrafi dokonać oceny i krytycznej analizy rozwiązań w zakresie cyberbezpieczeństwa; potrafi planować i przeprowadzać eksperymenty oraz dokonać interpretacji uzyskanych wyników i wyciągać wnioski; przy identyfikowaniu problemów i formułowaniu rozwiązania zadań inżynierskich oraz problemów badawczych (również zadań i problemów złożonych i nietypowych w kontekście zapewnienia cyberbezpieczeństwa) potrafi: wykorzystać (również w sposób innowacyjny) metody analityczne, symulacyjne i eksperymentalne oraz właściwie dobrane narzędzia, uwzględnić aspekty systemowe i pozatechniczne oraz dokonać wstępnej oceny ekonomicznej proponowanych rozwiązań; potrafi zidentyfikować oraz analizować podatność i zagrożenia dla bezpieczeństwa (danych, oprogramowania, systemów informacyjnych i sieci teleinformatycznych oraz ich komponentów) wykorzystując informacje pochodzące z

różnych źródeł; potrafi ocenić możliwości funkcjonowania systemu lub sieci w warunkach wystąpienia zagrożeń, przewidzieć ich skutki oraz zaproponować działania minimalizujące te skutki; potrafi (z zastosowaniem właściwie dobranych metod i narzędzi); zaprojektować, zrealizować, przetestować i ocenić fragment infrastruktury sprzętowej i oprogramowanie wykorzystane do zapewnienia bezpieczeństwa systemu informacyjnego lub sieci teleinformatycznej,

- absolwent potrafi (wg opracowanego samodzielnie harmonogramu) pracować indywidualnie i w zespole (również interdyscyplinarnym); potrafi opracować dokumentację, zaprezentować i uczestniczyć w dyskusji dot. realizacji zadania inżynierskiego; potrafi dyskutować na tematy techniczne z obszaru cyberbezpieczeństwa oraz dokonywać ocen przedstawianych rozwiązań i opinii; posługuje się językiem angielskim na poziomie B2; ma umiejętność samokształcenia się, absolwent rozumie potrzebę stałego aktualizowania wiedzy i podnoszenia kompetencji zawodowych oraz ekonomiczne, społeczne, inne pozatechniczne aspekty, skutki oraz odpowiedzialność działalności inżyniera; ma świadomość etyki zawodowej, profesjonalizmu oraz znaczenia wiedzy w rozwiązywaniu problemów inżynierskich; jest gotów do działania w sposób przedsiębiorczy i działa na rzecz interesu publicznego.

W odniesieniu do studiów II stopnia kierunku cyberbezpieczeństwo do kluczowych efektów uczenia się zaliczyć można:

- w zakresie wiedzy: absolwent zna metodologiczne podstawy prowadzenia badań naukowych, metodyki prowadzenia prac o charakterze badawczym w dziedzinie nauk inżynierijno-technicznych (w szczególności związanych z badaniami z zakresu cyberbezpieczeństwa); zna teorie i metody oraz zaawansowane narzędzia informatyczne stosowane do analizy wyników badań; ma zaawansowaną wiedzę z zakresu matematyki na potrzeby identyfikowania oraz innowacyjnego rozwiązywania złożonych i nietypowych zadań inżynierskich oraz problemów badawczych związanych z zapewnieniem cyberbezpieczeństwa; ma zaawansowaną wiedzę z zakresu zapewniania bezpieczeństwa systemów Internetu Rzeczy; ma zaawansowaną wiedzę z zakresu wybranych aspektów cyberbezpieczeństwa, tj. bezpieczeństwo: rozwiązań sprzętowych, komunikacji opartej na najnowszych standardach sieci bezprzewodowych; zna cykl życia systemów teleinformatycznych w kontekście bezpieczeństwa tych systemów,
- w kontekście umiejętności: absolwent potrafi przeprowadzić krytyczną analizę oraz ocenić funkcjonowanie rozwiązań technicznych z zakresu bezpieczeństwa systemów teleinformatycznych; potrafi postawić hipotezy, planować, przeprowadzać eksperymenty oraz badania w zakresie bezpieczeństwa systemów teleinformatycznych stosując zaawansowane narzędzia informatyczne oraz potrafi interpretować otrzymane wyniki; potrafi analizować danych w kontekście ich zastosowań w rozwiązywaniu problemów związanych z zapewnieniem bezpieczeństwa systemów teleinformatycznych oraz zabezpieczyć sieci bezprzewodowe najnowszych generacji i systemów Internetu Rzeczy; potrafi (stosując właściwie dobrane metody i narzędzia) zaprojektować (z elementami innowacyjności) rozwiązanie bezpieczeństwa systemów teleinformatycznych; w pracach badawczych oraz przy rozwiązywaniu zadań dotyczących zapewnienia bezpieczeństwa systemów teleinformatycznych potrafi wykorzystać metody analityczne, symulacyjne i eksperymentalne, właściwie dobrać i wykorzystać metody, techniki i narzędzia oraz przystosować istniejące lub opracować nowe metody i narzędzia i przeprowadzić weryfikację rozwiązania,

- w kontekście kompetencji społecznych: efekty związane z przedsiębiorczością, rolą społeczną absolwenta uczelni technicznej, odpowiedzialnym pełnieniem ról oraz aktualizowaniem wiedzy.

Wyżej wskazane zestawienie pozwala sformułować wniosek, że zarówno efekty uczenia się przyjęte dla I jak i II stopnia studiów kierunku cyberbezpieczeństwo są zgodne z celami kształcenia.

Opis sformułowanych efektów uczenia się jest w większości prawidłowy w kontekście poziomu zaawansowania i złożoności wiedzy oraz umiejętności, zgodnie z 6 poziomem Polskiej Ramy Kwalifikacji dla studiów pierwszego stopnia i 7 dla studiów drugiego stopnia. Jednak w niektórych przypadkach efektów uczenia się w obszarze wiedzy i umiejętności stwierdzono, że nieprecyzyjnie określono głębokość zdobywanej wiedzy czy umiejętności. Na przykład w odniesieniu do studiów I stopnia używa się sformułowań - elementarny - „ma elementarną wiedzę na temat procesów zachodzących w cyklu życia komponentów systemu informacyjnego lub sieci teleinformatycznej oraz tych systemów i sieci” lub nie wskazuje się głębokości np. „ma wiedzę w zakresie oprogramowania systemów komputerowych i sieci teleinformatycznych...”, „ma wiedzę w zakresie teleinformatyki...” czy „potrafi ocenić możliwości funkcjonowania systemu lub sieci w warunkach wystąpienia zagrożeń; potrafi przewidzieć...”. W odniesieniu do studiów II stopnia używa się określeń - zaawansowany - np. „ma zaawansowaną wiedzę z zakresu matematyki...”. Charakterystyki drugiego stopnia efektów uczenia się dla kwalifikacji na poziomach 6-8 Polskiej Ramy kwalifikacji typowe dla kwalifikacji uzyskiwanych w ramach systemu szkolnictwa wyższego i nauk określają, że student powinien pozyskać wiedzę „w zaawansowanym stopniu” a w obszarze umiejętności „formułować i rozwiązywać złożone i nietypowe problemy” (poziom 6), a pozyskać wiedzę „w pogłębionym stopniu” oraz „formułować i rozwiązywać złożone i nietypowe problemy i innowacyjnie wykonywać zadania” w odniesieniu do umiejętności (poziom 7). Sformułowania takie zastosowane są w odniesieniu do pojedynczych efektów uczenia się (np. „potrafi – przy identyfikowaniu problemów i formułowaniu specyfikacji zadań inżynierskich oraz problemów badawczych, w tym zadań i problemów złożonych i nietypowych, związanych z zapewnieniem cyberbezpieczeństwa...”), nie oddając w ten sposób właściwej głębokości wiedzy jaką powinien osiągnąć student. W związku z tym rekomenduje się dokonanie przeglądu kierunkowych efektów uczenia się oraz efektów przedmiotowych i takie ich przeformułowanie, aby nie wzbudzały wątpliwości w zakresie zaawansowania i głębokości wiedzy zdobywanej i umiejętności osiągniętych na studiach cyberbezpieczeństwo studia I i II stopnia.

Poddając analizie zdefiniowane efekty uczenia się i karty przedmiotów, na przykład dla przedmiotów *bezpieczeństwo społeczne, organizacyjne i zarządzanie cyberbezpieczeństwem* (studia I stopnia) czy *bezpieczeństwo Internetu Rzeczy* (studia II stopnia) efekty uczenia się przypisane do tych przedmiotów odnoszą się na przykład do znajomości w pogłębionym stopniu teorii i metod z zakresu zapewniania bezpieczeństwa systemów Internetu Rzeczy czy identyfikowania i formułowania specyfikacji złożonych zadań dotyczących cyberbezpieczeństwa, a w szczególności zapewniania bezpieczeństwa sieci bezprzewodowych najnowszych generacji i systemów Internetu Rzeczy. Natomiast dla przedmiotu *bezpieczeństwa społecznego, organizacyjnego i zarządzanie cyberbezpieczeństwem* (studia I stopnia) przypisano np. wiedzę w zakresie cyberbezpieczeństwa, obejmującą m.in. następujące zagadnienia: „bezpieczeństwo danych, bezpieczeństwo systemów i oprogramowania, ... bezpieczeństwo organizacyjne, społeczne i zarządzanie cyberbezpieczeństwem tworzącą podstawy do projektowania rozwiązań związanych z zapewnieniem bezpieczeństwa systemów informacyjnych i sieci teleinformatycznych” czy „potrafi dokonać krytycznej analizy i oceny istniejących rozwiązań w zakresie cyberbezpieczeństwa”. Znajduje to odzwierciedlenie również w pozostałych efektach uczenia się przyporządkowanych na przykład do przedmiotów skojarzonych z obszarem badawczym np.



*bezpieczeństwo sieci* do którego przyporządkowano przedmioty *bezpieczeństwo komunikacji* (studia I stopnia efekt uczenia się „potrafi – przy identyfikowaniu problemów i formułowaniu specyfikacji zadań inżynierskich oraz problemów badawczych związanych z zapewnieniem cyberbezpieczeństwa oraz rozwiązywaniu tych zadań...”), *bezpieczeństwo sieci 5G i 6G* (studia II stopnia efekty uczenia się „potrafi planować i przeprowadzać eksperymenty / badania, w tym symulacje komputerowe dotyczące bezpieczeństwa systemów teleinformatycznych, oraz interpretować uzyskane wyniki”) , *bezpieczeństwo Internetu Rzeczy* (studia II stopnia „potrafi formułować i testować hipotezy związane z prostymi problemami badawczymi dotyczącymi m.in. zapewnienia bezpieczeństwa systemów teleinformatycznych”). Na tej podstawie można przyjąć, że efekty uczenia się kierunkowe oraz dla zajęć lub grup zajęć dla studiów I i II stopnia są specyficzne dla ocenianego kierunku i są zgodne z aktualnym stanem wiedzy w dyscyplinie informatyka techniczna i telekomunikacja.

Efekty uczenia się uwzględniają w szczególności umiejętności związane z przygotowaniem do prowadzenia działalności naukowej (np.: na studiach I stopnia efekty uczenia się „potrafi – przy identyfikowaniu problemów i formułowaniu specyfikacji zadań inżynierskich oraz problemów badawczych, w tym zadań i problemów złożonych i nietypowych, związanych z zapewnieniem cyberbezpieczeństwa oraz ich rozwiązywaniu...”; na studiach II stopnia „potrafi planować i przeprowadzać eksperymenty/badania, w tym symulacje komputerowe dotyczące bezpieczeństwa systemów...”, „potrafi wykorzystać zaawansowane narzędzia informatyczne niezbędne do przeprowadzenia eksperymentów/badań związanych z zagadnieniami cyberbezpieczeństwa...”, „potrafi formułować i testować hipotezy...”), komunikowania się w języku obcym (na studiach I stopnia B2: „posługuje się językiem angielskim w stopniu wystarczającym do porozumiewania się (poziom B2), a także czytania ze zrozumieniem dokumentacji i instrukcji obsługi narzędzi informatycznych, urządzeń sieciowych oraz podobnych dokumentów”; na studiach drugiego stopnia B2+: „potrafi posługiwać się językiem angielskim na poziomie B2+ Europejskiego Systemu Opisu Kształcenia Językowego”) i kompetencje społeczne niezbędne w działalności zawodowej i naukowej właściwej dla kierunku cyberbezpieczeństwo (np. na studiach I stopnia „potrafi myśleć i działać w sposób przedsiębiorczy”; na studiach II stopnia „jest gotów do wypełniania zobowiązań społecznych, inspirowania i organizowania działalności na rzecz... a zwłaszcza formułowania i przekazywania społeczeństwu... informacji i opinii dotyczących zagrożeń związanych z cyberbezpieczeństwem i sposobów przeciwdziałania tym zagrożeniom...”).

Kluczowe kompetencje inżynierskie zdefiniowane w ramach efektów uczenia się dla studiów I i II stopnia kierunku cyberbezpieczeństwo związane są z typowymi oczekiwaniami i zapotrzebowaniem na rynku pracy, między innymi takimi jak: umiejętność zarządzania danymi i ich przetwarzania (np. „potrafi dokonać identyfikacji i sformułować specyfikację złożonych zadań dotyczących cyberbezpieczeństwa, a w szczególności: analizy danych w kontekście jej zastosowań w rozwiązywaniu problemów związanych z zapewnieniem bezpieczeństwa systemów teleinformatycznych...” - studia II stopnia; „potrafi wykorzystać informacje pochodzące z różnych źródeł do identyfikowania i analizy podatności i zagrożeń dla bezpieczeństwa danych, oprogramowania, poszczególnych komponentów” - studia I stopnia), znajomość paradygmatów i technik programowania (np. studia I stopnia „potrafi – zgodnie z zadaną specyfikacją – zaprojektować, zrealizować... fragment infrastruktury (sprzęt i oprogramowanie) służącej zapewnieniu bezpieczeństwa systemu informacyjnego lub sieci teleinformatycznej, używając właściwie dobranych metod i narzędzi”), umiejętność modelowania oraz symulacji obiektów i systemów (np. studia II stopnia „potrafi... wykorzystywać metody analityczne, symulacyjne i eksperymentalne... oraz zastosować właściwe metody, techniki i narzędzia, w tym

zaawansowane techniki...”), znajomość technik z zakresu inteligencji obliczeniowej, umiejętność prototypowania, programowania i konfigurowania systemów komputerowych, umiejętność analizowania i oceniania bezpieczeństwa systemów informatycznych i sieci komputerowych (np.: studia I stopnia „potrafi – zgodnie z zadaną specyfikacją – zaprojektować... przetestować i ocenić – ze względu na właściwie dobrany zestaw kryteriów... fragment infrastruktury (sprzęt i oprogramowanie) służącej zapewnieniu bezpieczeństwa systemu informacyjnego lub sieci teleinformatycznej, używając właściwie dobranych metod i narzędzi”, studia II stopnia „potrafi formułować i testować hipotezy związane z prostymi problemami badawczymi dotyczącymi m.in. zapewnienia bezpieczeństwa systemów teleinformatycznych”). Efekty uczenia się przyjęte dla ocenianego kierunku, w przypadku studiów pierwszego i drugiego stopnia, uwzględniają pełny zakres efektów uczenia się dla studiów o profilu ogólnoakademickim, prowadzących do uzyskania kompetencji inżynierskich.

Ww. analiza pozwala na stwierdzenie, że efekty uczenia się przyjęte na I i II stopnia studiów na kierunku cyberbezpieczeństwo są zgodne z wymaganiami wskazanymi dla ogólnoakademickiego profilu studiów.

Analiza programów kształcenia i wyżej wskazane zestawienie pozwala sformułować wniosek, że zarówno efekty uczenia się przyjęte dla I jak również II stopnia studiów kierunku cyberbezpieczeństwo są zgodne z prowadzonymi na Wydziale badaniami naukowymi w dyscyplinie informatyka techniczna i telekomunikacja. Określone efekty uczenia się są uszczegółowione efektami wskazanymi dla zajęć i wskazują na konkretny zakres wiedzy, umiejętności czy kompetencji społecznych. Na przykład efekt uczenia się wskazany dla studiów I stopnia – W07, który określono jako „wiedzę w zakresie cyberbezpieczeństwa, obejmującą m.in. następujące zagadnienia: bezpieczeństwo danych, bezpieczeństwo systemów i oprogramowania, bezpieczeństwo komunikacji, kryminalistyka cyfrowa, bezpieczeństwo organizacyjne, społeczne i zarządzanie cyberbezpieczeństwem, tworzącą podstawy do projektowania rozwiązań związanych z zapewnieniem bezpieczeństwa systemów informacyjnych i sieci teleinformatycznych” jest uszczegółowiony „ma wiedzę o protokołach kryptograficznych” (przedmiot *bezpieczeństwo danych*) czy „ma wiedzę z zakresu mechanizmów stosowanych w złośliwym oprogramowaniu dotyczących bezpieczeństwa systemu” (przedmiot *bezpieczeństwo systemów i oprogramowania*). Efekty uczenia się są sformułowane w sposób zrozumiały, co przedstawiono powyżej, są możliwe do osiągnięcia i pozwalają na stworzenie systemu ich weryfikacji.

**Zalecenia dotyczące kryterium 1 wymienione w uchwale Prezydium PKA w sprawie oceny programowej na kierunku studiów, która poprzedziła bieżącą ocenę (jeśli dotyczy)**

| Lp. | Zalecenia dotyczące kryterium 1 wymienione we wskazanej wyżej uchwale Prezydium PKA | Opis realizacji zalecenia | Ocena realizacji zalecenia<br>(zalecenie zrealizowane /<br>zalecenie niezrealizowane) |
|-----|-------------------------------------------------------------------------------------|---------------------------|---------------------------------------------------------------------------------------|
| 1.  | <b>Nie dotyczy</b>                                                                  | <b>Nie dotyczy</b>        | <b>Nie dotyczy</b>                                                                    |

**Propozycja oceny stopnia spełnienia kryterium 1**

Kryterium spełnione

## Uzasadnienie

Koncepcja i cele kształcenia na kierunku cyberbezpieczeństwo studia I i II stopnia są zgodne ze strategią Uczelni oraz polityką jakości, a także mieszczą się w dyscyplinie informatyka techniczna i telekomunikacja, do której oceniany kierunek studiów jest przyporządkowany. Koncepcja i cele kształcenia są związane z prowadzoną w Uczelni działalnością naukową w wymienionej wyżej dyscyplinie. Koncepcja i cele kształcenia zostały określone we współpracy z interesariuszami wewnętrznymi (nauczyciele akademicy i studenci), a także interesariuszami zewnętrznymi (otoczenie społeczno-gospodarcze, przedstawiciele firm i instytucji), przez co są one (koncepcja, cele) zorientowane na potrzeby otoczenia społeczno-gospodarczego, w tym w szczególności rynku pracy w obszarze związanym z cyberbezpieczeństwem. Efekty uczenia się określone dla studiów I i II stopnia są zgodne z koncepcją i celami kształcenia oraz profilem ogólnoakademickim, w części zgodne z odpowiednio 6 i 7 poziomem Polskiej Ramy Kwalifikacji. Wątpliwości budzi określenie stopnia zaawansowania i głębi zdobywanej wiedzy i osiągniętych umiejętności. Efekty uczenia się są zgodne z aktualnym stanem wiedzy, jak również z prowadzoną w Uczelni i na Wydziale działalnością naukową w ramach dyscypliny informatyka techniczna i telekomunikacja. Uwzględniają one (efekty) kompetencje badawcze, komunikowanie się w języku obcym na poziomie B2/B2+ Europejskiego Systemu Opisu Kształcenia Językowego, a także kompetencje społeczne niezbędne w działalności naukowej i funkcjonowaniu na współczesnym rynku pracy. Kierunkowe efekty uczenia się obejmują pełny zakres efektów prowadzących do uzyskania kompetencji inżynierskich. Określone dla ocenianego kierunku efekty uczenia się są możliwe do osiągnięcia i sformułowane w sposób zrozumiały, pozwalający na stworzenie systemu ich weryfikacji.

## Dobre praktyki, w tym mogące stanowić podstawę przyznania uczelni Certyfikatu Doskonałości Kształcenia

---

## Rekomendacje

1. Rekomenduje się dokonanie przeglądu kierunkowych efektów uczenia się oraz efektów przedmiotowych i takie ich przeformułowanie, aby nie wzbudzały wątpliwości w zakresie zaawansowania i głębi wiedzy zdobywanej i umiejętności osiągniętych na kierunku cyberbezpieczeństwo studia I i II stopnia.

## Zalecenia

---

**Kryterium 2. Realizacja programu studiów: treści programowe, harmonogram realizacji programu studiów oraz formy i organizacja zajęć, metody kształcenia, praktyki zawodowe, organizacja procesu nauczania i uczenia się**

## Analiza stanu faktycznego i ocena spełnienia kryterium 2

Treści programowe przedstawione w kartach przedmiotów studiów I stopnia odnoszą się do dyscypliny naukowej informatyka techniczna i telekomunikacja. Program kształcenia nie przewiduje realizacji



specjalności Są one zgodne z aktualnym stanem wiedzy i metodyki badań w tej dyscyplinie. Absolwent studiów I stopnia na kierunku cyberbezpieczeństwo posiada wiedzę i umiejętności, m.in. z zakresu matematyki, informatyki, telekomunikacji i elektroniki, które są niezbędne do kształtowania specjalistycznych kompetencji w zakresie cyberbezpieczeństwa oraz które umożliwiają rozwój i uzupełnianie tych kompetencji wraz z postępem technologicznym oraz zmianami zachodzącymi w sferze społeczno-gospodarczej. Absolwent wykorzystuje wiedzę i umiejętności do formułowania i rozwiązywania problemów związanych z zapewnieniem bezpiecznego działania systemów komputerowych i sieci teleinformatycznych w obliczu różnorodnych zagrożeń. Jak np. identyfikowanie i analizowanie zagrożeń dla bezpieczeństwa danych, systemów informacyjnych i sieci teleinformatycznych, w oparciu o informacje pochodzące z wielu źródeł.

Absolwenci studiów II stopnia na kierunku cyberbezpieczeństwo posiadają zaawansowaną wiedzę w zakresie cyberbezpieczeństwa, znają kluczowe procesy zachodzące w systemach teleinformatycznych, które są niezbędne do zapewnienia ich bezpiecznego funkcjonowania. Dotyczy to w szczególności bezpieczeństwa: rozwiązań sprzętowych oraz komunikacji opartej na najnowszych standardach sieci bezprzewodowych. Wykorzystując tę wiedzę, potrafią identyfikować i formułować specyfikacje złożonych zadań, między innymi w zakresie: analizy danych w kontekście rozwiązywania problemów związanych z bezpieczeństwem systemów teleinformatycznych i zapewniania bezpieczeństwa sieci bezprzewodowych najnowszych generacji oraz systemów Internetu Rzeczy (IoT). Ponadto, absolwenci potrafią projektować innowacyjne rozwiązania dobierając właściwe metody i narzędzia oraz weryfikować poprawności zaproponowanych rozwiązań. Absolwenci formułują i testują hipotezy związane z problemami badawczymi dotyczącymi bezpieczeństwa systemów teleinformatycznych. Treści programowe są zgodne z efektami uczenia się określonymi dla poszczególnych zajęć, a także uwzględniają najnowszą wiedzę z zakresu dyscypliny, do której odnoszą się efekty uczenia się.

Dla przykładu:

- treści w ramach przedmiotu *kryminalistyka cyfrowa*, który realizowany jest na studiach I stopnia składają się między innymi: metody cyfrowej kryminalistyki śledczej w zakresie systemów sprzętowo-programowych (pozyskiwanie danych cyfrowych z urządzeń, pamięci i systemów plików na potrzeby ustanowienia dowodów cyfrowych; metody cyfrowej kryminalistyki śledczej w zakresie strumieni komunikacji (pozyskiwanie danych z sieci przewodowych i bezprzewodowych, analiza i interpretacja danych sieciowych); metody analizy złośliwego oprogramowania statycznej i dynamicznej (analiza próbek, odkrywanie wektorów ataku i zastosowanych technik wykorzystania dziur w systemach); zarządzanie incydentami naruszenia bezpieczeństwa komputerowego, co pozwala na osiągnięcie efektu uczenia się „potrafi ocenić możliwości funkcjonowania systemu lub sieci w warunkach wystąpienia zagrożeń; potrafi przewidzieć skutki... ataków stwarzających zagrożenie dla bezpieczeństwa systemów informacyjnych i sieci teleinformatycznych oraz zaproponować działania minimalizujące te skutki” oraz efektów przypisanych do przedmiotu – potrafi modelować zagrożenia z wykorzystaniem standardowych metody oraz potrafi stosować metody analityczne do pozyskanego cyfrowego materiału dowodowego,
- treści w ramach przedmiotu *techniki i technologie Big Data* realizowanego na II stopniu studiów treści programowe obejmują Apache Spark (konceptcja, zastosowanie Resilient Distributed Datasets i DataFrame, architektura Spark – cluster manager, executor, przetwarzanie z systemem rozproszonego przechowywania i przetwarzania plików Hadoop MapReduce – treści pozwalają na osiągnięcie efektu uczenia się „w pogłębionym stopniu zna i rozumie wybrane fakty, teorie i

metody, stanowiące zaawansowaną wiedzę z zakresu analizy danych w kontekście jej zastosowań w rozwiązywaniu problemów dotyczących cyberbezpieczeństwa” oraz efektu zna koncepcję przetwarzania w Apache Spark, w tym stosowane struktury danych RDD, dataframe.

Ponadto treści programowe, a w szczególności te powiązane z zajęciami praktycznymi takimi jak ćwiczenia laboratoryjne oraz projekty, uwzględniają współczesne rozwiązania stosowane w środowisku pracy inżyniera. Przykładem mogą być przedmioty: *systemy komputerowe: architektura i programowanie, sieci mobilne i sieci internetu rzeczy* - w odniesieniu do studiów I stopnia czy *bezpieczne systemy cyfrowe oraz analiza danych w cyberbezpieczeństwie* - w odniesieniu do studiów II stopnia. Wykorzystuje się w nich właściwe dla zadań inżynierskich aspekty rozwiązywania problemów. W związku z powyższym można stwierdzić, że treści programowe są kompleksowe i specyficzne dla zajęć tworzących program studiów i zapewniają uzyskanie wszystkich efektów uczenia się. Na kierunku cyberbezpieczeństwo wprowadza się aspekty kształcenia problemowego opartego na koncepcji Problem Based Learning, realizowane są projekty zespołowe, a studenci mają możliwość udziału w rozwiązywaniu problemów badawczych.

Czas trwania studiów I stopnia na ocenianym kierunku wynosi 7 semestrów (3,5 roku). Nakład pracy mierzony łączną liczbą punktów ECTS konieczny do ukończenia studiów wynosi 210 punktów ECTS. Czas trwania studiów II stopnia na kierunku *cyberbezpieczeństwo* wynosi 3 semestry (1,5 roku). Nakład pracy mierzony łączną liczbą punktów ECTS konieczny do ukończenia studiów wynosi 90 punktów ECTS. Wskazane wartości spełniają wymagania ustawowe. Punkty ECTS są przydzielane razem dla wszystkich form danych zajęć. Nakłady pracy, mierzone liczbą punktów ECTS, niezbędne do osiągnięcia efektów uczenia się przypisanych do zajęć są poprawnie oszacowane i zapewniają osiągnięcie przez studentów efektów uczenia się. Z analizy programu kształcenia wynika, że liczba punktów ECTS z bezpośrednim udziałem nauczyciela akademickiego zależy ściśle od zakresu działań studenta na zajęciach i samodzielnej jego pracy, a w wyznaczaniu liczby punktów ECTS wykorzystywana jest formuła, w której uwzględnia się liczbę godzin kontaktowych, łączny nakład pracy studenta oraz liczbę punktów ECTS przypisaną do przedmiotu.

Program kształcenia oraz karty przedmiotów wskazują, że nakład pracy studenta wyrażony w godzinach realizacji zajęć wynosi dla I stopnia 2709 (Uchwała Rady Wydziału Elektroniki i Technik Informatycznych Nr 17/2019 z dnia 29 stycznia 2019 w sprawie wniosku o utworzenie studiów stacjonarnych pierwszego stopnia o profilu ogólnoakademickim na kierunku *cyberbezpieczeństwo* i uchwalenia programu tych studiów. Liczby godzin zajęć wymagających bezpośredniego udziału nauczycieli akademickich i studentów określone w programie studiów dla poszczególnych zajęć zapewniają osiągnięcie przez studentów efektów uczenia się. Łączna liczba punktów ECTS jaką student musi uzyskać w ramach zajęć prowadzonych z bezpośrednim udziałem nauczycieli akademickich wg przyjętych regulacji na studiach I stopnia wynosi 108 punktów ECTS (50,5%) i wartość ta jest zgodna z Ustawą i jest większa od 50% całkowitej liczby punktów ECTS niezbędnych do ukończenia studiów oraz zapewnia osiągnięcie przez studentów wszystkich zakładanych efektów uczenia się.

Wskazana w załączniku do Uchwały Nr 218/L/2022 Senatu Politechniki Warszawskiej z dnia 25 maja 2022 r. łączna liczba godzin zajęć dla studiów II stopnia wynosi 900 godzin (nie wliczając zajęć indywidualnych - badań i realizacji pracy dyplomowej). Liczby godzin zajęć wymagających bezpośredniego udziału nauczycieli akademickich i studentów określone w programie studiów dla poszczególnych zajęć zapewniają osiągnięcie przez studentów efektów uczenia się. W ww. załączniku wskazano, że dla studiów II stopnia w ramach zajęć prowadzonych łączna liczba punktów ECTS, jaką

student musi uzyskać w ramach zajęć prowadzonych z bezpośrednim udziałem nauczycieli wynosi 46 punktów ECTS (51,1%). Jednak nie we wszystkich kartach przedmiotów objętych programem studiów na II stopniu kierunku *cyberbezpieczeństwo* (w sekcji opisu przedmiotu) formułuje się w sposób czytelny i jednoznaczny wskazanie „liczby punktów ECTS na zajęciach wymagających bezpośredniego udziału nauczycieli akademickich”. Na przykład w odniesieniu do cyklu przedmiotów związanych z prowadzeniem badań i przygotowaniem pracy dyplomowej brak jest ww. wskazania dla przedmiotów *pracownia dyplomowa* czy *pracownia projektowa*. W związku z powyższym rekomenduje się przegląd programu studiów kierunku cyberbezpieczeństwo II stopnia i kart przedmiotów objętych tym programem oraz ich aktualizację, tak aby liczba godzin realizowanych z bezpośrednim udziałem nauczycieli akademickich i przyporządkowana im liczba punktów ECTS była wskazana we wszystkich kartach przedmiotów. Poprawność wyodrębnienia modułów zajęć w ramach harmonogramu realizacji programu studiów jest prawidłowa. Poszczególne moduły są zwarte tematycznie i jednocześnie zawierają obszary wiedzy z zakresu informatyki technicznej i telekomunikacji. Dla studiów I stopnia zajęcia pogrupowano w moduły: wychowanie fizyczne (semestr 1,2,3), języki obce (semestr 2,3,4), przedmioty ekonomiczno-społeczne (semestr 1,5), podstawy projektowania (semestr 1), matematyka (semestr 1,2,3), fizyka (semestr 2,3), podstawy elektroniki i telekomunikacji (semestr 3,4), informatyka techniczna (semestr 1-5), teleinformatyka (semestr 2-6), cyberbezpieczeństwo (semestr 1-7), przedmioty obieralne techniczne (semestr 7), dyplomowanie (semestr 6,7), praktyka. W odniesieniu do studiów II stopnia kierunek cyberbezpieczeństwo wskazano moduły: przedmioty humanistyczno-społeczne (semestr 1,2), podstawy teoretyczne cyberbezpieczeństwa (semestr 1), cyberbezpieczeństwo – moduły PBL (semestr 1,2), cyberbezpieczeństwo (semestr 1-3), przedmioty obieralne cyberbezpieczeństwo/teleinformatyka (semestr 1,2), przedmioty obieralne techniczne (semestr 3), prowadzenie badań i dyplomowanie (semestr 1-3). Analiza kart przedmiotów przypisanych do wskazanych wyżej modułów pozwala stwierdzić, że sekwencja zajęć jest prawidłowa i pozwala na osiągnięcie przez studentów efektów uczenia się. Na uwagę zasługuje wprowadzony w pierwszym semestrze studiów pierwszego stopnia układ przedmiotów: *wprowadzenie do cyberbezpieczeństwa* (pierwsze, proste projekty związane z obszarem cyberbezpieczeństwa), *pozatechniczne aspekty pracy inżyniera* (efektywne pozyskiwanie wiedzy, rozwiązywanie problemów, analiza studium przypadku, społeczne, ekonomiczne i inne pozatechniczne uwarunkowania działalności zawodowej inżyniera), *podstawy techniki cyfrowej* (proste systemy cyfrowe), *szybkie prototypowanie inżynierskie* (indywidualnie/w zespołach konstruowania mini-robotów). Taka sekwencja przedmiotów wzmacnia aspekty problemowego podejścia do zadań inżynierskich i pracy (również) zespołowej wprowadzając już na pierwszym semestrze projekty o charakterze implementacyjnym.

Analiza kart przedmiotów pozwala stwierdzić, że zajęcia w podziale na formy zajęć dla ocenianego kierunku cyberbezpieczeństwo I i II stopnia są realizowane w sposób zróżnicowany (wykład, laboratorium, ćwiczenia, projekt). Liczby godzin zajęć w podziale na procentowy udział tych form zajęć dla ocenianego kierunku studiów I i II stopnia wynoszą:

- wykłady 31% (I stopień studiów)/29% (II stopień studiów),
- ćwiczenia 18% (I stopień studiów)/8% (II stopień studiów),
- laboratoria 18% (I stopień studiów)/4% (II stopień studiów),
- projekty i seminaria 33% (I stopień studiów)/59% (II stopień studiów).

Zwrócić należy uwagę na prawidłowy dobór proporcji form zajęć praktycznych, w szczególności zajęć projektowych, które umożliwiają studentom uczestnictwo w badaniach lub ich prowadzenie.

W związku z powyższym, proporcje liczby godzin zajęć realizowanych w poszczególnych formach zapewniają osiągnięcie przez studentów efektów uczenia się.

Studenci kierunku cyberbezpieczeństwo na I i II poziomie realizują kształcenie wg jednolitego programu, tj. bez wyboru specjalności. Oferta przedmiotów obieralnych, możliwość wyboru tematyki pracy dyplomowej oraz wybór miejsca realizacji praktyki (studia I stopnia) pozwalają studentom na komponowanie ścieżki kształcenia wg preferencji w odniesieniu do zakresu cyberbezpieczeństwa, jak na przykład: bezpieczeństwo danych, bezpieczeństwo sprzętowych komponentów systemów komputerowych i sieci teleinformatycznych, czy zarządzanie cyberbezpieczeństwem. Program studiów na ocenianym kierunku umożliwia wybór zajęć w wymiarze 74 punktów ECTS (35%) na studiach I stopnia i 40 punktów ECTS (44,4%) na studiach II stopnia, co pozostaje w zgodzie z przyjętymi regulacjami.

Program studiów na kierunku cyberbezpieczeństwo obejmuje również zajęcia oraz grupy zajęć związane z prowadzoną na uczelni działalnością naukową w dyscyplinie informatyka techniczna i telekomunikacja. Łączna liczba punktów ECTS przyporządkowana zajęciom związanym z prowadzoną w uczelni działalnością naukową w dyscyplinie informatyka techniczna i telekomunikacja, do której przyporządkowany jest kierunek studiów - wynosi 135 punktów ECTS dla studiów I stopnia i 71 punktów ECTS dla studiów II stopnia. Do zajęć, które korespondują z działalnością naukową z zakresu ww. dyscypliny można zaliczyć na przykład:

- obszar badawczy bezpieczeństwo sieci – przedmioty: *bezpieczeństwo komunikacji* (studia I stopnia), *bezpieczeństwo sieci 5G i 6G* (studia II stopnia), *bezpieczeństwo Internetu Rzeczy* (studia II stopnia),
- obszar badawczy bezpieczeństwo oprogramowania – przedmiot: *bezpieczeństwo systemów i oprogramowania* (studia II stopnia),
- obszar badawczy bezpieczeństwo danych – przedmioty: *bezpieczeństwo danych* (studia I stopnia).

Analiza kart przedmiotu i programu kształcenia pozwala sformułować wniosek, że zajęciom powiązanym z prowadzoną w Uczelni działalnością naukową w dyscyplinie informatyka techniczna i telekomunikacja, przypisanych zostało 136 punktów ECTS (64,76%) studia I stopnia i 65 punktów ECTS (72,2%) studia II stopnia.

Program studiów obejmuje zajęcia przeznaczone na kształcenie w zakresie znajomości co najmniej jednego języka obcego. Na kierunku cyberbezpieczeństwo studia I stopnia realizowane jest kształcenie w ramach modułu język obcy w wymiarze 12 punktów ECTS realizowane przez trzy semestry (60 godzin/4 punkty ECTS za każdy semestr), w odniesieniu do studiów II stopnia przedmioty prowadzone w języku angielskim to: *pattern recognition* (30 godz. 2 punkty ECTS), *non-technical dimensions of cybersecurity* (60 godz. 4 punkty ECTS), *methodological and ethical issues of technoscientific research* (30 godz. 2 punkty ECTS).

Zajęcia z dziedziny nauk humanistycznych lub społecznych zostały uwzględnione do realizacji na kierunku cyberbezpieczeństwo. Na ocenianym kierunku dla studiów I stopnia wprowadzono blok przedmioty ekonomiczno-społeczne, w którym oferuje się dwa przedmioty obowiązkowe i jeden w formie obieralnej (poza techniczne *aspekty pracy inżyniera, przedsiębiorczość w praktyce*, odpowiednio 3,2 punkty ECTS oraz obieralny przedmiot z grupy przedmioty ekonomiczno-społeczne, np. *filozofia informacji i techniki*). Na studiach II stopnia przewiduje się do realizacji zajęcia w ramach bloku przedmioty humanistyczno-społeczne, w ramach którego realizowane są dwa przedmioty

(*przedsiębiorczość startupowa* 3 punkty ECTS, *cyberprzestępczość - wyzwania prawne* 2 punkty ECTS). Powyższe pozwala postawić wniosek, że wymiar punktów ECTS za zajęcia z dziedziny nauk humanistycznych lub społecznych (minimum 5 punktów ECTS) jest zgodny z wymogiem ustawowym.

Na kierunku cyberbezpieczeństwo studia I i II stopnia nie są prowadzone zajęcia z wykorzystaniem metod i technik kształcenia na odległość.

Metody kształcenia wykorzystywane w programie studiów kierunku cyberbezpieczeństwo są różnorodne, zaliczają się do nich na przykład:

- oparte na słowie – stanowiące dla studentów główne źródło wiedzy oparte na wykładzie, na którym omawiane są zagadnienia teoretyczne, dokonywana jest klasyfikacja czy prezentowane są metody badawcze oraz zajęciach seminaryjnych na których głównym elementem jest zaangażowanie studenta poprzez przygotowanie opracowania na zadany temat i jego przedstawienie oraz udział w dyskusji,
- oglądowe – gdzie wiedza przekazywana jest w formie pokazu na wykładzie lub obserwacji na ćwiczeniach audytoryjnych i na zajęciach laboratoryjnych przy aktywnym zaangażowaniu studentów,
- praktyczne – gdzie źródłem wiedzy i umiejętności są dla studentów zajęcia praktyczne związane z instruktażem ze strony nauczycieli akademickich (ćwiczenia, ćwiczenia laboratoryjne), w tym zajęcia projektowe i zajęcia laboratoryjne, które realizowane indywidualnie oraz w zespołach, szybkie prototypowanie,
- problemowe - bazujące na samodzielnym rozwiązywaniu, problemów np. projekty pozwalające na praktycznym zastosowaniu wiedzy, praca projektowa z wykorzystaniem metodyki Design Thinking, w tym zajęcia projektowe, które realizowane indywidualnie oraz w zespołach.

Ww. metody kształcenia korelują ze specyfiką zajęć. Na przykład realizacja zadań projektowych zazwyczaj obejmuje etapy: sformułowanie problemu, dobór metod i narzędzi, przeprowadzenie badań/rozwiązanie problemu i wykonanie implementacji oraz opracowanie wyników i ich prezentacja. Zajęcia zintegrowane wprowadzone do programu kierunku cyberbezpieczeństwo studia II stopnia np. *analiza danych w cyberbezpieczeństwie*, *bezpieczeństwo Internetu Rzeczy*, w ramach których stosuje się metodę PBL (project-based learning) to przykład wdrożenia najnowszych osiągnięć dydaktyki akademickiej.

Metody kształcenia, które stosowane są w realizacji programu kształcenia można uznać za stymulujące do samodzielności i pełnienia aktywnej roli w procesie uczenia się. Program kształcenia jest tak skomponowany, że metody kształcenia, które przygotowują do rozwiązywania problemów, przygotowania i prowadzenia pracy badawczej wprowadzane są od pierwszych semestrów (np. projekty w przedmiotach *szybkie prototypowanie inżynierskie* studia I stopnia 1 semestr, *metody matematyczne w cyberbezpieczeństwie* studia II stopnia 1 semestr). Aktywności podejmowane w zakresie realizacji zajęć przypisanych do dyplomowania przygotowują i prowadzą do uczestnictwa studentów w działalności naukowej

W związku z powyższym uznaje się, że metody te są specyficzne, różnorodne i zapewniają osiągnięcie zakładanych efektów uczenia się.



Uchwała Senatu Politechniki Warszawskiej Nr 58/L/2020 z dnia 25 listopada 2020 r. w sprawie ustalania studiów na w Politechnice Warszawskiej, reguluje wymagania w tym zakresie wskazując, że na I stopniu studiów prowadzonych w języku polskim studenci zobowiązani są zdać egzamin z języka obcego na poziomie B2. W odniesieniu do zaleceń dla II stopnia studiów wskazano, że zalecenie zaliczenia co najmniej jednego przedmiotu prowadzonego w języku obcym na poziomie B2+ (język obcy z elementami języka specjalistycznego). Na zajęciach w ramach języka obcego (studia I stopnia) i przedmiotach realizowanych w języku obcym (studia II stopnia) wykorzystywane są różne, właściwe metody kształcenia (np. prezentacja, dyskusja, przygotowanie raportu), należy zwrócić uwagę, że dyskusja pełni również rolę aktywizującą. Metody te umożliwiają nabycie kompetencji w zakresie opanowania języka obcego co najmniej na poziomie B2+ (studia II stopnia) i B2 (studia I stopnia).

Metody kształcenia umożliwiają dostosowanie procesu uczenia się do zróżnicowanych potrzeb grupowych i indywidualnych studentów głównie poprzez metody oparte na działaniu praktycznym np. nauki pracy w grupie w ramach zajęć projektowych, realizacji projektów zespołowych, wyboru typu i tematyki pracy dyplomowej. Studenci mogą dostosowywać tempo studiowania poprzez wybór indywidualnej ścieżki kształcenia (wybór przedmiotów obieralnych i metod kształcenia stosowanych w wybranych zajęciach). Metody kształcenia mogą być także dostosowywane do potrzeb indywidualnych studenta np. studentów z niepełnosprawnością czy wybitnie uzdolnionych studentów poprzez samodzielne dochodzenie do wiedzy z wykorzystaniem zindywidualizowanych metod projektowych i problemowych

W jednostce na ocenianym kierunku stosuje się zapisy Regulaminu Studiów Politechniki Warszawskiej w odniesieniu do studentów z niepełnosprawnością. Metody kształcenia mogą być także dostosowywane do potrzeb indywidualnych studenta np. studentów z niepełnosprawnością czy wybitnie uzdolnionych studentów poprzez samodzielne dochodzenie do wiedzy z wykorzystaniem zindywidualizowanych metod projektowych i problemowych. Biuro ds. Społecznej Odpowiedzialności Uczelni, Sekcja ds. Osób z Niepełnosprawnościami ściśle współpracuje w wydziałach w celu dostosowania np. warunków zdawania egzaminów.

Metody i techniki kształcenia na odległość, w przypadku zajęć kształtujących umiejętności praktyczne nie są stosowane. Na zajęciach na kierunku cyberbezpieczeństwo nie prowadzi się kształcenia z wykorzystaniem metod i technik kształcenia na odległość. Jednakże Uczelnia zapewnia dostęp do narzędzi informatycznych, które wspomagają zdobywanie wiedzy przez studenta: platforma MS Teams oraz platforma LeOn. Wykorzystywane są one przez nauczycieli akademickich do umieszczania w ich zasobach dodatkowych materiałów, dydaktycznych lub do konsultacji.

Organizację praktyk studenckich reguluje Regulamin organizacji i finansowania obowiązkowych praktyk studenckich objętych programem studiów I i II stopnia, jednolitych studiów magisterskich, stacjonarnych i niestacjonarnych, wprowadzony Zarządzeniem nr 45 /2021 Rektora Politechniki Warszawskiej z dnia 21 maja 2021 r.

Praktyki realizowane są w wymiarze 4 tygodni 160 godzin (4 punkty ECTS).

Efekty uczenia się zakładane dla praktyk są zgodne z efektami uczenia się przypisanymi do pozostałych zajęć lub grup zajęć

Zgodnie z Regulaminem, student może zrealizować praktykę zarówno w podmiocie otoczenia społeczno-gospodarczego (z którym podpisano stosowne porozumienie) jak i w jednej z jednostek organizacyjnych Politechniki Warszawskiej. Podstawą do skierowania na praktykę jest



ustandaryzowane w treści trójstronne „Porozumienie o organizacji obowiązkowych praktyk studenckich”, którego stronami są Wydział, Podmiot przyjmujący na praktykę oraz student kierowany na tę praktykę. Na stronach internetowych Wydziału dostępna jest lista podmiotów, stanowiących podstawową grupę firm przyjmujących na praktyki. Student ma także możliwość odbycia praktyki w podmiocie wskazanym przez siebie. Podstawę stanowi w takiej sytuacji podpisane porozumienie oraz uzyskane od wydziałowego opiekuna praktyk - „Skierowanie na praktykę”. Tak przyjęta forma weryfikacji podmiotu przyjmującego na praktykę oraz forma zawartych umów, umożliwiają realizację praktyk w miejscu, które zarówno pod względem infrastruktury jak i realizowanych prac, daje możliwość realizacji celów programu praktyki kierunkowej.

Zaliczenie praktyki odbywa się na podstawie przedstawionego przez studenta zestawu dokumentów: Podania o zaliczenie praktyki studenckiej, Porozumienie o organizacji obowiązkowych praktyk studenckich, zaświadczenia o odbyciu praktyki – wypełnianego przez podmiot przyjmujący oraz (sporządzonego przez studenta) raportu z odbytej praktyki. Formaty wszystkich tych dokumentów ustandaryzowano, a ich wzorce dostępne są na stronie internetowej Wydziału.

Żaden z przedstawionych dokumentów, podpisywanych z pracodawcą, a także dostarczanych w ramach realizacji praktyki nie definiuje jednoznacznie oczekiwania uczelni wobec podmiotu przyjmującego na praktykę, w zakresie planowanych efektów uczenia się, jakie student uzyskuje w trakcie praktyki. Zespół oceniający rekomenduje wprowadzenie do treści umów, podpisywanych z przyjmującym na praktykę, literalnie zapisanych oczekiwań w zakresie realizowanych efektów uczenia się dla studenta. Pomimo powyższej uwagi, przyjęte metody weryfikacji i oceny osiągnięcia przez studentów efektów uczenia się zakładanych dla praktyk, a także sposób dokumentowania przebiegu praktyk i realizowanych w ich trakcie zadań są trafnie dobrane i umożliwiają skuteczne sprawdzenie i ocenę stopnia osiągnięcia efektów uczenia się przez studentów.

Nadzór merytoryczny nad przebiegiem praktyki oraz warunkami jej realizacji sprawuje, wyznaczony spośród nauczycieli akademickich, opiekun praktyki. W żadnym z dokumentów przywołujących tę funkcję nie sformalizowano wymagań kompetencyjnych wobec opiekunów praktyk. Należy zwrócić uwagę, że zarówno treść Porozumienia jak i Regulaminu nie definiują sposobu postępowania w sytuacji konfliktowej. Rekomenduje się wprowadzenie zapisów składających tego rodzaju obowiązek na ręce opiekuna praktyk ze strony uczelni, a także koordynatora ze strony podmiotu przyjmującego na praktykę.

Stosowane operacyjnie nazewnictwo praktyki zaliczanej na podstawie wykonywanej pracy, jako „praktyki dobrowolnej” mocno komplikuje ocenę oraz nadzór nad realizacją takich praktyk. Zespół oceniający rekomenduje weryfikację stosowanego nazewnictwa oraz ujednolicenia zasad zaliczania praktyk dla osób pracujących.

Harmonogram sesji egzaminacyjnych ustalony jest przez Dziekana Wydziału w odniesieniu do harmonogramu roku akademickiego ustalonego przez Rektora. W odniesieniu do sesji egzaminacyjnej, analiza programów kształcenia pozwala stwierdzić, że w sesji egzaminacyjnej student przystępuje nie więcej niż do trzech egzaminów na studiach I stopnia i dwóch egzaminów na studiach II stopnia. Zajęcia realizowane są w cyklu tygodniowym, przy czym semestr trwa 15 tygodni. Dziekan Wydziału Elektroniki i Technik Informacyjnych odpowiada za rozkład zajęć na kierunku cyberbezpieczeństwo, a zajęcia są planowane z uwzględnieniem równomiernego rozłożenia obciążenia co daje możliwość na cykliczną weryfikację efektów uczenia się oraz na bieżące przekazywanie studentom informacji zwrotnej o osiągniętych efektach uczenia się. Na podstawie udostępnionego harmonogramu zajęć widać, że

zajęcia realizowane są od poniedziałku do piątku pomiędzy godziną 8:00 a 19:00 i prowadzone są zwykle w blokach 2 lub 3 godzinnych. Średnio na dzień student realizuje 5 godzin zajęć (zazwyczaj nie więcej niż 7 i nie mniej niż 3 godziny dziennie). Taki układ planu, w szczególności indywidualne dostosowanie tempa realizacji zajęć pozwala na efektywne wykorzystanie czasu przeznaczonego na udział w zajęciach oraz umożliwia studentom wygospodarowanie czasu na samodzielne uczenie się.

Indywidualizacja ścieżki kształcenia to element, który reguluje tempo realizacji zajęć (wybór przedmiotów). Takie rozplanowanie zajęć w kontekście czasu przewidzianego na udział w zajęciach pozwala na efektywne wykorzystanie czasu na samodzielne uczenie się.

W związku z powyższym można uznać, że organizacja roku akademickiego i rozplanowanie zajęć zapewniają efektywne wykorzystanie przez studentów czasu przewidzianego na udział w zajęciach i samodzielne uczenie się, a także zapewniają sprawdzenie i ocenę efektów uczenia, jak również dostarczenie studentom informacji zwrotnej o uzyskanych efektach.

**Zalecenia dotyczące kryterium 2 wymienione w uchwale Prezydium PKA w sprawie oceny programowej na kierunku studiów, która poprzedziła bieżącą ocenę (jeśli dotyczy)**

| Lp. | Zalecenia dotyczące kryterium 2 wymienione we wskazanej wyżej uchwale Prezydium PKA | Opis realizacji zalecenia | Ocena realizacji zalecenia<br>(zalecenie zrealizowane / zalecenie niezrealizowane) |
|-----|-------------------------------------------------------------------------------------|---------------------------|------------------------------------------------------------------------------------|
| 1.  | <b>Nie dotyczy</b>                                                                  | <b>Nie dotyczy</b>        | <b>Nie dotyczy</b>                                                                 |

**Propozycja oceny stopnia spełnienia kryterium 2**

Kryterium spełnione

**Uzasadnienie**

Treści programowe na kierunku cyberbezpieczeństwo studia I i II stopnia są zgodne z efektami uczenia się oraz z aktualnym stanem wiedzy i metodyki badań w dyscyplinie informatyka techniczna i telekomunikacja, do której oceniany kierunek studiów jest przyporządkowany. Treści programowe są również zgodne zakresem działalności naukowej prowadzonej na Uczelni w ramach tej dyscypliny. Treści programowe są kompleksowe i specyficzne dla zajęć tworzących program studiów i zapewniają uzyskanie wszystkich określonych dla zajęć i kierunkowych efektów uczenia się. Czas trwania studiów, nakład pracy mierzony łączną liczbą punktów ECTS, koniecznych do ukończenia studiów, jak również nakład pracy niezbędny do osiągnięcia efektów uczenia się przypisanych do zajęć i grup zajęć są poprawnie oszacowane i zapewniają osiągnięcie przez studentów efektów uczenia się. Liczba godzin zajęć wymagających bezpośredniego udziału (studentów i nauczycieli akademickich) określona w programie studiów łącznie oraz dla poszczególnych zajęć lub grup zajęć zapewniają osiągnięcie przez studentów efektów uczenia się, a liczba punktów ECTS przypisana tym zajęciom, z zastrzeżeniem uwagi dotyczącej studiów II stopnia (jednoznaczny zapis liczby godzin w ramach zajęć prowadzonych z bezpośrednim udziałem nauczycieli i odpowiadającym ich punktów ECTS) jest zgodna z wymaganiami

ustawowymi. Sekwencja zajęć zapewnia osiągnięcie przez studentów efektów uczenia się. Dobór form zajęć i proporcje liczby godzin zajęć realizowanych w poszczególnych formach są właściwe. Harmonogram realizacji programu studiów umożliwia wybór zajęć, zgodnie z obowiązującymi przepisami, według zasad, które pozwalają studentom na elastyczne kształtowanie ścieżki kształcenia. Harmonogram realizacji programu studiów obejmuje zajęcia lub grupy zajęć związane z prowadzoną w Uczelni działalnością naukową w dyscyplinie, do której został przyporządkowany kierunek, w wymaganym wymiarze punktów ECTS. Harmonogram realizacji programu studiów obejmuje zajęcia poświęcone kształceniu w zakresie znajomości języka obcego, jak również zajęcia z dziedziny nauk humanistycznych lub nauk społecznych (5 punktów ECTS), co jest zgodne z wymogami ustawowymi. Metody kształcenia są różnorodne, specyficzne, zapewniają osiągnięcie przez studentów wszystkich efektów uczenia się, a także stymulują studentów do samodzielności i pełnienia aktywnej roli w procesie uczenia się. Umożliwiają również stosowanie właściwych metod i narzędzi, w tym zaawansowanych technik informacyjno-komunikacyjnych tam, gdzie jest to niezbędne. Stosowane metody kształcenia umożliwiają udział w działalności naukowej, umożliwiają uzyskanie kompetencji w zakresie opanowania języka obcego co najmniej na poziomie B2+ oraz umożliwiają dostosowanie procesu uczenia się do zróżnicowanych potrzeb grupowych i indywidualnych studentów, w tym potrzeb studentów z niepełnosprawnością, jak również realizowanie indywidualnych ścieżek kształcenia.

Efekty uczenia się zakładane dla praktyk są zgodne z efektami uczenia się przypisanymi do pozostałych zajęć lub grup zajęć. Treści programowe, wymiar praktyk oraz przypisana im liczba punktów ECTS zapewniają osiągnięcie przez studentów zakładanych efektów uczenia się.

Zaliczenie praktyk odbywa się na podstawie zdefiniowanej dokumentacji, pozwalającej na prawidłową weryfikację uzyskanych efektów uczenia się. Zarówno program praktyk jak i efekty uczenia się osiągane na praktykach, podlegają systematycznej ocenie.

Plan zajęć umożliwia efektywne wykorzystanie czasu przeznaczonego na udział w zajęciach i samodzielne uczenie się. Czas przeznaczony na sprawdzanie i ocenę efektów uczenia się umożliwia weryfikację wszystkich efektów uczenia się oraz dostarczenie studentom informacji zwrotnej o uzyskanych efektach.

### **Dobre praktyki, w tym mogące stanowić podstawę przyznania uczelni Certyfikatu Doskonałości Kształcenia**

---

### **Rekomendacje**

1. Rekomenduje się przegląd programu studiów II stopnia i jego aktualizację, tak aby liczba godzin realizowanych z bezpośrednim udziałem nauczycieli akademickich i przyporządkowana liczba im liczba punktów ECTS była wskazana we wszystkich kartach przedmiotów.
2. Wprowadzenie do treści umów podpisywanych z przyjmującym na praktykę, literalnie zdefiniowanych oczekiwań (programu praktyki) w zakresie realizowanych efektów uczenia się dla studenta.
3. Wprowadzenie zapisów w formalnych dokumentach kierujących na praktykę, definiujących sposób postępowania w sytuacji konfliktowej.

4. Weryfikacja stosowanego nazewnictwa oraz ujednolicenia zasad zaliczania praktyk dla osób pracujących.

## Zalecenia

---

### **Kryterium 3. Przyjęcie na studia, weryfikacja osiągnięcia przez studentów efektów uczenia się, zaliczanie poszczególnych semestrów i lat oraz dyplomowanie**

#### **Analiza stanu faktycznego i ocena spełnienia kryterium 3**

W Uchwale Nr 393/L/2023 Senatu Politechniki Warszawskiej z dnia 28 czerwca 2023 roku w sprawie warunków, trybu i terminu rekrutacji w roku akademickim 2024/2025 wskazano regulacje, które obowiązują na ocenianym kierunku. W załączniku nr 2 do ww. Uchwały dotyczącej zasad kwalifikacji kandydatów na studia I stopnia wskazano, że procedura kwalifikacyjna dla ocenianego kierunku realizowana w ramach konkursu dla kierunków studiów prowadzonych w Warszawie, a zakwalifikowanie na studia nastąpi w zależności od liczby uzyskanych punktów kwalifikacyjnych (i wskazanych preferencji kandydata dot. szeregowania preferowanych kierunków studiów). W ww. załączniku wskazano formułę, przyjętą na potrzeby wyznaczenia liczby punktów kwalifikacyjnych. O przyjęciu na studia decyduje komisja rekrutacyjna. Komisja ta, uwzględniając ustalone liczby miejsc ustala liczby osób zakwalifikowanych na studia, na podstawie iteracyjnej symulacji wyników procedury kwalifikacyjnej. Liczba punktów kwalifikacyjnych (PK) ustalana była zgodnie z formułą:  $PK = \text{punkty z matematyki} \times \text{współczynnik wagowy dla punktów z matematyki (1)} + \text{punkty z przedmiotu do wyboru lub punkty z dyplomu potwierdzającego kwalifikacje zawodowe na poziomie technika} \times \text{współczynnik wagowy dla punktów z przedmiotu do wyboru (fizyka/chemia/informatyka/biologia 1/0,75/1/0,5 lub dla punktów z dyplomu potwierdzającego kwalifikacje zawodowe na poziomie technika + punkty z języka obcego} \times \text{współczynnik wagowy dla punktów z języka obcego (0,25)}$ . W rekrutacji 2024/2025 liczba punktów kwalifikacyjnych (próg) dla kandydatów na studia cyberbezpieczeństwo pierwszego stopnia wyniósł 193. Zasady rekrutacji na studia I stopnia zapewniają kandydatów o kwalifikacjach wstępnych pozwalających na osiągnięcie kierunkowych efektów uczenia się. Wg załącznika nr 3 do ww. Uchwały w Politechnice Warszawskiej, o przyjęciu na studia II stopnia decyduje komisja rekrutacyjna, która dokonuje analizy dokumentów złożonych przez kandydata. W pierwszym kroku kwalifikacji komisja ocenia (na podstawie dokumentów) czy kandydat na studia drugiego stopnia na ocenianym kierunku studiów posiada kompetencje wymagane do podjęcia tych studiów. Wg regulacji uznaje się, że takie kompetencje posiadają kandydaci, którzy ukończyli studia pierwszego stopnia na tym samym kierunku studiów lub kierunku zbliżonym programowo, co studia drugiego stopnia, na które aplikują. Na tym etapie komisja analizuje przekazane przez kandydata dokumenty pod względem formalnym i merytorycznym, i może zaprosić kandydata na rozmowę kwalifikacyjną lub egzamin. Po przeprowadzeniu analizy dokumentów lub egzaminu komisja może stwierdzić, że kandydat nie posiada kompetencji wymaganych do podjęcia studiów drugiego stopnia, pomimo spełnienia warunku ukończenia studiów pierwszego stopnia na tym samym kierunku studiów lub kierunku, który jest zbliżony programowo do kierunku studiów drugiego stopnia. Od decyzji Komisji Rekrutacyjnych przysługuje odwołanie do Rektora. Na podstawie zgłoszeń, analizy złożonych dokumentów oraz wyniku egzaminu tworzony jest ranking, na podstawie którego przyjmowani są kandydaci. W przypadku, gdy liczba kandydatów przekracza ustalony limit, uruchamiana jest zróżnicowana procedura rekrutacyjna, wg której 80% przyjętych na studia mogą to być osoby kończące ten sam kierunek na poziomie I stopnia

na tym samym Wydziale. Wprowadzono zapis, że wymagane jest, aby ww. kandydat zakończył kształcenie na I stopniu studiów co najmniej z oceną dobrą (na dyplomie). W związku z powyższym należy przyjąć, że warunki rekrutacji na studia, kryteria kwalifikacji i procedury rekrutacyjne są przejrzyste i selektywne oraz umożliwiają dobór kandydatów posiadających wstępną wiedzę i umiejętności na poziomie niezbędnym do osiągnięcia efektów uczenia się. Jednak zastrzeżenia budzi bezstronność zasad rekrutacji na studia II stopnia w kontekście zapewnienia równych szans kandydatom (zróżnicowana procedura rekrutacyjna, 80% absolwenci tego samego wydziału tego samego kierunku). W związku z powyższym rekomenduje się ustalenie jednego kryterium przyjęcia na studia II stopnia dla wszystkich kandydatów.

Proces rekrutacji odbywa się z wykorzystaniem systemu informatycznego, w którym każdy zarejestrowany kandydat posiada indywidualne konto rekrutacyjne. W warunkach rekrutacji (na rok 2024/2025) nie wyszczególniono wymagań dotyczących oczekiwanych kompetencji cyfrowych w odniesieniu do kandydatów. Wymaga się od kandydata umiejętności obsługi systemów informatycznych w stopniu pozwalającym na zarejestrowanie się i przekazanie odpowiednich informacji drogą elektroniczną. W Uchwale nie wskazano wymagań sprzętowych związanych z kształceniem z wykorzystaniem metod i technik kształcenia na odległość, jednak uczelnia zapewnia sprzęt do tego celu oraz przeszkolenie studentów w tym zakresie.

W związku z powyższym można sformułować wniosek, że warunki rekrutacji na studia, kryteria kwalifikacji i procedury rekrutacyjne są przejrzyste i selektywne, umożliwiają dobór kandydatów posiadających wstępną wiedzę i umiejętności na poziomie niezbędnym do osiągnięcia zakładanych efektów uczenia się. Są bezstronne i zapewniają kandydatom równe szanse w podjęciu studiów na kierunku cyberbezpieczeństwo, z zastrzeżeniem, że wprowadzenie zasady zastosowania zróżnicowanej procedury rekrutacyjnej po przekroczeniu ustalonego limitu kandydatów nie można uznać za w pełni bezstronne.

Liczbę miejsc, na które mogą zostać przyjęci kandydaci na studia o określonym kierunku oraz stopniu, profilu i formie kształcenia oraz liczbę miejsc dla osób, które mogą zostać przyjęte na studia w wyniku potwierdzenia efektów uczenia się, określa Rektor. Zasady i warunki potwierdzania efektów uczenia się wprowadzone w Uczelni wprowadzono Uchwałą Nr 387/XLIX/2019 Senatu Politechniki Warszawskiej z dnia 18 września 2019 r. oraz Zrządzeniem nr 51/2019 Rektora Politechniki Warszawskiej z dnia 23 września 2019 r. w sprawie przyjęć na studia w wyniku potwierdzania efektów uczenia się. Taka procedura jest możliwa do realizacji na ocenianym kierunku, gdyż dyscyplina naukowa informatyka techniczna i telekomunikacja, w wyniku ewaluacji za lata 2017-2021 uzyskała ocenę A.

Dziekan, który podjął decyzję o realizacji procedury potwierdzania efektów uczenia się powołuje na wydziale komisję ds. potwierdzenia efektów uczenia się. Komisja, w której stałymi członkami są wydziałowy lub kierunkowy petnomocnik ds. potwierdzania efektów uczenia się (jako przewodniczący) oraz - jak wskazuje Uchwała - osoba zaliczona do „kadry kluczowej dla kierunku”. Ponadto (niestałymi) członkami jest (co najmniej) jeden nauczyciel odpowiedzialny za realizację przedmiotu wskazanego we wniosku oraz przedstawiciel studentów. W wyniku procedury, która realizowana jest na podstawie złożonych przez kandydata dokumentów oraz sprawdzianów wiedzy i umiejętności można uzyskać nie więcej niż 50% punktów ECTS przypisanych do zajęć objętych programem studiów określonego kierunku, poziomu, formy i profilu kształcenia.

Zgodnie z zapisami ogólnouczelnianymi stosowanymi na Wydziale, student może zostać przyjęty na studia w wyniku potwierdzenia efektów uczenia się lub przeniesienia z innej uczelni (również zagranicznej). Regulamin Studiów Politechniki Warszawskiej (paragraf 13 ust. 2) wskazuje w tym zakresie, że warunkiem przyjęcia na studia w trybie przeniesienia z innej uczelni jest zaliczenie przez studenta co najmniej pierwszego roku studiów drugiego stopnia lub pierwszego semestru studiów drugiego stopnia w uczelni macierzystej oraz uzyskanie pisemnego potwierdzenia o wszczęciu procedury odejścia z uczelni macierzystej w ramach przeniesienia. Przeniesienie na kierunek cyberbezpieczeństwo (I/II stopnia) odbywa się na wniosek studenta złożony nie później niż 1 miesiąc przed rozpoczęciem semestru, w którym student ma zostać przyjęty na studia. Dziekan Wydziału przyjmującego studenta określa warunki przyjęcia na studia oraz wyznacza dodatkowe przedmioty do realizacji wynikające z różnic programowych (i terminy zaliczenia). Ponadto student może także wystąpić do Dziekana z wnioskiem o uznanie osiągnięcia efektów uczenia się w wyniku działalności zawodowej, naukowej lub innej, w którym zawarta będzie dokumentacja osiągnięcia efektów uczenia się. Dziekan określa tryb i sposób udokumentowania wniosku oraz limit punktów możliwych do uzyskania w wyniku uznania osiągnięcia efektów uczenia się. Wniosek o uznanie osiągnięcia efektów uczenia się powinien być zaopiniowany przez wyznaczonego przez Dziekana nauczyciela akademickiego.

W związku z powyższym można uznać, że warunki i procedury potwierdzania efektów uczenia się uzyskanych poza systemem studiów zapewniają możliwość identyfikacji właściwych efektów uczenia się oraz oceny ich adekwatności w zakresie odpowiadającym efektom uczenia się określonym w programie studiów. Warunki i procedury uznawania efektów uczenia się uzyskanych w innej uczelni, (w tym w uczelni zagranicznej) zapewniają możliwość ich identyfikacji oraz oceny ich adekwatności w zakresie odpowiadającym efektom uczenia się określonym w programie studiów ocenianego kierunku.

Regulamin Studiów Politechniki Warszawskiej określa zasady dyplomowania (sekcja VI Dyplomowanie i ukończenie studiów). Wg zapisów praca dyplomowa jest samodzielnym opracowaniem zagadnienia naukowego lub praktycznego albo dokonaniem technicznym, prezentującym ogólną wiedzę i umiejętności studenta związane ze studiami na danym kierunku, poziomie i profilu oraz umiejętności samodzielnego analizowania i wnioskowania. Proces dyplomowania jest przeprowadzany z wykorzystaniem systemu Archiwum Prac Dyplomowych (APD-USOS). Stanowisko nr 3/L/2022 Senatu Politechniki Warszawskiej z dnia 21 września 2022 r. w sprawie wytycznych w zakresie prac dyplomowych w Politechnice Warszawskiej wskazuje m.in. aspekty rozróżnienia i zdefiniowania prac dyplomowych kończących studia pierwszego i drugiego stopnia. Praca dyplomowa inżynierska powinna wykazać posiadanie przez dyplomanta umiejętności rozwiązywania problemów, opartej na znajomości podstaw teoretycznych lub doświadczeniach empirycznych oraz wykorzystywania znanych metod, analiz i/lub komputerowych programów dotyczących rozpatrywanego problemu. Praca inżynierska m.in. powinna dotyczyć procesów i urządzeń technicznych i technologicznych. Praca dyplomowa magisterska stanowi samodzielne rozwiązanie przez autora zaawansowanego problemu technicznego i powinna wykazać umiejętność korzystania z metod badawczych i analitycznych oraz umiejętności definiowania i rozwiązywania problemów danej dziedziny. Praca dyplomowa, wg Regulaminu studiów, może być elementem programu prac badawczych Uczelni lub studenckiego ruchu naukowego, a także może też być realizowana we współpracy z podmiotem zewnętrznym. Postęp realizacji prac studenta nad wykonywaniem pracy dyplomowej inżynierskiej jest monitorowany przez promotora w ramach konsultacji i na zajęciach *seminarium dyplomowe, pracowania dyplomowa i przygotowanie pracy dyplomowej* od szóstego semestru studiów I stopnia. Postęp realizacji prac



studenta nad wykonywaniem pracy dyplomowej magisterskiej jest monitorowany przez promotora w ramach konsultacji i na zajęciach pracownia dyplomowa i seminarium dyplomowe od drugiego semestru studiów. Po zakończeniu realizacji pracy dyplomowej student zgłasza do dziekanatu gotowość do złożenia pracy wraz z potwierdzeniem tego faktu przez promotora. Po uzyskaniu zgody, student wprowadza pracę do systemu APD, następnie weryfikowana jest w Jednolitym Systemie Antyplagiatowym (JSA).

Dziekan powołuje komisję egzaminu dyplomowego, w której skład wchodzi co najmniej 4 osoby (przewodniczący komisji, promotor, recenzent oraz nauczyciel akademicki reprezentujący kierunek studiów cyberbezpieczeństwo). W czasie egzaminu dyplomowego student otrzymuje co najmniej dwa pytania problemowe (z listy), które odnoszą się do całego toku studiów odpowiednio I i II stopnia, następnie komisja ustala oceny z egzaminu, ustala oceny cząstkowe za poszczególne części egzaminu oraz ustala ocenę końcową studiów.

W związku z powyższym można stwierdzić, że zasady i procedury dyplomowania są prawidłowe, specyficzne i zapewniają potwierdzenie osiągnięcia przez studentów efektów uczenia się na zakończenie studiów.

Ogólne jednolite zasady sprawdzania i oceniania stopnia osiągania efektów uczenia się określa część V Regulaminu Studiów w Politechnice Warszawskiej. Zobowiązuje on kierownika przedmiotu m.in. do określenia metod etapowej i/lub końcowej weryfikacji osiągnięcia efektów uczenia się (np. egzamin, sprawdziany pisemne i ustne, sprawozdania z wykonanych ćwiczeń laboratoryjnych, opracowanie dokumentacji projektu), zasad zaliczania przedmiotu i wystawiania oceny końcowej z przedmiotu, a także terminów i trybu ogłaszania ocen uzyskiwanych przez studentów oraz zasad poprawiania ocen, możliwości i zasad udziału studentów w dodatkowych terminach sprawdzianów i egzaminów. Szczegółowe zasady sprawdzania i oceniania stopnia osiągania efektów uczenia się ustalane są dla każdego przedmiotu osobno. Informacja o zasadach oceniania i metodach przeprowadzenia oceny znajduje się w regulaminach przedmiotów, które zostały przedstawione podczas wizytacji. Testy, rozwiązania zadań, raporty, sprawozdania są archiwizowane na platformie edukacyjnej LeOn w przypadku ich postaci elektronicznej. W przypadku przeprowadzenia weryfikacji w formie pisemnej (papierowej) wykładowcy są zobowiązani do archiwizowania dokumentacji zgodnie z Zarządzeniem nr 144 Rektora PW z dnia 20 listopada 2020 r. (oraz Zarządzenie nr 114/2021 Rektora PW z dnia 25/11/2021) w sprawie zasad przechowywania dokumentacji poświadczającej dokonanie weryfikacji osiągniętych efektów uczenia się dla przedmiotu. Pozytywna ocena z przedmiotu oznacza osiągnięcie przez studenta wszystkich efektów uczenia się dla przedmiotu.

Regulamin studiów określa jednolitą skalę ocen (par. 18), a także zobowiązuje prowadzącego zajęcia do udostępnienia studentom wyników weryfikacji osiągnięcia efektów uczenia się niezwłocznie po dokonaniu ich oceny, ale nie później niż 48 godzin przed terminem kolejnego egzaminu lub sprawdzianu. Na wniosek studenta prowadzący zajęcia niezwłocznie umożliwia studentowi wgląd do jego ocenionych prac pisemnych. W Regulaminie studiów określa także postępowanie w sytuacjach konfliktowych, np. w przypadku, gdy student zgłasza zastrzeżenia dotyczące przeprowadzonej procedury weryfikacji osiągnięcia efektów uczenia się dla danego przedmiotu może w ciągu 4 dni roboczych od terminu ogłoszenia jej wyników złożyć do dziekana umotywowany wniosek o przeprowadzenie komisyjnej weryfikacji osiągnięcia efektów uczenia się. Dziekan może także zarządzić komisyjną weryfikację osiągnięcia efektów uczenia się z własnej inicjatywy. Komisyjna weryfikacja osiągnięcia efektów uczenia się powinna odbyć się w ciągu 7 dni od dnia złożenia wniosku przez

studenta lub zarządzenia przez dziekana. Komisję, składającą się z co najmniej trzech nauczycieli akademickich, powołuje dziekan. Na wniosek studenta do komisji może zostać powołany wskazany przez niego nauczyciel akademicki lub przedstawiciel wydziałowego organu samorządu studenckiego. Niezaliczenie przedmiotu na danym etapie studiów skutkuje koniecznością powtarzania zajęć z tego przedmiotu, to jest ponownej realizacji tego przedmiotu, realizacji przedmiotu równoważnego lub przedmiotu z tej samej grupy przedmiotów w zależności od programu studiów.

Student z niepełnosprawnością ma prawo do weryfikacji osiągnięcia efektów uczenia się w trybie indywidualnym. Zakres indywidualizacji weryfikacji efektów uczenia się określa dziekan na wniosek studenta i dostosowuje do możliwości studenta. Podsumowując, Regulamin studiów zapewnia równe traktowanie studentów w procesie weryfikacji stopnia oceniania efektów uczenia się, w tym możliwość adaptowania metod organizacji sprawdzania efektów uczenia się do potrzeb studentów z niepełnosprawnościami. Zasady określone w Regulaminie studiów określają postępowania w sytuacjach konfliktowych związanych z weryfikacją efektów uczenia się oraz sposoby reagowania na zachowania nieetyczne i niezgodne z prawem. Ponadto, Regulamin studiów gwarantuje studentom rzetelność i przejrzystość procesu weryfikacji stopnia osiągnięcia efektów uczenia się, a poufność ocen wprowadza bezstronność tego procesu. Ponadto, określa także zasady przekazywania studentom informacji zwrotnej dotyczącej osiągniętych efektów uczenia się.

Weryfikacja i ocena osiągnięcia przez studentów efektów uczenia się stosowana w procesie nauczania i uczenia może odbywać się z wykorzystaniem metod i technik kształcenia na odległość z wykorzystaniem narzędzi MS Teams oraz LeOn, rozwiązania te zapewniają identyfikację studenta (indywidualne konto) oraz bezpieczeństwo danych dotyczących studentów (ochrona przed nieautoryzowanym dostępem). Ww. platformy stosowane są pomocniczo w realizacji zajęć w siedzibie Wydziału/Uczelni.

Metody weryfikacji i oceny osiągnięcia przez studenta efektów uczenia się są indywidualnie dobierane dla przedmiotu. Jest on ściśle powiązany z formą zajęć dydaktycznych oraz zdefiniowanymi efektami uczenia się, których opanowanie przez studenta podlega ewaluacji w trakcie realizacji przedmiotu. Metody weryfikacji osiągniętych przez studentów efektów uczenia się wskazane są w karcie przedmiotu oraz regulaminie przedmiotu. Zapewniają ujednolicone wymagania wobec zdających w ramach danego przedmiotu, zapewniają przeprowadzenie egzaminu lub zaliczenia z uwzględnieniem szczególnych potrzeb zdającego oraz zapobiegają dyskryminacji. Jako przykład można wskazać poprawny dobór różnorodnych metod dla poszczególnych efektów uczenia się - stosuje się: sprawdziany (wiedza); zadania laboratoryjne, sprawozdania z wykonanych ćwiczeń laboratoryjnych, raporty, dokumentacja projektów (umiejętności), czy dyskusja (kompetencje społeczne). Realizowane formy sprawdzające są rozłożone w semestrze (co pozwala na ocenę postępów). Opanowanie języka obcego na wymaganym poziomie B/B2+ realizowane jest z wykorzystaniem właściwych metod (np. wypowiedzi pisemne i ustne, w tym z użyciem języka specjalistycznego). Weryfikacja efektów uczenia się w zakresie wiedzy (np. realizowana w formie egzaminu, kolokwium, testu), w zakresie umiejętności (np. realizowana w formie przeprowadzenia obliczeń projektowych, realizacji projektu przy użyciu narzędzi informatycznych) czy w zakresie kompetencji społecznych (np. zespołowa realizacja zadania projektowego, dyskusja) to istotne metody weryfikacji efektów uczenia się i obszaru dyscypliny, do której przypisany jest oceniany kierunek. Na Wydziale stosowane są również procedury uznawania efektów uczenia się dla przedmiotu, osiągniętych w wyniku uczestniczenia studenta w pracach koła naukowego.

W Księdze Jakości Wydziału Elektroniki i Technik Informacyjnych (wydanie trzecie) w sekcji Zagadnienia etyczne, przeciwdziałanie inflacji ocen sformułowano zalecenia również w odniesieniu do aspektów etyki. Zasady określone w Regulaminie studiów określają postępowania w sytuacjach konfliktowych związanych z weryfikacją efektów uczenia się oraz sposoby reagowania na zachowania nieetyczne i niezgodne z prawem.

Podsumowując, w związku z powyższym można sformułować wniosek, że metody weryfikacji i oceny osiągnięcia przez studentów efektów uczenia się oraz postępów w procesie uczenia się zapewniają skuteczną weryfikację i ocenę stopnia osiągnięcia efektów uczenia się, umożliwiają sprawdzenie i ocenę przygotowania do prowadzenia działalności naukowej oraz udziału w tej działalności, a także umożliwiają sprawdzenie i ocenę opanowania języka obcego co najmniej na poziomie B2 (studia I stopnia) i na poziomie B2+ (w tym języka specjalistycznego). Funkcjonują zasady postępowania w sytuacjach konfliktowych związanych z weryfikacją i oceną efektów uczenia się oraz sposoby zapobiegania i reagowania na zachowania nieetyczne czy niezgodne z prawem.

Potwierdzeniem osiągnięcia efektów uczenia się przez studentów są wyniki prac etapowych i egzaminacyjnych oraz prac dyplomowych. Zespół oceniający dokonał oceny skuteczności osiągania zakładanych efektów uczenia się poddając analizie prace etapowe. Do oceny wybrano zajęcia zróżnicowane pod kątem form zajęć: *bezpieczeństwo systemów i oprogramowania* (wykład, projekt), *usługi i aplikacje internetowe i mobilne: projektowanie i programowanie* (wykład, projekt, laboratorium), *bezpieczeństwo społeczne, organizacyjne i zarządzanie cyberbezpieczeństwem* (wykład, projekt), *bezpieczeństwo Internetu Rzeczy* (zajęcia zintegrowane, projekt).

Prace etapowe były na odpowiednim poziomie (choć nie na wszystkich udostępnionych pracach widoczne były informacje o ocenie), weryfikowały efekty uczenia się dla zajęć zgodne z kartami przedmiotów. W pojedynczych przypadkach prowadzący nie wskazał błędów popełnionych przez studentów, lecz wpisana została sumaryczna liczba punktów. Jednak nie dla wszystkich prac można znaleźć komentarz do wykonanych przez studenta zadań bądź udzielonych odpowiedzi. Rekomenduje się ujednolicić system komentowania form sprawdzających i ich właściwego opisywania.

Analiza prac dyplomowych i protokołów z egzaminów dyplomowych wykazała, że prace są prowadzone na odpowiednim poziomie i są zgodne z wymaganiami dotyczącymi prac inżynierskich i magisterskich. Są to prace o charakterze projektowo-implementacyjnym i/lub badawczym. Prace magisterskie zawierają elementy badawcze i analityczne niezbędne na profilu ogólnoakademickim. Prace inżynierskie zawierają właściwe dla prac inżynierskich elementy projektowe/rozwiązywania zadań. Oceniane prace dyplomowe wskazywały na osiągnięcie zakładanych efektów uczenia się i przygotowania do wykonywania zawodu. Przykładowe prace dyplomowe dotyczą między innymi: automatycznego wykrywania obecności złośliwego oprogramowania w systemie Windows, badanie efektywności zastosowania reguł w łamaniu haseł czy automatyzacja tworzenia ustrukturyzowanych planów reagowania na incydenty z wykorzystaniem informacji o cyberzagrożeniach. Prace dyplomowe poddane weryfikacji mieszczą się w dyscyplinie, do której przyporządkowano oceniany kierunek studiów. Strona edycyjna prac nie budziła zastrzeżeń. W opiniach/recenzjach wskazuje się mocne i słabe strony prac i odnoszą się do wszystkich aspektów pracy dyplomowej. Opiekunowie pracy i recenzenci wystawili zasadne oceny. W przypadku ocen obniżonych w opinii znajduje się uzasadnienie merytoryczne. Pytania zadawane w trakcie egzaminu są adekwatne do zakresu i poziomu studiów.

Publikacje naukowe z udziałem studentów ocenianego kierunku, a także prace dyplomowe, których tematyka jest powiązana z działalnością naukową lub bezpośrednio powiązana z projektami naukowo-

badawczymi realizowanymi w dyscyplinie informatyka techniczna i telekomunikacja to ważny aspekt przygotowania do pracy badawczej. Przedstawiono wykaz publikacji w których współautorami są studenci ocenianego kierunku, co jest dowodem na osiągnięcie przez studentów kompetencji badawczych jest ich aktywność w zakresie publikacji.

Podsumowując, efekty uczenia się osiągnięte przez studentów są utrwalone w postaci prac etapowych i egzaminacyjnych oraz ich wyników w projektach, jak również w pracach dyplomowych. Rodzaj, forma, tematyka i metodyka prac egzaminacyjnych, etapowych, projektowych, a także dyplomowych oraz stawiane im wymagania są dostosowane do poziomu i profilu ogólnoakademickiego, a także do efektów uczenia się zdefiniowanych dla kierunku i wpisują się dyscyplinę informatyka techniczna i telekomunikacja. Ponadto studenci kierunku są współautorami publikacji naukowych w dyscyplinie, do której oceniany kierunek jest przyporządkowany, co stanowi potwierdzenie osiągnięcia kompetencji badawczych.

**Zalecenia dotyczące kryterium 3 wymienione w uchwale Prezydium PKA w sprawie oceny programowej na kierunku studiów, która poprzedziła bieżącą ocenę (jeśli dotyczy)**

| Lp. | Zalecenia dotyczące kryterium 3 wymienione we wskazanej wyżej uchwale Prezydium PKA | Opis realizacji zalecenia | Ocena realizacji zalecenia<br>(zalecenie zrealizowane / zalecenie niezrealizowane) |
|-----|-------------------------------------------------------------------------------------|---------------------------|------------------------------------------------------------------------------------|
| 1.  | <b>Nie dotyczy</b>                                                                  | <b>Nie dotyczy</b>        | <b>Nie dotyczy</b>                                                                 |

**Propozycja oceny stopnia spełnienia kryterium 3**

spełniony

**Uzasadnienie**

Warunki rekrutacji (oraz kryteria kwalifikacji) i procedury rekrutacyjne są przejrzyste i zapewniają kandydatom równe szanse w podjęciu studiów na kierunku cyberbezpieczeństwo z wyłączeniem sytuacji, gdy liczba kandydatów na studia II stopnia jest wyższa niż ustalony limit. Kryteria kwalifikacji są przejrzyste, selektywne oraz umożliwiają dobór kandydatów posiadających wstępną wiedzę i umiejętności na poziomie niezbędnym do osiągnięcia zakładanych efektów uczenia się.

Warunki i procedury uznawania efektów uczenia się uzyskanych w innej uczelni lub poza edukacją formalną zapewniają możliwość identyfikacji efektów uczenia się oraz oceny ich adekwatności w zakresie odpowiadającym efektom uczenia się określonym w programie studiów.

Zasady i procedury dyplomowania zapewniają potwierdzenie osiągnięcia przez studentów efektów uczenia się na zakończenie procesu kształcenia. Ogólne zasady weryfikacji i oceny osiągnięcia przez studentów efektów uczenia się umożliwiają równe traktowanie studentów w procesie weryfikacji i oceniania efektów uczenia się oraz możliwość adaptowania metod i

organizacji sprawdzania efektów uczenia się do potrzeb studentów z niepełnosprawnością. Zasady te zapewniają bezstronność, rzetelność i przejrzystość procesu weryfikacji oraz wiarygodność i porównywalność ocen. Określone są zasady przekazywania studentom informacji zwrotnej dotyczącej stopnia osiągnięcia efektów uczenia się na każdym etapie studiów. Są także określone zasady postępowania w sytuacjach konfliktowych związanych z weryfikacją i oceną efektów uczenia się oraz sposoby zapobiegania i reagowania na zachowania nieetyczne i niezgodne z prawem.

Metody weryfikacji i oceny efektów uczenia się oraz postępów w nauce zapewniają skuteczną weryfikację i ocenę stopnia osiągnięcia wszystkich efektów uczenia się, umożliwiają sprawdzenie przygotowania i uczestnictwa lub prowadzenia działalności naukowej oraz umożliwiają sprawdzenie i ocenę opanowania języka obcego co najmniej na poziomie B2 i B2+ w zakresie znajomości języka specjalistycznego z zakresu informatyki technicznej i telekomunikacji.

Zarówno prace dyplomowe jak i prace etapowe umożliwiają sprawdzenie i ocenę przygotowania oraz udział w działalności naukowej w obszarze informatyka techniczna i telekomunikacja. Osiągnięcie efektów uczenia się przez studentów jest potwierdzane na podstawie prac etapowych i egzaminacyjnych oraz wyników tych prac, sprawozdań z realizacji projektów, ćwiczeń laboratoryjnych, a także prac dyplomowych. Rodzaj, forma, tematyka, metodyka, jak również stawiane wymagania w przypadku prac egzaminacyjnych, etapowych, projektów, ćwiczeń laboratoryjnych, a także prac dyplomowych są dostosowane do poziomu i profilu ogólnoakademickiego, efektów uczenia się oraz zastosowań wiedzy z zakresu dyscypliny, do której kierunek jest przyporządkowany - informatyka techniczna i telekomunikacja.

#### **Dobre praktyki, w tym mogące stanowić podstawę przyznania uczelni Certyfikatu Doskonałości Kształcenia**

---

#### **Rekomendacje**

1. Rekomenduje się ustalenie jednolitych zasad przyjęcia na studia II stopnia dla wszystkich kandydatów.
2. Rekomenduje się ujednolicić system komentowania prac sprawdzających (głównie etapowych) i ich kompleksowego opisywania (punkty/ocena).

#### **Zalecenia**

---

#### **Kryterium 4. Kompetencje, doświadczenie, kwalifikacje i liczebność kadry prowadzącej kształcenie oraz rozwój i doskonalenie kadry**

##### **Analiza stanu faktycznego i ocena spełnienia kryterium 4**

Zajęcia na kierunku cyberbezpieczeństwo prowadzi 89 nauczycieli akademickich, wśród których można wyróżnić: 7 osób posiadających tytuł naukowy profesora, 17 osób posiadających stopień naukowy doktora habilitowanego, 51 osób posiadających stopień naukowy doktora oraz 14 osób z

tytułem zawodowym magistra. Aktywność nauczycieli akademickich skupiona jest głównie wokół dyscypliny informatyka techniczna i telekomunikacja, do której przyporządkowany został oceniany kierunek. Działalność naukowa widoczna jest w wielu obszarach: publikacji oraz projektów naukowo-badawczych i prac zleconych dla przemysłu, a także zrealizowanych wdrożeń. Nauczyciele akademicy prowadzący zajęcia na kierunku w dyscyplinie informatyka techniczna i telekomunikacja w latach 2020 - 2025 opublikowali łącznie ponad 600 publikacji i referatów konferencyjnych.

Nauczyciele akademicy prowadzący zajęcia posiadają aktualny i udokumentowany dorobek naukowy oraz doświadczenie zawodowe w zakresie dyscypliny informatyka techniczna i telekomunikacja, do których przyporządkowane są efekty uczenia się, umożliwiające prawidłową realizację zajęć, w tym nabywanie przez studentów kompetencji badawczych. Dorobek naukowy rozwijany jest w obszarze cyberbezpieczeństwa: bezpieczeństwo sieci komputerowych, analiza cyfrowa sygnałów, systemy przekazu i przetwarzania danych dla heterogenicznych zastosowań IoT, systemy obliczeń na brzegu sieci (Edge Computing), maszynowe uczenie, metody ukrywania informacji w sieciach botnet, czy systemy wykrywania zagrożeń cybernetycznych. Dorobek naukowy osób prowadzących zajęcia na kierunku jest ściśle powiązany z tematyką prowadzonych zajęć dydaktycznych. Doświadczenie zawodowe rozwijane jest w obszarze cyberbezpieczeństwa między innymi poprzez budowanie i wdrażanie systemów cyberbezpieczeństwa, projektowanie bezpiecznych sieci, audytowanie bezpieczeństwa, zarządzanie incydentami, analizy powłamaniowe, doradztwo strategiczne z zakresu cyberbezpieczeństwa.

Obecnie na ocenianym kierunku studiów kształci się 215 studentów (183 na I stopniu, a 32 na stopniu II). Współczynnik liczby studentów na jednego prowadzącego wynosi 2,42 co jest wartością zapewniającą wyjątkowo dobrą realizację zajęć dydaktycznych. Struktura kwalifikacji oraz liczebność kadry w stosunku do liczby studentów umożliwia prawidłową realizację zajęć.

Potwierdzeniem dobrego przygotowania dydaktycznego osób prowadzących zajęcia na kierunku cyberbezpieczeństwo są nagrody i wyróżnienia oraz Medale Komisji Edukacji Narodowej, które uzyskali pracownicy. Szczególnym wyróżnieniem jest nagroda w konkursie „Złota Kreda” dla najlepszych nauczycieli akademickich, którą przyznaje Samorząd Studencki. Wśród osób prowadzących zajęcia na kierunku jest kilka osób, którym przyznano tę nagrodę.

Nauczyciele akademicy prowadzący zajęcia na ocenianym kierunku studiów posiadają kompetencje dydaktyczne, w tym związane z wykorzystaniem metod i technik kształcenia na odległość, umożliwiające prawidłową realizację zajęć. Kompetencje dydaktyczne kadry prowadzącej zajęcia zostały potwierdzone m.in. w trakcie hospitacji zajęć przez zespół oceniający PKA. Hospitowane zajęcia były prowadzone na wysokim poziomie przez nauczycieli o dużych umiejętnościach dydaktycznych. Stosowane metody dydaktyczne były dostosowane do specyfiki prowadzonych zajęć. Realizowane na hospitowanych zajęciach treści programowe były zgodne z treściami zawartymi w sylabusie zajęć. Kadra prowadząca zajęcia na kierunku jest doświadczonym zespołem o ugruntowanych kompetencjach dydaktycznych. Należy docenić wieloletnie doświadczenie dydaktyczne i doświadczenie zawodowe kadry. Osoby prowadzące zajęcia na kierunku cyberbezpieczeństwo poszerzają swoje kompetencje dydaktyczne poprzez szkolenia, kursy lub studia podyplomowe. W programie Kompetentny wykładowca, organizowanym przez Dział Szkoleń CZliTT pracownicy z obsady kierunku uczestniczyli w kilkudziesięciu szkoleniach. Kursy obejmują takie obszary kompetencji dydaktycznych jak: innowacyjne umiejętności dydaktyczne, umiejętności informatyczne, umiejętności prezentacyjne, a także w zakresie prowadzenia dydaktyki w języku



obcym i zarządzania informacją, autoprezentacji, emisji głosu, technik tworzenia prezentacji, w tym multimedialnych, i narzędzi zdalnych.

Przydział zajęć oraz obciążenie godzinowe osób prowadzących zajęcia na ocenianym kierunku studiów jest właściwy i umożliwia prawidłową realizację zajęć. Średnia wielkość zaplanowanych godzin w obciążeniu dydaktycznym dla osób prowadzących zajęcia na kierunku zapewnia osiągnięcie przez studentów efektów uczenia się.

Zajęcia dydaktyczne są przydzielane poszczególnym osobom zgodnie z ich wykształceniem i doświadczeniem zawodowym, a także profilem działalności naukowo-badawczej oraz dydaktycznej. Za realizację poszczególnych zajęć odpowiadają jednostki organizacyjne, którym zlecono ich prowadzenie. O personalnym podziale zajęć dydaktycznych decydują kierownicy przedmiotowych jednostek. Podczas rozdziału zajęć brane są pod uwagę zainteresowania naukowe poszczególnych nauczycieli, ich dorobek naukowy i doświadczenie zawodowe. Dobór osób prowadzących zajęcia jest poprawny i uwzględnia dorobek naukowy, doświadczenie zawodowe oraz osiągnięcia dydaktyczne. Jest on adekwatny do potrzeb związanych z prawidłową realizacją zajęć. Wykłady na kierunku prowadzone są przynajmniej przez osoby ze stopniem doktora. Natomiast zajęcia umożliwiające nabywanie przez studentów umiejętności praktycznych na poziomie inżynierskim prowadzone są przez doświadczonych dydaktyków oraz praktyków pracujących też w sektorze cyberbezpieczeństwa. Na poziomie studiów magisterskich zajęcia prowadzą nauczyciele akademicki, prowadzący badania z dyscypliny informatyka techniczna i telekomunikacja w obszarze cyberbezpieczeństwa.

Zajęcia na ocenianym kierunku prowadzone są w zdecydowanej większości przez nauczycieli akademickich, dla których Uczelnia jest podstawowym miejscem pracy. Dla studiów pierwszego stopnia jest to 2314 godzin na 2580 godzin (89,69%), a dla studiów drugiego stopnia 765 godzin na 900 godzin (85%), czyli spełnione są wymagania dotyczące studiów o profilu ogólnoakademickim, gdzie co najmniej 75% godzin zajęć dydaktycznych prowadzonych jest przez nauczycieli akademickich zatrudnionych w tej uczelni jako podstawowym miejscem pracy.

Nauczyciele akademicki prowadzący zajęcia dydaktyczne na ocenianym kierunku są oceniani przez studentów w zakresie spełniania obowiązków związanych z kształceniem. Ankiety studenckie są przeprowadzane po zakończeniu każdych zajęć dydaktycznych. Ankieta zawiera pytania pozwalające ocenić przygotowanie nauczyciela do zajęć, jego relacje ze studentami oraz organizację zajęć.

W przypadku wyników ankietyzacji dotyczących sposobu prowadzenia zajęć przez nauczyciela akademickiego, znacząco niższych od średniej w danej jednostce, właściwy kierownik jednostki organizacyjnej dokonuje dodatkowej oceny sposobu prowadzenia zajęć przez danego nauczyciela z wykorzystaniem dostępnych narzędzi. Nauczyciele akademicki, którzy uzyskali najlepsze wyniki są wyróżniani przez Dziekana Wydziału.

Nauczyciele akademicki prowadzący zajęcia na kierunku cyberbezpieczeństwo są oceniani przez innych nauczycieli akademickich. Osoba hospitująca po sporządzeniu protokołu hospitacji omawia ich wyniki z hospitowanym nauczycielem. Daje to możliwość rozwoju każdemu z hospitowanych nauczycieli, zgłoszenia ewentualnych rekomendacji i pobudzenia ich aktywności. Wyniki hospitacji mają wpływ na wyniki okresowej oceny nauczycieli akademickich. Po przeprowadzeniu hospitacji, a następnie dyskusji z osobą prowadzącą wizytowane zajęcia, wizytator sporządza notatkę zawierającą podstawowe wnioski, rady i ewentualne zalecenia służące rozwijaniu umiejętności nauczyciela akademickiego. Kopia notatki podpisanej przez obie osoby jest przechowywana przez bezpośredniego

przełożonego osoby hospitowanej przez okres nie krótszy niż cztery lata i na życzenie jest udostępniana przełożonym.

W Uczelni prowadzona jest również okresowa ocena nauczycieli akademickich. Ocena okresowa jest dokonywana nie rzadziej niż raz na 4 lata lub na wniosek Rektora. Ocena okresowa jest prowadzona w następujących obszarach aktywności: działalność dydaktyczna, działalność naukowo-badawcza i działalność organizacyjna. Postawa nauczyciela akademickiego jest monitorowana i oceniana na podstawie: seminariów, ankiet nauczycieli, publikacji oraz hospitacji z przeprowadzonych zajęć dydaktycznych. Daje to możliwość rozwoju każdemu z ocenianych nauczycieli, zgłoszenia ewentualnych rekomendacji i pobudzenia ich aktywności.

W polityce kadrowej Wydziału zwraca się szczególną uwagę na wymianę pokoleniową kadry oraz awanse pracowników. Podstawowym elementem polityki kadrowej są otwarte konkursy. Komisje konkursowe powoływane w tym celu określają zasady rozpisywanych konkursów zgodnie z zaleceniami Europejskiej Karty Naukowca (EKN) oraz określonymi zarządzeniami Rektora. Ważnymi kryteriami w ocenie kandydatów na stanowiska naukowo-dydaktyczne jest dorobek publikacyjny, udział w projektach badawczych, doświadczenia zdobyte w ośrodkach zagranicznych. Strategia rozwoju młodej kadry zakłada systematyczne zatrudnianie najlepszych absolwentów szkół doktorskich oraz osób posiadających doświadczenie w firmach komercyjnych.

Polityka kadrowa umożliwia kształtowanie kadry prowadzącej zajęcia zapewniające prawidłową ich realizację, sprzyja stabilizacji zatrudnienia i trwałemu rozwojowi nauczycieli akademickich i innych osób prowadzących zajęcia, kreuje warunki pracy stymulujące i motywujące członków kadry prowadzącej kształcenie do rozpoznawania własnych potrzeb rozwojowych i wszechstronnego doskonalenia.

W ramach wsparcia i motywowania kadry są oferowane przez jednostki centralne PW szkolenia takie jak np.: nowe programy oferujące wizyty studyjno-szkoleniowe w czołowych światowych uczelniach zagranicznych, studia podyplomowe w obszarze podnoszenia kompetencji zarządczych, coaching indywidualny i zespołowy, specjalistyczne szkolenia certyfikowane. Istotnym elementem systemu jest podejście indywidualne. Na poziomie wydziałów i zakładów polega to na wspieraniu rozwoju poszczególnych pracowników (w obszarach naukowym, dydaktycznym i organizacyjnym) z uwzględnieniem ich potencjału osobistego.

System wspierania i motywowania kadry do rozwoju naukowego obejmuje: przyznawanie grantów badawczych wspierających prowadzenie działalności naukowej w ramach środków finansowych pochodzących z subwencji na Wydziale; przyznawanie grantów w ramach "Inicjatywa Doskonałości-Uczelnia Badawcza" IDUB; przyznawanie nagród za osiągnięcia naukowe w ramach Projektu "Inicjatywa Doskonałości-Uczelnia Badawcza" (IDUB); nagrody Rektora za osiągnięcia naukowe; możliwość obniżania pensum dydaktycznego w przypadku kierowania grantami zewnętrznymi pozyskanymi w drodze konkursów; organizowanie seminariów naukowych w ramach jednostek i konferencji; możliwość korzystania ze staży zagranicznych (płatne urlopy naukowe); bezpłatne szkolenia w zakresie wykorzystania narzędzi i technologii informatycznych w procesie dydaktycznym.

System wspierania i motywowania kadry do podnoszenia kompetencji dydaktycznych obejmuje: szkolenia, na których mogą rozwinąć kompetencje w zakresie innowacyjnych umiejętności dydaktycznych, informatycznych, prezentacyjnych, a także w zakresie prowadzenia dydaktyki w języku obcym i zarządzania informacją. Szkolenia realizowane były w ramach projektów NERW NERW2 realizowanych w latach 2018-2023 w PW; szkolenia w ramach projektu „Politechnika

Warszawska Ambasadorem Innowacji na Rzecz Dostępności” (finansowanie z Programu Operacyjny Wiedza Edukacja Rozwój), którego celem było zwiększenie poziomu dostosowania Politechniki Warszawskiej do potrzeb osób z niepełnosprawnościami m.in. w zakresie procedur kształcenia i wyposażenia pracowników w umiejętności przydatne w kontakcie z osobami z różnymi niepełnosprawnościami; staże dydaktyczne w ramach projektu ENHANCE, ERASMUS+; w początkowym okresie pandemii na Uczelni i Wydziale przeprowadzono szkolenia wspomagające umiejętność zdalnego nauczania. Wszyscy zainteresowani pracownicy mieli możliwość w nich uczestnictwa. W miarę możliwości finansowych realizowane są zakupy nowego sprzętu komputerowego (laptopy, tablety graficzne, kamery, głośniki); działalność Studium Języków Obcych skierowana do pracowników: pomoc w tłumaczeniach, konsultacje językowe, wsparcie metodyczno-językowe.

Polityka kadrowa realizowana na Uczelni obejmuje zasady rozwiązywania konfliktów, a także reagowania na przypadki zagrożenia lub naruszenia bezpieczeństwa, jak również wszelkich form dyskryminacji i przemocy wobec członków kadry. Zasady te są sformułowane w odpowiednim zarządzeniu Rektora PW. W Politechnice Warszawskiej nie akceptuje się żadnych działań lub zachowań mających charakter dyskryminacji, molestowania, molestowania seksualnego lub mobbingu. Zakazuje się wszelkich działań i zachowań noszących cechy dyskryminacji, molestowania, molestowania seksualnego lub mobbingu i zobowiązuje się wszystkich pracowników do przeciwdziałania stosowaniu tych działań i zachowań przez inne osoby. Każdy pracownik jest zobowiązany, aby przejawy dyskryminacji, molestowania, molestowania seksualnego i mobbingu wobec własnej osoby lub innych pracowników niezwłocznie zgłaszać pracodawcy za pośrednictwem m.in.: uczelnianego rzecznika zaufania, rzeczników zaufania, społecznych inspektorów pracy, związków zawodowych.

**Zalecenia dotyczące kryterium 4 wymienione w uchwale Prezydium PKA w sprawie oceny programowej na kierunku studiów, która poprzedziła bieżącą ocenę (jeśli dotyczy)**

| Lp. | Zalecenia dotyczące kryterium 4 wymienione we wskazanej wyżej uchwale Prezydium PKA | Opis realizacji zalecenia | Ocena realizacji zalecenia<br>(zalecenie zrealizowane / zalecenie niezrealizowane) |
|-----|-------------------------------------------------------------------------------------|---------------------------|------------------------------------------------------------------------------------|
| 1.  | Nie dotyczy                                                                         | Nie dotyczy               | Nie dotyczy                                                                        |

**Propozycja oceny stopnia spełnienia kryterium 4**

Kryterium spełnione

**Uzasadnienie**

Doświadczenie i dorobek naukowy osób prowadzących zajęcia jest powiązany z dyscypliną naukową informatyka techniczna i telekomunikacja, do której przyporządkowany jest kierunek oraz umożliwia przygotowanie studentów do prowadzenia badań naukowych w ramach pierwszego stopnia, a także

uczestnictwo w badaniach studentów drugiego stopnia. Nauczyciele akademicki są autorami licznych publikacji naukowych o zasięgu krajowym i międzynarodowym i realizują krajowe i międzynarodowe projekty badawcze. Struktura kwalifikacji oraz liczebność kadry w stosunku do liczby studentów umożliwia prawidłową realizację programu studiów. Nauczyciele akademicki posiadają kompetencje dydaktyczne umożliwiające prawidłową realizację zajęć zarówno w formie stacjonarnej, jak również z wykorzystaniem technik i metod kształcenia na odległość. Dobór nauczycieli akademickich prowadzących zajęcia na kierunku cyberbezpieczeństwo jest transparentny i adekwatny do potrzeb programu studiów. Polityka kadrowa prowadzona jest właściwie, nauczyciele poddawani są ocenie, są ankietowani, zapoznawani z opiniami, opinie są uwzględniane, wyniki są analizowane i wykorzystywane przy przydzielaniu zajęć dydaktycznych oraz w polityce płacowej. Organizowane są szkolenia dla nauczycieli akademickich i innych osób prowadzących zajęcia w zakresie podnoszenia kompetencji dydaktycznych, w tym związanych z kształceniem z wykorzystaniem metod i technik kształcenia na odległość. Realizowana polityka kadrowa obejmuje również zasady rozwiązywania konfliktów, jak też reagowania na przypadki zagrożenia, naruszenia bezpieczeństwa bądź dyskryminacji.

#### **Dobre praktyki, w tym mogące stanowić podstawę przyznania uczelni Certyfikatu Doskonałości Kształcenia**

---

#### **Rekomendacje**

---

#### **Zalecenia**

---

### **Kryterium 5. Infrastruktura i zasoby edukacyjne wykorzystywane w realizacji programu studiów oraz ich doskonalenie**

#### **Analiza stanu faktycznego i ocena spełnienia kryterium 5**

Studenci kierunku cyberbezpieczeństwo korzystają z infrastruktury dydaktycznej w budynku Wydziału Elektroniki i Technik Informacyjnych (WEiTI) położonym przy ul. Nowowiejskiej 15/19. Wydział dysponuje nowoczesną i kompleksowo przygotowaną bazą dydaktyczną i naukową, zapewniającą możliwość realizacji atrakcyjnych zajęć dydaktycznych oraz prowadzenia badań naukowych.

W budynku znajdują się 32 sale wykładowe o łącznej powierzchni ponad 2500 m<sup>2</sup>. Cztery z nich to duże aule: dwie mieszczące po 198 osób i dwie po 145 osób, które są wyposażone w rzutniki multimedialne, komputery oraz systemy nagłośnienia. Pozostałe sale mają pojemność od 26 do 120 osób. Wszystkie są wyposażone w ekrany i rzutniki multimedialne. W części sal znajdują się komputery podłączone do rzutników, a pozostałe są przygotowane do podłączenia komputerów przenośnych.

Na WEiTI znajduje się ponad 100 laboratoriów o łącznej powierzchni ok. 6000 m<sup>2</sup>. Część laboratoriów to laboratoria komputerowe, inne to laboratoria specjalistyczne, w których są prowadzone zajęcia wykorzystujące specjalistyczny sprzęt i/lub oprogramowanie. Studenci kierunku na zajęciach korzystają między innymi z następujących laboratoriów:

- Laboratorium Systemów Cyfrowych, w którym znajdują się stacje robocze PC Linux z oprogramowaniem CAD firm: Cadence, Synopsys, Siemens EDA, wykorzystywane m.in. do przedmiotu *bezpieczne systemy cyfrowe*
- Laboratorium Radiokomunikacji i Internetu Rzeczy, w którym znajdują się Komputery PC (win 11, Linux Ubuntu 22.04), interfejsy Software Defined radio ADALM-PLUTO oraz RTL-SDR, analizator widma Rigol RSA5032N z opcjami rozszerzającymi, oscyloskopy Keysight DSOX1204G (2 szt), oscyloskop Agilent DSO7054A, analizatory stanów logicznych, multimetry cyfrowe Voltcraft VC271SE, lutownice, zasilacze laboratoryjne UNI-T UTP3303, mikroskop elektroniczny, narzędzia ręczne, piec do lutowania rozpliwowego, różnorodne elementy elektroniczne, zestawy ewaluacyjne RFID/NFC firmy Infineon, zestawy ewaluacyjne STM32 z serii NUCLEO, m.in. U545, L476RG, zestawy ewaluacyjne nRF5340-DK i nRF52840, zestawy różnorodnych czujników (termometry, akcelerometry, Time-of-Flight, radary, czytniki RFID, mikrofony, kodeki audio itp.) oraz elementów wykonawczych (diody LED, wyświetlacze, serwo mechanizmy, głośniczki, silniczki), modemy dla sieci komórkowych, moduły interfejsów radiokomunikacyjnych Sub-1GHz i 2.4 GHz, kamery IP, urządzenia powszechnego użytku wyposażone w komunikację radiową (np. dzwonki do drzwi, żarówki itp.) z oprogramowaniem GNU Radio Companion, Gqrx, Sigdigger, Universal Radio Hacker, rtl\_433, Wireshark, nmap, STM32CubeIDE, Python, broker MQTT Mosquitto, nRF Connect, nRF Toolbox, Cortex-M Optimized Crypto Stack (CMOX), wykorzystywane m.in. do przedmiotu *bezpieczeństwo Internetu Rzeczy*
- Laboratorium Sygnałów i systemów, w którym znajdują się komputery PC (win 11, Linux Ubuntu 22.04) z oprogramowaniem Matlab, wykorzystywane m.in. do przedmiotu *sygnały i systemy*
- Laboratorium PBL, w którym znajdują się komputery PC (win 11, Linux Ubuntu 22.04), zestawy Arduino, podstawowy sprzęt pomiarowy (oscyloskopy, multimetry) z oprogramowaniem Arduino IDE, Python wraz z bibliotekami / narzędziami dedykowanymi dla metod uczenia maszynowego / frameworki do przetwarzania dużych zbiorów danych, środowiska z interfejsem www do przetwarzania interaktywnego oraz wizualizacji, systemy kontroli wersji, konteneryzacja (Docker), wykorzystywane m.in. do przedmiotów: *szybkie prototypowanie inżynierskie, analiza danych w cyberbezpieczeństwie*
- Laboratorium Zarządzania Bezpieczeństwem, w którym znajdują się komputery PC (Windows 10/11, Linux Ubuntu 22.04), projektor cyfrowy z oprogramowaniem VirtualBox, przygotowane maszyny wirtualne do pobrania przez studentów z laboratorium, wskazane biblioteki kryptograficzne open source, specyfikacje algorytmów dostarczone studentom przez prowadzących projekty, wykorzystywane m.in. do przedmiotów: *bezpieczeństwo danych, zarządzanie bezpieczeństwem informacji, wstęp do cyberbezpieczeństwa*
- Laboratorium Usług i aplikacji, w którym znajdują się komputery PC (win 11, Linux Ubuntu 22.04), Serwery HP ProLiant Gen9, Generator ruchu Spirent Avalanche, klastry obliczeniowe Raspberry Pi, zakładowe centrum danych (łącznie 180 rdzeni) zbudowane z użyciem platformy OpenStack, stojak dwuuserwerowy przeznaczony do eksperymentowania z rozwiązaniami sieciowymi w centrum danych z oprogramowaniem VirtualBox, Debian Linux, NS2, Apache, Postman, 3CX VoIP Server, Twinkle SIP Client, PragmaDev Studio (wersja licencjonowana), WireShark, Nmap, programy pakietu Coreutils z systemu Debian, dedykowane oprogramowanie zainstalowane na maszynach wirtualnych utworzone przez pracowników ZSUT (emulator usług), WinSCP, Putty, Spirent TestCenter Layer 4-7,

ffmpeg, bento4, Dash Javascript player - Reference Client, Docker, OpenVPN, Android Studio IDE, Visual Studio Code, framework React, framework Flask OpenStack, emulator sieci eNSC, wykorzystywane m.in. do przedmiotów: *usługi i aplikacje Internetu, projektowanie i testowanie systemów i protokołów, projektowanie usług i aplikacji internetowych i mobilnych*

- Laboratoria Informatyczne, w których znajdują się komputery PC (MS Windows 10/11), serwer centralny Windows Server 2018 z oprogramowaniem Oracle Database, NoSQL: MongoDB, Cassandra, Riak i Redis, narzędzia do modelowania baz danych: Toad Data Modeler (wersja 7.2 lub wyższa), Toad for Oracle, SQL Developer, MongoDB Client, środowisko programistyczne: IDE Java: IntelliJ IDEA, Sterowniki JDBC/ODBC, narzędzie informatyczne do przetwarzania XML, wykorzystywane m.in. do przedmiotów: *bazy danych i Big Data, archiwa cyfrowe, uczenie maszynowe, modelowanie i symulacja komputerowa, metody analizy danych, wirtualne środowiska obliczeniowe*
- Laboratoria ogólnowidziałowe, w których znajdują się komputery typu PC, system operacyjny Linux Mate 20.04 z oprogramowaniem JDK v. 21, IntelliJ IDEA v. 2024.3.5, przeglądarka internetowa, Git/Gitlab, System zdalnego nauczania LeON, wykorzystywane m.in. do przedmiotów: *algorytmy i programowanie 1, algorytmy i programowanie 2, zaawansowane architektury procesorów, programowanie równoległe i rozproszone.*

Studenci kierunku mają zapewniony dostęp do wirtualnych laboratoriów i specjalistycznego oprogramowania wspomagającego kształcenie z wykorzystaniem metod i technik kształcenia na odległość. Część oprogramowania to wersje bezpłatne. Istnieje możliwość wypożyczenia platform dydaktycznych do konkretnych badań przez studentów.

Salę i specjalistyczne pracownię dydaktyczne, laboratoria badawcze oraz ich wyposażenie są zgodne z potrzebami procesu kształcenia i uczenia się na kierunku cyberbezpieczeństwo. Są one adekwatne do rzeczywistych warunków przyszłej pracy zawodowej oraz umożliwiają osiągnięcie przez studentów efektów uczenia się, w tym przygotowanie do prowadzenia działalności naukowej lub udział w tej działalności oraz prawidłową realizację zajęć.

Infrastruktura informatyczna wyposażenie techniczne pomieszczeń, pomoce i środki dydaktyczne, aparatura badawcza, specjalistyczne oprogramowanie są sprawne, nowoczesne, nieodlegające od aktualnie używanych w działalności naukowej oraz umożliwiają prawidłową realizację zajęć, w tym z wykorzystaniem zaawansowanych technik informacyjno-komunikacyjnych. Wszystkie laboratoria komputerowe mają dostęp do Internetu (złącze światłowodowe).

Liczba, wielkość i układ pomieszczeń są dostosowane do liczby studentów oraz liczebności grup i umożliwiają prawidłową realizację zajęć dydaktycznych, w tym samodzielne wykonywanie czynności badawczych.

Studenci kierunku cyberbezpieczeństwo mają możliwość korzystania z kilku jednostek bibliotecznych na terenie uczelni, w szczególności ze zbiorów Biblioteki, bibliotek instytutowych na WEiTI oraz Biblioteki Głównej PW. Biblioteka Główna PW, oprócz tradycyjnego dostępu do Wypożyczalni, oferuje dostęp do zasobów elektronicznych. Biblioteka na Wydziale dysponuje dwiema czytelniami:

- Czytelnia naukowa, w której użytkownicy pracują w ciszy, oferuje dostęp do naukowych czasopism polsko i angielskojęzycznych, podręczników akademickich oraz nowości wydawniczych tematycznie powiązanych z kierunkami studiów. Czytelnicy mają też dostęp do gniazd elektrycznych, do których mogą podłączyć własne laptopy, co pozwala im korzystać z sieci Wi-Fi, a tym samym z elektronicznych źródeł naukowych. Ze zbiorów czytelni mogą na miejscu korzystać wszyscy zainteresowani. Czytelnia jednorazowo może pomieścić 30 osób.



- Czytelnia cyfrowa jest miejscem do pracy w grupach. Można w niej głośno rozmawiać. Jest pomieszczeniem sprzyjającym „burzy mózgów”. Znajduje się tam 9 stanowisk komputerowych z dostępem do Internetu i pakietem LibreOffice. Tutaj można bez konieczności logowania się do systemu korzystać z elektronicznych pełnotekstowych publikacji naukowych, zamieszczonych w e-bazach, które subskrybuje dla społeczności Politechniki Biblioteka Główna. Użytkownicy mają do swojej dyspozycji 40 miejsc.

Biblioteka jest czynna od poniedziałku do piątku w godz. 9:00 – 18:00. Lokalizacja biblioteki, liczba, wielkość i układ pomieszczeń bibliotecznych, ich wyposażenie techniczne, liczba miejsc w czytelni, udogodnienia dla użytkowników, godziny otwarcia zapewniają warunki do komfortowego korzystania z zasobów bibliotecznych w formie tradycyjnej i cyfrowej.

Na ocenianym kierunku zapewniona jest zgodność infrastruktury dydaktycznej, naukowej i bibliotecznej oraz zasad korzystania z niej z przepisami BHP. Obszar ten uregulowany jest zarządzeniem Rektora nr 172/2020 w sprawie zapewnienia bezpieczeństwa w obiektach i na terenach oraz bezpieczeństwa i higieny pracy Politechniki Warszawskiej oraz zarządzeniem Rektora nr 165/2020 w sprawie szkoleń z zakresu bezpiecznych i higienicznych warunków kształcenia studentów oraz uczestników studiów podyplomowych Politechniki Warszawskiej. W każdym laboratorium dostępny jest regulamin korzystania z aparatury będącej na wyposażeniu sali, który określa także podstawowe zasady BHP obowiązujące w tym pomieszczeniu. Dodatkowo studenci i pracownicy odbywają obowiązkowe szkolenia BHP.

Studenci mają możliwość korzystania z sieci bezprzewodowej oraz pomieszczeń dydaktycznych, laboratoriów naukowych, komputerowych oraz specjalistycznego oprogramowania poza godzinami zajęć w celu wykonania zadań projektowych, czy prac dyplomowych. Poza godzinami zajęć studenci mają dostęp do bazy dydaktycznej po zgłoszeniu takiego zapotrzebowania do opiekuna (w przypadku pracy dyplomowej) lub prowadzących zajęcia. Często oprogramowanie jest dostępne zdalnie bez ograniczeń dzięki udostępnionym maszynom wirtualnym. Prawie wszystkie pomieszczenia Wydziału znajdują się w zasięgu sieci bezprzewodowej, która jest dostępna dla wszystkich pracowników i studentów.

Infrastruktura dydaktyczna i naukowa jest dostosowana do potrzeb osób z niepełnosprawnością, w sposób zapewniający tym osobom pełny udział w kształceniu i prowadzeniu działalności naukowej oraz korzystaniu z technologii informacyjno-komunikacyjnej, a także likwidację barier w dostępie do sal dydaktycznych, pracowni i laboratoriów, jak również zaplecza sanitarnego. Budynek jest wyposażony w windy i podjazdy. Osoby poruszające się na wózkach mają łatwy dostęp do Biblioteki, ponieważ mieści się ona na parterze. Przy wejściu głównym do budynku Wydziału jest podjazd. Dla osób poruszających się na wózkach do Czytelni Cyfrowej jest oddzielne wejście z podnośnikiem w skrzydle C budynku Wydziału. Dla osób niewidomych i słabo widzących, tak jak w całym budynku, w Bibliotece zastosowano tabliczki informacyjne w alfabecie Braille’a. W czytelni znajduje się biurko z elektroniczną regulacją wysokości. Jest to udogodnienie nie tylko dla osób poruszających się na wózkach. Dzięki regulacji wysokości biurko można dostosować do wzrostu użytkownika, przez co miejsce nauki staje się bardziej ergonomiczne i wygodne. W styczniu 2023 roku powstał plakat informacyjny dotyczący sprzętu, który znajduje się w poszczególnych bibliotekach PW i ma za zadanie ułatwić osobom z niepełnosprawnościami dostęp do różnych publikacji, czy pomóc w przygotowaniu materiałów na zajęcia. Plakat został opracowany przy współpracy Biblioteki WEiT z Biblioteką Główną i pozostałymi bibliotekami PW.

Infrastruktura informatyczna i oprogramowanie stosowane w kształceniu z wykorzystaniem metod i technik kształcenia na odległość umożliwia synchroniczną i asynchroniczną interakcję między studentami a nauczycielami akademickimi i innymi osobami prowadzącymi zajęcia, jest połączona z innymi systemami uczelnianymi, dostępna dla studentów o specjalnych potrzebach edukacyjnych, w tym studentów z niepełnosprawnościami.

Na wybranych zajęciach jest dostęp do zasobów wirtualnych, jak np. laboratoria teleinformatyczne, czy PLLAB (zasoby serwerowe), gdzie studenci otrzymują możliwość zdalnego korzystania z oprogramowania. W procesie dydaktycznym wykorzystywana jest platforma edukacyjna LeON, służąca do umieszczania materiałów dydaktycznych, przeprowadzania testów i zadań oraz komunikacji ze studentami. Dla każdego przedmiotu założona jest witryna przedmiotu (kurs), a uczestniczący w kursie studenci są automatycznie przenoszani z systemu zapisów w USOS. Poza tym platforma zawiera informacje i ogłoszenia istotne dla wszystkich jej użytkowników. Platforma jest dodatkowa zintegrowana z narzędziem do komunikacji synchronicznej (wideo spotkań) Big Blue Button - BBB. Wszyscy studenci PW mają dostęp do narzędzi MS Office 365, a przez to również do kolejnego narzędzia do komunikacji synchronicznej – MS Teams. Wszystkie wymienione powyżej narzędzia są intensywnie wykorzystywane przez studentów i wykładowców kierunku cyberbezpieczeństwo, a ich obsługą i pomocą użytkownikom zajmuje się dział IT.

Studenci i pracownicy Wydziału mogą korzystać z usług ponad dwudziestu jednostek systemu biblioteczno-informacyjnego Politechniki Warszawskiej, w szczególności: Bibliotek Wydziałowych, Biblioteki Głównej, a także Fili Biblioteki Głównej Campusu Południowego. Zbiory Biblioteki PW obejmują zarówno tomy drukowanych książek i czasopism, czasopisma elektroniczne, źródła informacji, książki elektroniczne jak i bazy danych. Obejmują one następujące bazy danych: katalog tradycyjnych zasobów zrealizowany w systemie Aleph, obejmujący księgozbiory wszystkich bibliotek Politechniki; bibliotekę cyfrową, zrealizowaną przy użyciu oprogramowania D-libra (zasoby historyczne i archiwalne); moduł E-źródła dający dostęp do 127 baz danych bibliograficzno-abstraktowych i pełnotekstowych (160 tys. tytułów książek i 6 tys. tytułów czasopism w dostępie pełnotekstowym). Do najważniejszych komercyjnych baz danych należą Web of Science, Scopus, CSA, PROQUEST, INSPEC oraz bazy największych wydawców (m.in.: Elsevier, Emerald, Springer, IEEE, ACM DL, Taylor and Francis, Wiley) – co oznacza pełen dostęp do liczących się bazy danych w zakresie cyberbezpieczeństwa. W Czytelni Cyfrowej studenci mają do swojej dyspozycji 9 stanowisk komputerowych z dostępem do Internetu i pakietem LibreOffice. W Bibliotece WEiTI zarówno dokumenty tradycyjne, jak i elektroniczne, użytkownicy mogą wyszukać i przeglądać poprzez wyszukiwarkę PRIMO.

Na Uczelni funkcjonuje zintegrowany informatyczny system biblioteczny, który pozwala na jednoczesne przeszukiwanie wszystkich katalogów bibliotek uczelnianych, a także możliwość rezerwowania, zamawiania, wypożyczania i samodzielnego przedłużania terminu wypożyczenia książek, ze zbiorów wybranych bibliotek oraz zdalnego dostępu do zasobów cyfrowych książek i czasopism.

Biblioteka w swoich zbiorach posiada 17 198 woluminów. Gromadzone są dokumenty z zakresu cyberbezpieczeństwa, elektroniki, informatyki, telekomunikacji, inżynierii biomedycznej, automatyki, robotyki i dziedzin ściśle powiązanych z ocenianym kierunkiem. Gromadzenie księgozbioru opiera się na sylabusach i informacji bezpośrednio przekazywanej do Biblioteki przez nauczycieli akademickich, a także przez samych studentów, którzy chcieliby mieć jakiś konkretny tytuł w zbiorach biblioteki,

związany z kierunkiem studiów. Zbiory uzupełniane są także o nowości wydawnicze, które nie zawsze znajdują się w sylabusach, ale są literaturą wartościową poszerzającą wiedzę i rozwijającą zainteresowania związane z kierunkiem studiów lub kierunkami pokrewnymi u studentów. Biblioteka prenumeruje również wybrane czasopisma naukowe i branżowe z zakresu cyberbezpieczeństwa.

Biblioteka ma wprowadzony komputerowy system Aleph, który całkowicie zautomatyzował działanie Biblioteki. Aleph zintegrował konta biblioteczne czytelników w Bibliotece Głównej i Bibliotece Wydziałowej, jak również w innych bibliotekach systemu uczelnianego, które przystąpiły do Sieci Bibliotek PW. Czytelnicy od tej pory mają jedną kartę biblioteczną, którą stała się legitymacja (w przypadku studentów). Jest to olbrzymie ułatwienie dla studenta, który wszystkie swoje wypożyczenia z bibliotek PW widzi na jednym koncie. Może sam monitorować swoje zamówienia, wypożyczenia, zwroty i prolongaty. System także przypomina o zbliżających się terminach zwrotów wysyłając czytelnikom monity. Aleph to system, który pozwala użytkownikom zamawiać literaturę online. Czytelnicy również mogą samodzielnie trzykrotnie przedłużyć swoje wypożyczenia. Również istnieje możliwość wypełnienia deklaracji i zapisanie się do Biblioteki online. System Aleph synchronizuje się z systemem USOS i dzięki temu precyzyjnie ustawia ważność kont bibliotecznych studentów.

Zasoby biblioteczne są zgodne, co do aktualności, zakresu tematycznego i zasięgu językowego, a także formy wydawniczej, z potrzebami procesu nauczania i uczenia się, umożliwiają osiągnięcie przez studentów efektów uczenia się, w tym przygotowanie do prowadzenia działalności naukowej lub udział w tej działalności oraz prawidłową realizację zajęć.

Literatura zalecana w sylabusach jest dostępna w zasobach bibliotecznych w liczbie egzemplarzy dostosowanej do potrzeb procesu nauczania i uczenia się oraz liczby studentów. Biblioteka corocznie dokonuje powiększania zasobów bibliotecznych w ramach zakupu książek oraz prenumeraty czasopism. Zarówno nauczyciele akademicki, jak również studenci mogą zgłosić potrzebę dodatkowego zakupu wybranej pozycji literaturowej.

Dostęp do zasobów bibliotecznych i informacyjnych jest dostosowany do potrzeb osób z niepełnosprawnością, w sposób zapewniający tym osobom pełne korzystanie z zasobów. W ramach współpracy z Sekcją ds. Osób z Niepełnosprawnościami w Politechnice Warszawskiej otrzymano komputer z programem Window-Eyes PL, klawiatury specjalistyczne, monitor brajlowski (linijka), drukarkę brajlowską, elektroniczną lupę dla osób słabo widzących, czy myszkę typu BIGtrack.

Infrastruktura Wydziału jest poddawana przeglądowi, który jest realizowany zawsze przed rozpoczęciem roku akademickiego, również pod kątem zajęć z wykorzystaniem metod i technik kształcenia na odległość. Infrastruktura techniczna/laboratoryjna jest sukcesywnie odnawiana (dla przykładu w roku akademickim 2023/2024 wymieniono i przeprojektowano większość modułów laboratoryjnych z przedmiotów układowych. Ponadto zakupiono i wymieniono wszystkie oscyloskopy w laboratoriach Teorii Obwodów i Podstaw Pomiarów. Ponadto niektóre laboratoria zostały wyposażone w nowy sprzęt (komputery, oscyloskopy, generatory funkcyjne, itp.) kilka lat temu, w trakcie remontu i rozbudowy gmachu WEiTl. Uwagi studentów pojawiające się w ankietach są regularnie wykorzystywane do modernizacji laboratoriów i pracowni. Nowy sprzęt wzbogaca również laboratoria w przypadku konieczności stworzenia go samodzielnie. Przykładem takich zasobów może być laboratorium przygotowane na potrzeby przedmiotu *systemy Internetu Rzeczy*.

Podczas okresowych przeglądów aparatury zapewniony jest udział nauczycieli akademickich oraz studentów. Wyniki okresowych przeglądów, w tym wnioski z oceny dokonywanej przez studentów,

są wykorzystywane do doskonalenia infrastruktury dydaktycznej, naukowej i bibliotecznej wyposażenia technicznego pomieszczeń, pomocy i środków dydaktycznych, aparatury badawczej, specjalistycznego oprogramowania, zasobów bibliotecznych, informacyjnych oraz edukacyjnych.

**Zalecenia dotyczące kryterium 5 wymienione w uchwale Prezydium PKA w sprawie oceny programowej na kierunku studiów, która poprzedziła bieżącą ocenę (jeśli dotyczy)**

| Lp. | Zalecenia dotyczące kryterium 5 wymienione we wskazanej wyżej uchwale Prezydium PKA | Opis realizacji zalecenia | Ocena realizacji zalecenia<br>(zalecenie zrealizowane / zalecenie niezrealizowane) |
|-----|-------------------------------------------------------------------------------------|---------------------------|------------------------------------------------------------------------------------|
| 1.  | Nie dotyczy                                                                         | Nie dotyczy               | Nie dotyczy                                                                        |

**Propozycja oceny stopnia spełnienia kryterium 5**

Kryterium spełnione

**Uzasadnienie**

Uczelnia i Wydział dysponuje infrastrukturą dydaktyczną i naukową zabezpieczającą w pełni realizację procesu kształcenia na kierunku cyberbezpieczeństwo. Infrastruktura laboratoryjna umożliwia studentom przygotowanie do prowadzenia badań naukowych na studiach pierwszego stopnia oraz realizacji takich badań na studiach drugiego stopnia. Liczba i wielkość pomieszczeń dydaktycznych jest adekwatna do liczby studentów ocenianego kierunku. Pracownie i laboratoria są wyposażone w sposób umożliwiający osiągnięcie zakładanych efektów uczenia się w ramach zajęć laboratoryjnych, ćwiczeniowych i projektowych. Na szczególną uwagę zasługuje system zdalnego dostępu do zasobów sal laboratoryjnych i zasobów serwerowni wykonany przez pracowników Wydziału. Uczelnia dysponuje biblioteką, zapewniającą dostęp do bogatych zasobów książkowych oraz zbiorów cyfrowych. Zarówno infrastruktura dydaktyczna, jak również biblioteka jest przystosowana dla osób niepełnosprawnych. Na ocenianym kierunku prowadzone okresowe przeglądy infrastruktury dydaktycznej i naukowej. Uwagi w tym zakresie mogą składać studenci i pracownicy. Na tej podstawie wykonuje się remonty i modernizację infrastruktury.

**Dobre praktyki, w tym mogące stanowić podstawę przyznania uczelni Certyfikatu Doskonałości Kształcenia**

---

**Rekomendacje**

---

**Zalecenia**

---

## **Kryterium 6. Współpraca z otoczeniem społeczno-gospodarczym w konstruowaniu, realizacji i doskonaleniu programu studiów oraz jej wpływ na rozwój kierunku**

### **Analiza stanu faktycznego i ocena spełnienia kryterium 6**

Bardzo aktywna i rozbudowana współpraca z otoczeniem społeczno-gospodarczym oparta została przede wszystkim na osobistych kontaktach kadry kierunku. Z uwagi na częstotliwość oraz formę kontaktów nie powołano (jak dotychczas) żadnej formy instytucjonalnej, dla animowania współpracy.

Jako jedno z głównych forów wymiany informacji z otoczeniem, wykorzystywane są organizowane cyklicznie w drugiej połowie października i na przełomie lutego i marca, Targi Pracy. Obecność na tej imprezie, dużej liczby podmiotów biznesowych zainteresowanych kontaktem ze studentami kierunku, pozwala na bezpośrednią wymianę informacji i poruszanie ew. tematów do współpracy. Stałym elementem Targów są prelekcje, przygotowane przez przedstawicieli otoczenia społeczno-gospodarczego, skierowane do studentów ale i kadry Wydziału. Przykładowe tematy prelekcji to: „Praktyczne aspekty wykorzystania sond oscyloskopowych” – przygotowana przez firmę NDN czy „Funkcjonalny monitoring układów scalonych – rozwiązania sprzętowe i oprogramowanie” – zaprezentowana przez firmę Siemens.

Dobór partnerów otoczenia społeczno-gospodarczego jest w pełni zgodny z koncepcją i celami kształcenia kierunku oraz oczekiwaniami rynku pracy właściwego dla kierunku. Wśród partnerów obecne jest pełne spektrum podmiotów, w tym duże podmioty, o szerokim zakresie potrzeb i specjalizacji kompetencyjnej (np. Orange, T-Mobile, Asseco, KPMG itp.), a także szkoły średnie. Wypracowane kontakty formalizowane są w postaci umów/porozumień o współpracy w zakresie praktyk zawodowych, możliwości współpracy w zakresie badań naukowych czy działalności naukowo-dydaktycznej i organizacyjnej.

Choć przedstawiciele podmiotów otoczenia nie są bezpośrednio wykorzystywani do prowadzenia całych bloków zajęć, prowadzą jednak zajęcia o wybranej tematyce w ramach takiego bloku. Jako przykład można przedstawić przedmiot „Kryminalistyka cyfrowa”, którego dwugodzinną część prowadzi przedstawiciel Fundacji Bezpieczna Cyberprzestrzeń czy „Komputerowe i sieciowe systemy operacyjne”, których fragment prowadzi wykładowca WAT.

Efektom kontaktów są także prace dyplomowe, realizowane przez studentów, których tematyka powstaje w trakcie kontaktów studentów z zatrudniającymi ich podmiotami lub w trakcie praktyk. Przykładami prac realizowanych na potrzeby partnerów są np. „Automatyzacja obsługi zgłoszeń dotyczących powtarzalnych incydentów bezpieczeństwa”, praca magisterska przygotowana we współpracy z CERT Polska czy „Wdrażanie mechanizmów bezpieczeństwa definiowanych kodem dla środowiska chmurowego Kubernetes”, praca inżynierska (2024) - temat powiązany z rolą zawodową dyplomanta w firmie DevOps.

Inną formą współpracy jest uczestnictwo studentów w, prowadzonych z podmiotami otoczenia, pracach badawczych. Obecnie trwają prace przygotowawcze do publikacji wyników badań w projekcie prowadzonym wspólnie z firmą Cryptomage.

Bliska współpraca z podmiotami otoczenia pozwala na pozyskanie sprzętu czy materiałów. Choć nie zawsze dedykowane jedynie dla wizytowanego kierunku, wykorzystywane są jako wsparcie dla konkretnych przedmiotów i zajęć. Przykładowo, do grupy przedmiotów z techniki cyfrowej i systemów cyfrowych (wykorzystywane do prac dyplomowych z obszaru rozwiązań sprzętowych w Cyberbezpieczeństwie) pozyskano: Platformy do prototypowania FPGA oraz narzędzia CAD dla celów edukacyjnych - w ramach programu AMD/Xilinx University Program, Platformy Joule - w ramach współpracy studenckiego Koła Naukowego z Intel, Oscyloskopy MSO - w ramach wsparcia studenckiego Koła Naukowego przez firmę Tespol.

Bardzo aktywnie prowadzona jest także współpraca ze szkołami niższego szczebla edukacyjnego. Uczniom szkół średnich udostępniane są pracownie i laboratoria Wydziału. Przedstawiciele kadry kierunku prowadzą wybrane zajęcia z uczniami (np. w ramach projektu „Zawsze ciekawi”). Uczniom szkół średnich udostępniane są również zasobowy biblioteczny Wydziału, w tym źródła elektroniczne. W 2019 roku, wspólnie Ośrodkiem Edukacji Informatycznej i Zastosowań Komputerów w Warszawie oraz XXVII Liceum Ogólnokształcącym im. Tadeusza Czackiego w Warszawie Centrum uruchomiono Projekt Edukacyjny Stem PW - konkurs pozwalający promować i wspierać uczniów szkół średnich. W trzeciej edycji konkursu (2021) wzięło udział 501 uczniów z 47 szkół z całej Polski. Innym bliskim partnerem jest np.. Technikum Mechatroniczne nr 1, współpraca z którym zaowocowała (na potrzeby rekrutacyjne na wybranych kierunkach) budowania polityki uznawania dyplomów technika podczas rekrutacji.

Stała i operacyjnie sprawna współpraca wymaga ciągłej obserwacji i wprowadzania ew. korekt. Prace w tym obszarze koordynuje i realizuje na poziomie Uczelni koordynuje Dział Analiz Strategicznych (DAS). W ramach badania „Diagnoza potrzeb pracodawców i instytucji współpracujących z PW” – prowadzone są, mające charakter moderowanych badań jakościowych, spotkania z pracodawcami, organizowane w ramach dyscyplin naukowych oraz prowadzone są badania ankietowe. Dodatkowo, przeprowadzono także badania i analizy: „Identyfikacja potrzeb innowacyjnych podmiotów gospodarczych” oraz „Potrzeby innowacyjnych podmiotów gospodarczych względem uczelni, w tym PW”.

Wyniki badań, w postaci raportów i sprawozdań są przedstawiane na spotkaniach z Wydziałowym Pełnomocnikiem ds. Jakości Kształcenia oraz Radzie Wydziału.

**Zalecenia dotyczące kryterium 6 wymienione w uchwale Prezydium PKA w sprawie oceny programowej na kierunku studiów, która poprzedziła bieżącą ocenę (jeśli dotyczy)**

| Lp. | Zalecenia dotyczące kryterium 6 wymienione we wskazanej wyżej uchwale Prezydium PKA | Opis realizacji zalecenia | Ocena realizacji zalecenia<br>(zalecenie zrealizowane /<br>zalecenie niezrealizowane) |
|-----|-------------------------------------------------------------------------------------|---------------------------|---------------------------------------------------------------------------------------|
| 1.  | Nie dotyczy                                                                         | Nie dotyczy               | Nie dotyczy                                                                           |

**Propozycja oceny stopnia spełnienia kryterium 6**



Kryterium spełnione

### **Uzasadnienie**

Bieżąca i bardzo aktywna współpraca z podmiotami otoczenia społeczno-gospodarczego, pozwala na prowadzenie statycznych działań, podnoszących jakości kształcenia oraz uzyskania pełnej zgodności programu studiów z koncepcją i celami kształcenia. Bieżący kontakt z przedstawicielami otoczenia społeczno-gospodarczego prowadzony jest głównie z podmiotami działającymi w obszarach działalności zawodowej oraz reprezentantów rynku pracy właściwego dla wizytowanego kierunku. Przedstawiciele otoczenia społeczno-gospodarczego biorą czynny udział w stałej weryfikacji i rozwoju zarówno programu studiów, jak i sposobu kształcenia na kierunku. Organizowana współpraca prowadzona jest w formie niesformalizowanej (np. w postaci spotkań z przedstawicielami podmiotów, prowadzącymi seminaria lub wykłady tematyczne). Stosowane formy współpracy oraz stała wymiana informacji z otoczeniem społeczno-gospodarczym stanowią dobrą podstawę dla rozwoju i doskonalenia współpracy, a także modelowania i modernizacji programu studiów. Zakres oraz poziom współpracy jest monitorowany w procesie ciągłym. W oparciu o regularne rozmowy oraz ankiety powstają raporty, pozwalające na podejmowanie bieżących i aktywnych korekt zakresu współpracy.

**Dobre praktyki, w tym mogące stanowić podstawę przyznania uczelni Certyfikatu Doskonałości Kształcenia**

---

### **Rekomendacje**

---

### **Zalecenia**

---

**Kryterium 7. Warunki i sposoby podnoszenia stopnia umiędzynarodowienia procesu kształcenia na kierunku**

### **Analiza stanu faktycznego i ocena spełnienia kryterium 7**

Umiędzynarodowienie kierunku cyberbezpieczeństwo wpisuje się w Strategię rozwoju Politechniki Warszawskiej. Politechnika Warszawska dąży do statusu europejskiego centrum kształcenia – Uczelni otwartej na studentów z całego świata, nauczającej w sposób nowoczesny i efektywny, z dużym komponentem zajęć projektowych i silnym powiązaniem kształcenia z badaniami.

Studenci kierunku, zarówno studiów pierwszego stopnia, jak też studiów drugiego stopnia, mają możliwość uczestnictwa we wszystkich formach wymiany międzynarodowej dostępnej na Wydziale Elektroniki i Technik Informacyjnych i Uczelni. Na Wydziale jest powołany Pełnomocnik Dziekana ds.

międzynarodowej wymiany studentów, do którego może zgłosić się każdy student. Studenci korzystają z międzyuczelnianej wymiany studentów ramach programów Erasmus+, ATHENS oraz na zasadzie umów dwustronnych z uniwersytetami zagranicznymi. Wydział ma podpisanych ponad 100 umów o wymianie studenckiej z uczelniami zagranicznymi, w tym ma 3 umowy o podwójnym dyplomowaniu. W ramach tych wszystkich umów mogą uczestniczyć studenci kierunku cyberbezpieczeństwo. Wymiana międzynarodowa obejmuje zarówno studentów przyjeżdżających, jak też wyjeżdżających na wymianę w ramach programu Erasmus+ oraz innych programów i umów bilateralnych, a także nauczycieli akademickich.

Studenci kierunku najczęściej wyjeżdżają do następujących ośrodków: Fachhochschule Salzburg, Fachhochschule St. Pölten, Katholieke Universiteit Leuven, Ecole Polytechnique Federale de Lausanne, Technische Universität Berlin, Karlsruher Institut für Technologie, Universidad de Las Palmas de Gran Canaria, Universidad Carlos III de Madrid, Universidad Politecnica de Valencia, Institut National des Sciences Appliquées de Lyon, Università degli Studi di Genova, Kyungpook National University, Universidade de Lisboa oraz Helsinki Metropolia University of Applied Sciences.

W latach akademickich 2021-2025 za granicę wyjechało 29 studentów tego kierunku (na co najmniej jeden semestr), w tym 19 na studiach pierwszego stopnia i 10 na studiach drugiego stopnia. W ramach wymiany przyjechało 12 studentów, między innymi z Francji, Grecji, Hiszpanii, Portugalii i Włoch. Dodatkowo na kierunku studiuje 12 obcokrajowców z Ukrainy i Białorusi.

Na kierunku prowadzą zajęcia osoby z zagranicy na stałe pracujące na PW. Są to profesor z Hiszpanii, profesor z Ukrainy, dr z Hiszpanii oraz mgr z Iranu. Natomiast prowadzący zajęcia (7 osób) wyjechało w ramach podpisanych umów na uczelnię Beibu Gulf University w Chinach oraz do Kyungpook National University w Korei.

Zdobywanie kompetencji w języku angielskim jest istotnym elementem kształcenia będącym odpowiedzią na potrzeby otoczenia społeczno-gospodarczego, oraz gotowość do ich pogłębiania wraz z narastającą złożonością świata. Na poziomie uczelni dostępne są programy szkoleniowe dotyczące kompetencji językowych jak i programy wymiany akademickiej. Na kierunku prowadzone są lektoraty, głównie z języka angielskiego.

W ostatnich latach na kierunku cyberbezpieczeństwo powstało 5 prac dyplomowych napisanych w języku angielskim, z czego 4 na studiach pierwszego stopnia, a 1 na studiach drugiego stopnia.

Uczelnia posiada ofertę dydaktyczną w języku angielskim. Zajęcia do wyboru prowadzone w języku angielskim na kierunku cyberbezpieczeństwo, np. to: adaptive image recognition, introduction to artificial intelligence, czy data mining.

Pracownicy pracują w ramach projektów międzynarodowych, co również wpływa na zwiększenie umiędzynarodowienia procesu kształcenia na kierunku.

Monitorowanie wymiany studentów na Wydziale Elektroniki i Technik Informacyjnych należy do obowiązków Pełnomocnika Dziekana ds. międzynarodowej wymiany studentów. Corocznie sporządzane są zestawienia prezentowane na Radzie Wydziału i zamieszczane w Sprawozdaniu Dziekana. Wnioski płynące z zestawień obejmujące ocenę skali, zakresu i zasięgu aktywności służą do doskonalenia i intensyfikacji umiędzynarodowienia kształcenia. Prowadzone są spotkania informacyjne ze studentami, na których przedstawiane są dostępne na Wydziale możliwości wyjazdów na studia i praktyki zagraniczne oraz opinie wyjeżdżających.

**Zalecenia dotyczące kryterium 7 wymienione w uchwale Prezydium PKA w sprawie oceny programowej na kierunku studiów, która poprzedziła bieżącą ocenę (jeśli dotyczy)**

**(Ocenę realizacji zaleceń należy uwzględnić w ocenie spełnienia kryterium, mając na uwadze postanowienia ust. 4 pkt 2 zał. nr 3 do Statutu PKA)**

| Lp. | Zalecenia dotyczące kryterium 7 wymienione we wskazanej wyżej uchwale Prezydium PKA | Opis realizacji zalecenia | Ocena realizacji zalecenia<br>(zalecenie zrealizowane /<br>zalecenie niezrealizowane) |
|-----|-------------------------------------------------------------------------------------|---------------------------|---------------------------------------------------------------------------------------|
| 1.  | Nie dotyczy                                                                         | Nie dotyczy               | Nie dotyczy                                                                           |

#### **Propozycja oceny stopnia spełnienia kryterium 7**

Kryterium spełnione

#### **Uzasadnienie**

Rodzaj, zakres i zasięg umiędzynarodowienia procesu kształcenia są zgodne z koncepcją i celami kształcenia na kierunku cyberbezpieczeństwo. Stwarzane są również możliwości rozwoju międzynarodowej aktywności nauczycieli akademickich i studentów związanej z kształceniem na kierunku.

W ramach ocenianego kierunku prowadzone są okresowe oceny stopnia umiędzynarodowienia kształcenia, obejmujące ocenę skali, zakresu i zasięgu aktywności międzynarodowej kadry i studentów, a wyniki tych przeglądów są wykorzystywane do intensyfikacji umiędzynarodowienia kształcenia.

**Dobre praktyki, w tym mogące stanowić podstawę przyznania uczelni Certyfikatu Doskonałości Kształcenia**

---

#### **Rekomendacje**

---

#### **Zalecenia**

---

**Kryterium 8. Wsparcie studentów w uczeniu się, rozwoju społecznym, naukowym lub zawodowym i wejściu na rynek pracy oraz rozwój i doskonalenie form wsparcia**

#### **Analiza stanu faktycznego i ocena spełnienia kryterium 8**

Studenci kierunku cyberbezpieczeństwo realizowanego na Wydziale Elektroniki i Technik Informatycznych Politechniki Warszawskiej mają zapewnione stałe, systematyczne oraz kompleksowe wsparcie w procesie uczelnią się. Przybiera ono zróżnicowane formy i jest adekwatne do realizowanego profilu kształcenia. Jest również dostosowane do różnych grup odbiorców.

Studentom są przedstawiane obowiązujące zasady realizowania oraz zaliczania przedmiotów. Zasady te są również dostępne do wglądu na platformie USOS. Uczelnia zapewnia studentom merytoryczne oraz materialne wsparcie, zarówno w działalności naukowej, jak i organizacyjnej. Osobą będącą wsparciem dla studentów jest Kierownik Kierunku oraz dyrektorzy ds. nauczania w każdym z instytutów. Osoby te, w szczególności Kierownik, zaangażowane są w różnego rodzaju spotkania informacyjne, rozwiązywanie problemów, opiniowanie dokumentów itp. Osoby studiujące mają możliwość korzystania z infrastruktury oraz oprogramowania w czasie zajęć oraz poza ich godzinami. Uwzględnia to również dostęp do infrastruktury niezbędnej do wykorzystania na studiowanym kierunku. Studenci jako plus kierunku wskazują z informatyzowanie dużej ilości procesów, które ich dotyczą. Dzięki bibliotece zapewniony jest również dostęp do bibliografii wskazywanej w sylabusach przedmiotów. Wszyscy studenci w pierwszym roku studiów uczestniczą w obowiązkowym szkoleniu bibliotecznym oraz szkoleniu BHP. Dodatkowo na zajęciach wymagających szczególnego bezpieczeństwa udzielany jest instruktaż stanowiskowy. Na wydziale oraz w uczelni funkcjonują koła naukowe oraz organizacje studenckie, które umożliwiają studentom rozwój na różnych płaszczyznach. Koła naukowe cieszące się zainteresowaniem wśród studentów cyberbezpieczeństwa to m.in. Koło Cyberbezpieczeństwa oraz Koło Bezpieczeństwa Informatyki. Mają one zapewnione wsparcie infrastrukturalne. Uczelnia nierzadko zapewnia materialne wsparcie w działalności naukowej, finansując udziały w warsztatach, projektach, konkursach seminariach i konferencjach. Studenci mogą brać udział w programach wymiany międzynarodowej.

Ważnym celem indywidualnej formy studiów jest rozwijanie osobistych zainteresowań naukowych studentów wykazujących szczególne uzdolnienia oraz przygotowanie ich do pracy naukowej lub dydaktycznej. Cele powyższe mogą być osiągnięte dzięki oferowanym przez m.in. Centrum Studiów Zaawansowanych, Centrum Zarządzania Innowacjami i Transferem Technologii szkoleniom i warsztatom. Na uczelni funkcjonuje również Biuro Karier, wspierające studentów w znalezieniu pracy, wolontariatu, stażu czy praktyk oraz oferuje warsztaty i różnego rodzaju wsparcie m.in. w zakresie doradztwa zawodowego. Proces realizacji praktyk wspiera pracownik do tego wyznaczony przez Dziekana oraz 6 innych, po jednej w każdym instytucie. Istnieje możliwość rozwoju swoich zainteresowań za pomocą budżetu partycypacyjnego, akcji charytatywnych, krwiodawstwa, szlachetnej paczki itp. Na Uczelni oprócz działania kół naukowych odpowiadających za wsparcie rozwoju naukowego, działają również takie organizacje studenckie jak m.in. Akademicki Związek Sportowy, Chór Politechniki Warszawskiej, Zespół Tańca oraz Akademicki Klub Turystyczny "Maluch". Mogą one liczyć na wsparcie zarówno infrastrukturalne, jak i finansowe oraz organizacyjne.

Oferowane wsparcie jest dostosowane do potrzeb różnych grup studentów. Grupą, do której należy większość studentów kierunku, są osoby pracujące zawodowo. Mają one możliwość swobodnego studiowania i jednoczesnej pracy. Ułatwieniem jest w tym wypadku możliwość wpłynięcia na zmiany w harmonogramie zajęć, ustalenia indywidualnego terminu konsultacji, czy

zawnioskowanie o indywidualizację procesu kształcenia. Na wsparcie poprzez m.in. elastyczne terminy zaliczeń, czy zapomogi mogą liczyć również studenci będący rodzicami. Wszyscy studenci PW mogą ubiegać się o zakwaterowanie w domach studenckich PW. W Uczelni działa Biuro ds. Społecznej Odpowiedzialności Uczelni, w skład której wchodzi Sekcja ds. Osób z niepełnosprawnościami. Studenci z niepełnosprawnościami mogą liczyć m.in. na wsparcie opiekuna osoby z niepełnosprawnością oraz w nieskrępowany sposób korzystać z infrastruktury Uczelni, w tym z komputerów specjalnie dostosowanych do ich potrzeb. W Uczelni funkcjonują również Wydziałowi Pełnomocnicy ds. Osób z Niepełnosprawnościami. Studenci z niepełnosprawnościami mogą również ubiegać się o stypendium dla osób niepełnosprawnych. Studenci znajdujący się w trudnej sytuacji mogą ubiegać się o stypendium socjalne oraz o zapomogi. Cały proces stypendialny, obejmujący wszystkie rodzaje stypendiów, jest dla studentów zrozumiały i działa prawidłowo.

Skargi i wnioski mogą być zgłaszane do samorządu studenckiego, władz dziekańskich, komisji dyscyplinarnych, prorektora ds. studenckich oraz rzeczników zaufania. W przypadku gdy student nie zgadza się z decyzją, istnieje możliwość odwołania się do JM Rektora. Głównym sposobem zgłoszeń jest bezpośredni kontakt studentów z pracownikami uczelni. Dzięki temu, że jest on wypracowany w perspektywie wielu lat, działa poprawnie. Przykładami problematycznego wniosku studentów było zgłoszenie powtarzającego się problemu z jednym z nauczycieli. Po wielu rozmowach i próbach rozwiązania problemu podjęto decyzję o rozwiązaniu stosunku pracy pomiędzy Uczelnią i nauczycielem akademickim. W Uczelni przyjęto również politykę przeciwdziałania mobbingowi i dyskryminacji, która określa rolę oraz zakres działania wspomnianych rzeczników zaufania. Funkcjonuje również pełnomocnik ds. równego traktowania.

Dostępne jest również nieodpłatne wsparcie psychologiczne. Studenci potwierdzają, że informacja o oferowanym wsparciu psychologicznym jest im skutecznie przekazywana na wiele różnych sposobów, takich jak m.in. ekrany na korytarzach, plakaty oraz mailing. Warto zauważyć jednak, że podnoszony jest temat panującego chaosu w wykorzystywanych platformach edukacyjnych i informacyjnych. W szczególności studenci pierwszego roku wskazują występujący problem z odnalezieniem się wśród dużej liczby niepowiązanych ze sobą stron internetowych. Studenci kierunku podają też jako przykład dużą liczbę platform edukacyjnych, na których prowadzony jest kierunek (np. USOS, LeOn, Moodle, MS Teams). Powoduje to częściowy problem z efektywnym przekazywaniem części istotnych informacji. W związku z tym rekomenduje się weryfikację oraz uporządkowanie treści i sposobów ich przekazywania w celu prostszego i efektywniejszego dostępu do nich. Na wydziale funkcjonuje również prodziekan ds. studenckich, który odpowiedzialny jest za sprawy studenckie. Poprzez współpracę z placówkami medycznymi, studenci mają ułatwiony dostęp do opieki medycznej.

Do działań motywujących studentów do lepszych i wybitnych wyników w nauce można bez wątplenia zaliczyć szereg wspomnianych już stypendiów, możliwości zróżnicowanego rozwoju swoich pasji i zainteresowań. To na co warto zwrócić uwagę, to aspekty, które wskazują sami studenci. Są to między innymi panująca na wydziale atmosfera oraz system priorytetowego zapisu na zajęcia. Uczelnia dla studentów osiągających bardzo dobre i wybitne wyniki w nauce funduje nagrody i wyróżnienia.

Jednostką administracyjną odpowiedzialną za obsługę spraw studenckich jest dziekanat studencki oraz sekretariaty instytutów. Wśród pracowników są osoby posługujące się językami

obcymi, co pozwala na efektywną obsługę studentów z zagranicy. Załatwianie spraw dostępne jest zarówno w formie zdalnej, jak i stacjonarnej. Pracownicy uczelni mają możliwość udziału w szkoleniach doskonalących ich poziom współpracy ze studentami. Za zdalną obsługę odpowiada system USOS. Studenci mogą korzystać z konsultacji oferowanych przez nauczycieli akademickich. Ich forma i terminy są ustalane przez prowadzących, jednak istnieje możliwość dostosowania ich do potrzeb różnych grup studentów. Osoby studiujące mogą liczyć na stałe wsparcie wszystkich pracowników uczelni. Doceniają stworzoną atmosferę, która sprzyja efektywnemu studiowaniu. Jednostki Uczelni odpowiadające za wsparcie osób studiujących działają poprawnie i spełniają swoją funkcję.

Na poziomie Uczelni oraz Wydziału funkcjonuje samorząd studencki. Spełnia on ustawowe zadania, reprezentując społeczność studencką na forum Uczelni i Wydziału, odpowiadając za sprawy socjalno-bytowe studentów, projektowanie i opiniowanie programu studiów oraz dbając o integrację środowiska studenckiego. Wydziałowa Rada Samorządu ma zapewnione finansowanie. Samorząd posiada do swojej dyspozycji zaplecze infrastrukturalne. Członkowie samorządu są obecni i biorą udział w pracach gremiów zapewniających jakość kształcenia oraz kształtujących wydział i uczelnię potwierdzając, że biorą czynny udział w pracach nad programem studiów. Wydziałowa Rada Samorządu ściśle współpracuje z władzami wydziału. Ocenia tę współpracę pozytywnie. Ponadto wspólnie realizują wiele inicjatyw studenckich. Na pierwszym semestrze studiów studenci uczestniczą w organizowanych przez Wydziałową Radę Studentów szkoleniach z praw i obowiązków studenta oraz z ogólnych informacji dot. studiów i studiowania. W opinii zarówno władz wydziału, jak i studentów kierunku, Wydziałowa Rada Studentów jest aktywna i efektywnie pracuje na rzecz dobra studentów.

Uczelnia przeprowadza anonimową ankietyzację ewaluującą zajęcia dydaktyczne. Studenci mają możliwość ocenić m.in. kwestie organizacyjne dotyczące zajęć, materiałów dydaktycznych, czy przygotowania prowadzącego do zajęć. Uczelnia przeprowadza cykliczne badanie #powiedzPW, które w każdej kolejnej edycji porusza inny obszar studiowania. Badanie prowadzone jest w formie ankiety online. Raport z opracowanymi wynikami w formie infografik publikowany jest na stronie internetowej uczelni. Kolejnym cyklicznym badaniem, jest ankieta dotycząca pracy dziekanatu. Wykonywane są również inne, zróżnicowane tematycznie, doraźne badania. Co roku ankietowani są również studenci pierwszego roku pod kątem ich motywacji i uwarunkowań przy wyborze kierunku. Pozostałe sposoby badania skuteczności systemu wsparcia studentów są sposobami nieformalnymi, wypracowanymi na podstawie wieloletniej współpracy pomiędzy studentami a Uczelnią. Polegają na licznych spotkaniach oraz konsultacjach studentów, samorządu, władz dziekańskich, Kierownika Kierunku. Studenci dostrzegają zmiany wprowadzane na podstawie prowadzonych badań wsparcia studentów w procesie uczenia się. Przykładem zmian jest wydłużenie godzin otwarcia jednego z wejść do budynku oraz zwiększenie liczby godzin z matematyki na kierunku.

**Zalecenia dotyczące kryterium 8 wymienione w uchwale Prezydium PKA w sprawie oceny programowej na kierunku studiów, która poprzedziła bieżącą ocenę (jeśli dotyczy)**

*(Ocenę realizacji zaleceń należy uwzględnić w ocenie spełnienia kryterium, mając na uwadze postanowienia ust. 4 pkt 2 zał. nr 3 do Statutu PKA)*



| Lp. | Zalecenia dotyczące kryterium 8 wymienione we wskazanej wyżej uchwale Prezydium PKA | Opis realizacji zalecenia | Ocena realizacji zalecenia<br>(zalecenie zrealizowane / zalecenie niezrealizowane) |
|-----|-------------------------------------------------------------------------------------|---------------------------|------------------------------------------------------------------------------------|
| 1.  | <b>Nie dotyczy</b>                                                                  | <b>Nie dotyczy</b>        | <b>Nie dotyczy</b>                                                                 |

### Propozycja oceny stopnia spełnienia kryterium 8

kryterium spełnione

### Uzasadnienie

Wsparcie studentów kierunku cyberbezpieczeństwo przybiera zróżnicowane formy. Jest realizowane w sposób uwzględniający wsparcie oraz dostosowanie do różnych grup studentów. Sprzyja rozwojowi naukowemu, społecznemu i zawodowemu oraz stosuje narzędzia motywujące i zachęcające studentów do ciągłego rozwoju oraz uzyskiwania bardzo dobrych wyników w nauce. Daje możliwość rozwoju zainteresowań oraz pasji poprzez działalność w kołach naukowych, organizacjach i samorządzie studenckim. Udostępnia specjalistyczną infrastrukturę pozwalającą na ciągły rozwój studentów. Pomaga w wejściu na rynek pracy. Samorząd studencki, koła naukowe oraz różnego rodzaju organizacje studenckie mają zapewnione wsparcie zarówno finansowe, jak i organizacyjne i infrastrukturalne.

Wsparcie studentów w procesie uczenia się jest badane, a pozyskiwane od studentów informacje są wykorzystywane w działaniach doskonalących.

### Dobre praktyki, w tym mogące stanowić podstawę przyznania uczelni Certyfikatu Doskonałości Kształcenia

---

### Rekomendacje

1. Rekomenduje się weryfikację oraz uporządkowanie treści i sposobów ich przekazywania w wykorzystywanych platformach edukacyjnych i informacyjnych w celu prostszego i efektywniejszego dostępu do nich.

### Zalecenia

---

### Kryterium 9. Publiczny dostęp do informacji o programie studiów, warunkach jego realizacji i osiągniętych rezultatach

#### Analiza stanu faktycznego i ocena spełnienia kryterium 9

Uczelnia prowadząca kierunek zapewnia publiczny dostęp do aktualnej i kompleksowej informacji o programie studiów i warunkach jego realizacji, posiada kilka oficjalnych stron

internetowych. Są to m.in. główna strona uczelni, Biuletyn Informacji Publicznej, strona wydziału, czy strona kierunku. Wszystkie stanowią przestrzeń do uzyskania informacji o uczelni oraz prowadzonych przez nią studiach. Strony zapewniają dostęp do informacji dla szerokiego grona odbiorców, który jest niezależny od miejsca, czasu, używanego rodzaju sprzętu czy oprogramowania. Oznacza to, że informacje udostępniane w witrynach internetowych mogą być wyświetlane na różnych urządzeniach, przy użyciu różnych przeglądarek, bez konieczności logowania oraz w dowolnym miejscu i o dowolnej porze. W większości dostępne są w języku polskim i angielskim. Aktualnie, witryny są w przebudowie i reorganizacji, wprowadzając m.in. dostosowania dla osób z niepełnosprawnościami, czy migrowanie treści pomiędzy stronami w celu ujednolicenia. Należy jednak zauważyć, że zakres dostosowania strony do osób ze specjalnymi potrzebami jest minimalny i nie występuje we wszystkich wymienionych stronach. Dlatego rekomenduje się dostosowanie wszystkich stron Uczelni do wymogów pozwalających na nieskrępowane używanie ich przez osoby ze specjalnymi potrzebami.

Uczelnia na prowadzonych stronach przedstawia informacje dotyczące Politechniki Warszawskiej, wydziałów oraz kierunku cyberbezpieczeństwo. Na stronach można znaleźć wszystkie podstawowe informacje o studiach, takie jak najważniejsze akty prawne obowiązujące w uczelni, program studiów z wszystkimi wymaganymi elementami, m.in. efektami uczenia się. Strony zawierają istotne dla studenta informacje dotyczące wsparcia w procesie uczenia się oraz innych informacji dotyczących studiowania jak informacje o kołach naukowych i organizacjach studenckich, mobilności studenckiej, konkursach oraz aktualnościach. Strona główna zapewnia ciągły i kompleksowy dostęp do informacji dla kandydatów, takich jak m.in. program studiów, cel kształcenia, czy zasady rekrutacji. Publikacje obejmują również tematykę dotyczącą i dedykowaną dla absolwentów oraz dotyczącą współpracy z otoczeniem społeczno-gospodarczym. Osoby zainteresowane dalszym kształceniem się, mogą zapoznać się z ofertą studiów pierwszego i drugiego stopnia, studiów podyplomowych oraz Szkoły Doktorskiej. Zapewniony jest swobodny dostęp dla interesariuszy wewnętrznych oraz zewnętrznych. Strona internetowa wydziału prowadzącego kierunek posiada dedykowane podstrony, dotyczące nawiązanych już współprac, ale także możliwości ich nawiązania. Dostępne są dane kontaktowe do jednostek Uczelni. Należy jednak zwrócić uwagę na istotną kwestię, jaką jest niespójność. Wszystkie wymienione strony funkcjonują niezależnie od siebie i często nie odwołują się do siebie nawzajem. Utrudnia to znacznie poruszanie się po nich i znalezienie pożądanej informacji. Niektóre z informacji znajdują się np. na stronie głównej Uczelni, a niektóre na stronie Wydziału czego nie dostrzega się intuicyjnie, ponieważ strony niewspółpracują sobą. Wszystkie strony różnią się również w aspektach wizualnych. Każda z nich jest zaprojektowana inaczej. W celu poprawy jakości i ułatwienia dostępu do informacji publicznej rekomenduje się wprowadzenie współpracy pomiędzy wykorzystywanymi platformami internetowymi oraz ich ujednolicenie. Informacje udostępniane są również za pomocą mediów społecznościowych, takich jak Facebook.

Uczelnia monitoruje aktualność, rzetelność, zrozumiałość, kompleksowość informacji o studiach oraz jej zgodności z potrzebami odbiorców głównie poprzez spotkania i rozmowy zarówno w gremiach uczelnianych, jak i podczas mniej oficjalnych spotkań. Uwagi z grona społeczności akademickiej najczęściej zgłaszane są do przedstawicieli wybranych grup oraz do wybranych pracowników uczelni. Dodatkowo uwagi dotyczące dostępu do informacji publicznej mogą być przekazywane poprzez przeprowadzane na Uczelni badania i ankiety. Zarządzaniem

stroną internetową na poziomie Uczelni zajmuje się Biuro Promocji i Informacji. Strony na poziomie Wydziału prowadzą pracownicy Wydziału.

**Zalecenia dotyczące kryterium 9 wymienione w uchwale Prezydium PKA w sprawie oceny programowej na kierunku studiów, która poprzedziła bieżącą ocenę (jeśli dotyczy)**

| Lp. | Zalecenia dotyczące kryterium 9 wymienione we wskazanej wyżej uchwale Prezydium PKA | Opis realizacji zalecenia | Ocena realizacji zalecenia<br>(zalecenie zrealizowane /<br>zalecenie niezrealizowane) |
|-----|-------------------------------------------------------------------------------------|---------------------------|---------------------------------------------------------------------------------------|
| 1.  | <b>Nie dotyczy</b>                                                                  | <b>Nie dotyczy</b>        | <b>Nie dotyczy</b>                                                                    |

**Propozycja oceny stopnia spełnienia kryterium 9**

Kryterium spełnione

**Uzasadnienie**

Uczelnia zapewnia publiczny dostęp do informacji o studiach. Jest on zapewniony w bardzo szerokim zakresie tematycznym, uwzględniając informacje przeznaczone dla wszystkich grup interesariuszy, w tym kandydatów na studia, społeczności akademickiej oraz interesariuszy zewnętrznych. Udostępniane informacje, jak i wykorzystywane witryny nie są w żadnym stopniu ograniczone czasem, miejscem, używanym sprzętem czy oprogramowaniem.

Informacje o studiach obejmują szeroki zakres tematyczny. Dostępny do wglądu jest program studiów ze wszystkimi niezbędnymi informacjami, informacje dla kandydatów tj. terminarz rekrutacji oraz zasady rejestracji na studia, informacje i aktualności dla społeczności akademickiej, informacje o wsparciu studentów w procesie uczenia się, informacje o współpracach oraz możliwości ich nawiązania dedykowane dla interesariuszy zewnętrznych.

Zakres przedmiotowy i jakość informacji o studiach poddawany jest działaniom monitorującym pod względem jego aktualności, rzetelności, zrozumiałości, kompleksowości informacji o studiach oraz jego zgodności z potrzebami różnych grup odbiorców. Dostrzega się obszary wymagające poprawy, jednak nie są to błędy wpływające na ocenę stopnia spełnienia kryterium.

**Dobre praktyki, w tym mogące stanowić podstawę przyznania uczelni Certyfikatu Doskonałości Kształcenia**

---

**Rekomendacje**

1. Rekomenduje się dostosowanie wszystkich stron Uczelni do wymogów pozwalających na nieskrępowane używanie ich przez osoby ze specjalnymi potrzebami.
2. Rekomenduje się wprowadzenie współpracy pomiędzy wykorzystywanymi platformami internetowymi oraz ich ujednolicenie.

## Zalecenia

---

### **Kryterium 10. Polityka jakości, projektowanie, zatwierdzanie, monitorowanie, przegląd i doskonalenie programu studiów**

#### **Analiza stanu faktycznego i ocena spełnienia kryterium 10**

W Politechnice Warszawskiej funkcjonuje Uczelniany System Zapewnienia Jakości Kształcenia (USZJK). Działania prowadzone w zakresie jakości kształcenia na kierunku cyberbezpieczeństwo są zgodne z aktualną Strategią Rozwoju Uczelni oraz wytycznymi Strategii Bolońskiej i opierają się o przepisy prawa, regulacje wewnętrzne oraz rekomendacje dotyczące jakości kształcenia zawarte w Standardach i Wskazówkach Dotyczących Jakości Kształcenia w Europejskim Obszarze Szkolnictwa Wyższego. Jakość kształcenia na Wydziale Elektroniki i Technik Informatycznych PW, odpowiedzialnego za realizację kształcenia na kierunku cyberbezpieczeństwo, jest zapewniana i weryfikowana z wykorzystaniem wewnętrznego Systemu Zapewniania i Doskonalenia Jakości Kształcenia. Głównym dokumentem definiującym USZJK na Wydziale EiTI jest Księga Jakości Kształcenia Wydziału Elektroniki i Technik Informatycznych Politechniki Warszawskiej, przyjęta Uchwałą Rady Wydziału. Księga ta była aktualizowana w 2022r., a obecnie trwają prace nad jej kolejną aktualizacją uwzględniającą uwagi zawarte w raporcie oceny PKA innego kierunku prowadzonego na Wydziale.

Zarówno na poziomie Uczelni jak i na poziomie Wydziału Elektroniki i Technik Informatycznych wyznaczone zostały ciała odpowiedzialne za nadzór nad działalnością edukacyjną oraz zapewnienie i doskonalenie jakości kształcenia. Na poziomie Uczelni za sprawy związane z kształceniem i zapewnieniem jakości kształcenia odpowiada Prorektor ds. Studiów, Komisja Senacka ds. Kształcenia, Uczelniana Rada ds. Jakości Kształcenia oraz Pełnomocnik ds. Jakości Kształcenia i Akredytacji, którego zadania obejmują: podejmowanie działań o charakterze koncepcyjnym i organizacyjnym oraz koordynacja przedsięwzięć zmierzających do zapewniania i podnoszenia jakości studiów; koordynowanie działań w ramach systemu akredytacji; przedstawianie propozycji i wniosków związanych z funkcjonowaniem systemu zapewniania jakości studiów; współdziałanie z jednostkami organizacyjnymi Uczelni w zakresie wprowadzania systemu jakości. Główny nadzór nad procesami dotyczącymi jakości kształcenia na Wydziale sprawuje Dziekan i Prodziekani, ds. nauczania oraz ds. studiów, a także pełnomocnicy Dziekana ds. Wydziałowego Systemu Zapewniania Jakości Kształcenia. Zadaniem Pełnomocnika jest inspirowanie i koordynowanie działań mających na celu podnoszenie poziomu kształcenia na Wydziale. Pełnomocnik odpowiada za wdrażanie i realizację Wydziałowego Systemu Zapewniania Jakości Kształcenia. Ponadto w działania te zaangażowani są dyrektorzy instytutów, a zwłaszcza kierownicy zakładów odpowiedzialni za właściwy poziom i rozwój kształcenia oraz ustalanie obsady zajęć dydaktycznych. Wewnętrzny System Zapewnienia Jakości Kształcenia jest więc zdefiniowany formalnie, a jego struktura i zakresy odpowiedzialności są określone prawidłowo.

Zatwierdzanie, zmiany oraz wycofanie programu studiów dokonywane jest na Uczelni w sposób formalny, w oparciu o oficjalnie przyjęte procedury zawarte w uchwałach Senatu i zarządzeniach rektora (w tym: uchwała Senatu PW nr 58/L/2020 w sprawie ustalania programów studiów w Politechnice Warszawskiej oraz zarządzenie Rektora PW nr 158/2020 w sprawie procedury

tworzenia studiów, zaprzestania prowadzenia studiów oraz procedury wprowadzania zmian w programie studiów). Procesy te inicjowane są przez Dziekana Wydziału, który składa wniosek o zmiany za pośrednictwem Działu ds. Studiów, po zaopiniowaniu przez Radę Wydziału (ciało opiniodawczo-doradcze Dziekana), a także przez Wydziałową Komisję ds. Jakości Kształcenia i WRS. Rektor kieruje wniosek wraz projektem zmian do Senackiej Komisji ds. Kształcenia (opinia wniosku pod kątem formalnym). Zmiany zostają zatwierdzone podczas posiedzenia Senatu w formie uchwały.

Przyjęcie na studia odbywa się w oparciu o formalnie przyjęte warunki i kryteria kwalifikacji kandydatów, zatwierdzane corocznie uchwałą Senatu. Szczegółowe zasady rekrutacji na studia w roku ak. 2024/2025 określa Uchwała nr 393/L/2023 z dnia 28/06/2023 w sprawie warunków i trybu rekrutacji na studia jednolite magisterskie oraz studia pierwszego i drugiego stopnia, profili kształcenia oraz form tych studiów na poszczególnych kierunkach, prowadzonych w roku akademickim 2024/2025. Rekrutacja na studia pierwszego stopnia jest realizowana na podstawie wyniku egzaminu maturalnego z odpowiednio przypisanymi wagami dla przedmiotów i poziomów matury. Przyjęcia na studia drugiego stopnia przeprowadzane są na podstawie rankingu, przy czym kandydaci kończący ten sam kierunek przyjmowani są na podstawie wyników ukończonych studiów I stopnia, a dla pozostałych przeprowadzana jest ocena kompetencji w odniesieniu do wymagań wynikających z programu studiów I stopnia. Ponadto w przypadku nadmiaru kandydatów w stosunku do liczby miejsc 80% przyjętych na studia na kierunek cyberbezpieczeństwo mogą to być osoby kończące ten sam kierunek na poziomie I stopnia na tym samym wydziale. Rekomenduje się więc ustalenie jednolitych zasad przyjęcia na studia II stopnia dla wszystkich kandydatów.

Zasady monitorowania i doskonalenia programu studiów określone są w przepisach wewnętrznych Uczelni. Ocena procesu kształcenia oraz uzyskiwanych efektów uczenia się prowadzona jest na wielu poziomach. Program kształcenia monitorowany jest na bieżąco przez Komisję ds. Kształcenia oraz kierowników kierunku. Komisja ds. Kształcenia kontroluje także, czy ewentualne zmiany na innych prowadzonych kierunkach nie stwarzają konieczności lub możliwości zmian w programie danych studiów. Kluczową funkcję w ocenie programu studiów pełnią osoby prowadzące zajęcia i kierownicy poszczególnych zajęć, a także opiekunowie specjalności i kierunku. Ocena taka wykonywana jest także dla wybranych zajęć i przedmiotów przez Prodziekana ds. Nauczania (np. z inicjatywy kierownika jednostki i/lub studentów). Analizie poddawane są np. analizy ocen w tym prac etapowych i końcowych, informacje płynące z otoczenia społeczno-gospodarczego, w tym systematyczne badania rynku pracy i karier absolwentów, a także opinie studentów i nauczycieli akademickich. Przedstawiciele studentów są także statymi członkami komisji dziekańskich i Rady Wydziału. Pracownicy mogą zgłaszać wnioski do kierowników zakładów lub Komisji ds. Jakości Kształcenia. Opinie i uwagi pochodzące od interesariuszy zewnętrznych zdobywane są głównie poprzez kontakty nieformalne. Informacja zwrotna o programie wykorzystywana w ocenie i doskonaleniu programu studiów pozyskiwana jest także od absolwentów kierunku cyberbezpieczeństwo. Zespół oceniający PKA zidentyfikował jednak niedociągnięcia w zakresie sposobu zdefiniowania efektów uczenia się, w szczególności w odniesieniu do stopnia zaawansowania i głębi wiedzy zdobywanej i umiejętności osiągniętych na kierunku cyberbezpieczeństwo na obu stopniach studiów. Ponadto wskazany jest przegląd i aktualizacja kart przedmiotów (szczególnie na studiach drugiego stopnia), tak aby liczba godzin realizowanych z bezpośrednim udziałem nauczycieli akademickich i przyporządkowana liczba im liczba

punktów ECTS była wskazana we wszystkich kartach. Pewne niedociągnięcia zauważono również w procesie kierowania na praktykę, gdzie np. w treści umów podpisywanych z przyjmującym na praktykę brakuje zdefiniowanych oczekiwań (programu praktyki) w zakresie realizowanych efektów uczenia się dla studenta. Rekomenduje się więc podjęcie działań poprawiających skuteczność systemu zapewnienia jakości kształcenia w zakresie monitorowania programu studiów, w szczególności w odniesieniu do dokumentacji kierunku.

Monitorowanie programu studiów jest dokonywane również poprzez ankietyzację i hospitację zajęć. Ankietyzacji poddawane są wszystkie zajęcia prowadzone w danym semestrze, a wyniki wykorzystywane są przez władze wydziału w sposób motywujący nauczycieli do wprowadzania korzystnych zmian w sposobie realizacji zajęć. Podczas hospitacji ocenie podlega m.in. zgodność treści zajęć z programem zajęć, realizacja założonych efektów uczenia się na zajęciach, dobór i wykorzystywanie środków dydaktycznych. Monitorowanie procesu dyplomowania przejawia się podczas wyznaczania opiekunów prac dyplomowych i ich recenzentów oraz sprawdzania prac dyplomowych pod kątem spełniania przez nich wymagań określonych dla każdego poziomu studiów. W wyniku analizy przeprowadzonego procesu ankietyzacji ciągłej weryfikacji poddawany jest m.in. program studiów. W efekcie konsultacji ze studentami wprowadzono np. modyfikacje w przedmiotach matematycznych (Matematyka 1-4), co pozytywnie wpłynęło na możliwość prawidłowego przyswojenia materiału dydaktycznego przez studentów.

W ramach funkcjonowania wewnętrznego systemu zapewnienia jakości kształcenia prowadzone jest także monitoring infrastruktury i zasobów wykorzystywanych w procesie dydaktycznym. Zidentyfikowano jednak pewne niedociągnięcia w tym zakresie, w szczególności dotyczące niezbyt czytelnego sposobu przekazywania treści w wykorzystywanych platformach edukacyjnych i informacyjnych, a także niedostatecznego dostosowania wszystkich stron internetowych Uczelni do wymogów osób ze specjalnymi potrzebami. Rekomenduje się więc podjęcie działań poprawiających skuteczność systemu zapewnienia jakości kształcenia w zakresie monitorowania infrastruktury i zasobów wykorzystywanych w procesie dydaktycznym, w szczególności uproszczenia i ujednolicenia dostępu do informacji zawartych w różnych platformach cyfrowych Uczelni i efektywniejszego dostępu do nich.

Jakość kształcenia na kierunku jest nie była poddawana dotychczas zewnętrznej ocenie (kierunek uruchomiono w 2019 r), ale wyniki ocen Polskiej Komisji Akredytacyjnej przeprowadzonych na innych kierunkach są wykorzystywane w doskonaleniu jakości kształcenia na kierunku cyberbezpieczeństwo. Ostatnie takie modyfikacje w programie studiów kierunku cyberbezpieczeństwo wprowadzono w 2020r. dla studiów pierwszego stopnia, a w 2024 r. dla studiów drugiego stopnia.

#### **Zalecenia dotyczące kryterium 10 wymienione w uchwale Prezydium PKA w sprawie oceny programowej na kierunku studiów, która poprzedziła bieżącą ocenę (jeśli dotyczy)**

*(Ocenę realizacji zaleceń należy uwzględnić w ocenie spełnienia kryterium, mając na uwadze postanowienia ust. 4 pkt 2 zał. nr 3 do Statutu PKA)*

| Lp. | Zalecenia dotyczące kryterium 10 wymienione we wskazanej wyżej uchwale Prezydium PKA | Opis realizacji zalecenia | Ocena realizacji zalecenia<br>(zalecenie zrealizowane / |
|-----|--------------------------------------------------------------------------------------|---------------------------|---------------------------------------------------------|
|-----|--------------------------------------------------------------------------------------|---------------------------|---------------------------------------------------------|



|    |                    |                    |                                       |
|----|--------------------|--------------------|---------------------------------------|
|    |                    |                    | <i>zalecenie<br/>niezrealizowane)</i> |
| 1. | <b>Nie dotyczy</b> | <b>Nie dotyczy</b> | <b>Nie dotyczy</b>                    |

### Propozycja oceny stopnia spełnienia kryterium 10

Kryterium spełnione

#### Uzasadnienie

Uczelnia zapewnia nadzór merytoryczny, organizacyjny i administracyjny nad kształceniem prowadzonym na kierunku cyberbezpieczeństwo. Zakres odpowiedzialności poszczególnych osób sprawujących nadzór nad kierunkiem, w tym zakres odpowiedzialności za zapewnienie i doskonalenie jakości kształcenia został w sposób przejrzysty określony.

Zatwierdzanie i zmiany programu studiów oraz przyjęcie na studia odbywają się w oparciu o formalnie określone zasady. Prowadzona jest ocena programu studiów w oparciu o spostrzeżenia interesariuszy procesu kształcenia, w szczególności kierowników zajęć oraz wyniki nauczania, a wyniki tej oceny prowadzą do doskonalenia programu. W ocenie programu studiów biorą udział interesariusze wewnętrzni (nauczyciele akademicki oraz studenci), a także zewnętrzni (pracodawcy i absolwenci). Uczelniany System Zapewnienia Jakości Kształcenia ma charakter dojrzały, a jednocześnie podlega ciągłemu doskonaleniu z aktywnym udziałem interesariuszy wewnętrznych i zewnętrznych.

#### Dobre praktyki, w tym mogące stanowić podstawę przyznania uczelni Certyfikatu Doskonałości Kształcenia

---

#### Rekomendacje

Rekomenduje się podjęcie działań poprawiających skuteczność systemu zapewnienia jakości kształcenia w zakresie ujednolicenia zasad rekrutacji na studia drugiego stopnia, monitorowania programu studiów, w szczególności dokumentacji kierunku, a także monitorowania infrastruktury i zasobów wykorzystywanych w procesie dydaktycznym, w szczególności w zakresie dostępu do informacji zawartych w różnych platformach cyfrowych Uczelni.

#### Zalecenia

---