Uchwała nr 5.26.06.2023
Senatu Uniwersytetu Pedagogicznego
im. Komisji Edukacji Narodowej w Krakowie
z 26 czerwca 2023

**w sprawie: przyporządkowania kierunku studiów Cyberbezpieczeństwo I stopnia, profil praktyczny, do dyscyplin naukowych i zatwierdzenia efektów uczenia się**

Działając na podstawie art. 53 ust. 1 i 2 oraz art. 28 ust. 1 pkt. 13 Ustawy z dnia 20 lipca 2018 roku – Prawo o szkolnictwie wyższym i nauce (t. j. Dz. U. z 2023 poz. 742) oraz § 23 pkt. 23 Statutu Uczelni Senat Uniwersytetu Pedagogicznego im. Komisji Edukacji Narodowej w Krakowie postanowił co następuje:

**§ 1**

Przyporządkowuje się kierunek studiów **Cyberbezpieczeństwo** (studia I stopnia, profil praktyczny) do dyscyplin naukowych wskazanych w § 2 niniejszej uchwały oraz wskazuje jako dyscyplinę wiodącą – **informatyka techniczna i telekomunikacja**.

**§ 2**

Kierunek, o którym mowa w § 1, przyporządkowany zostaje do niżej wymienionych dyscyplin:

- **informatyka techniczna i telekomunikacja – 55%** - dyscyplina wiodąca
- nauki o bezpieczeństwie – 30%
- informatyka – 10%
- matematyka – 5%.

**§ 3**

Opis zakładanych efektów uczenia się dla kierunku, o którym mowa w § 1, stanowi załącznik do niniejszej uchwały Senatu.

**§ 4**

Uchwała wchodzi w życie z dniem podjęcia.

Rektor

prof. dr hab. Piotr Borek

1. Nazwa kierunku **Cyberbezpieczeństwo** (studia I stopnia)
2. **Dziedziny i dyscypliny**, do których jest przyporządkowany kierunek:

| | ***Zgodnie z rozporządzeniem MEiN z dnia 11 października 2022 r. w sprawie dziedzin nauki i dyscyplin naukowych oraz dyscyplin artystycznych (Dz.U z 2022 r., poz. 2202)*** | |
|---|---|---|
| ***Dziedziny*** | *nauk ścisłych i przyrodniczych; nauk inżynieryjno-technicznych; nauk społecznych* | |
| ***Dyscyplina wiodąca*** | *Informatyka techniczna i telekomunikacja* | *55%* |
| ***Pozostałe dyscypliny:*** | *nauki o bezpieczeństwie*<br>*informatyka*<br>*matematyka* | *30%*<br>*10%*<br>*5%* |

**3. Sylwetka absolwenta**

Absolwent kierunku *Cyberbezpieczeństwo* uczestnicząc w procesie dydaktycznym, realizowanym za pomocą innowacyjnych metod kształcenia, zdobywa interdyscyplinarną wiedzę z zakresu nauk inżynieryjno-technicznych, ścisłych i przyrodniczych oraz społecznych w zakresie cyberbezpieczeństwa, jak również rozumie i potrafi efektywnie analizować procesy zachodzące w środowisku cyfrowym w biznesie i podmiotach publicznych oraz osób fizycznych. Ma wiedzę z zakresu:

- kryptografii,
- tworzenia, konfiguracji i wykorzystania narzędzi oraz technologii związanych z bezpieczeństwem systemów oraz sieci komputerowych lokalnych i rozległych (w celu zabezpieczania ich funkcjonowania w instytucjach publicznych oraz u wszelkiego rodzaju podmiotów prowadzących działalność gospodarczą),
- działania aplikacji i usług elektronicznych w Internecie (a także w sieciach o mniejszym zasięgu, w tym lokalnych),
- dostępnych rozwiązań w obszarze zabezpieczeń sieci teleinformatycznych, systemów komputerowych, aplikacji oraz projektowania tego typu systemów.

Ponadto zna zagrożenia cyberprzestrzeni i świata wirtualnego, w tym m.in.:

- aspekty prawne, kryminologiczne i techniczne cyberprzestępczości,
- patologiczne formy korzystania z mediów i cyberprzemocy,
- zagrożenia bezpieczeństwa informacyjnego.

**4. Cel studiów**

Celem studiów I stopnia na kierunku C*yberbezpieczeństwo* jest zdobycie umiejętności i kompetencji w zakresie:

- wykorzystania nowoczesnych narzędzi technologii informacyjno-komunikacyjnych w ramach sieci teleinformatycznych, systemów operacyjnych i technik tworzenia aplikacji,
- pracy w różnego typu środowiskach programistycznych,

- doboru, konfiguracji i eksploatacji specjalistycznego sprzętu sieciowego (szczególnie w zastosowaniach dotyczących projektowania i integracji systemów bezpieczeństwa),
- zabezpieczania systemów teleinformatycznych przed atakami oraz dokonywania analizy struktur wrażliwych, w tym sieci komputerowych, w kontekście ich podatności na ataki,
- kształtowania kultury bezpieczeństwa współczesnego człowieka, minimalizacji zagrożeń w celu zapewnienia ochrony danych osobowych, finansów, tożsamości i prywatności, zwalczania cyberprzestępczości, jak również zapobiegania patologiom cyfrowym.

**5. Kierunkowe efekty uczenia się i ich odniesienie do efektów kształcenia dla obszaru/ów nauki:**

Efekty uczenia się

| Symbol efektu kierunkowego | Kierunkowe efekty uczenia się | Odniesienie do efektów uczenia się zgodnych z Polską Ramą Kwalifikacji | |
|---|---|---|---|
| | | Symbol charakterystyk uniwersalnych I stopnia[1] | Symbol charakterystyk II stopnia[2] |
| **WIEDZA – ABSOLWENT zna i rozumie:** | | | |
| K_W01 | w zaawansowanym stopniu fakty i teorie stanowiące wiedzę z przedmiotów ścisłych, zwłaszcza matematyki i fizyki, niezbędną do opisu i analizy działania sieci komputerowych i urządzeń sieciowych, a także innych urządzeń zakresu technik komputerowych oraz algorytmów ich funkcjonowania | P6U_W | P6S_WG |
| K_W02 | w zaawansowanym stopniu fakty i teorie stanowiące wiedzę w zakresie zabezpieczania architektury systemów komputerowych i urządzeń sieciowych w lokalnych i rozległych sieciach komputerowych | P6U_W | P6S_WG |
| K_W03 | elementarne algorytmy, języki i techniki programowania oraz zasady projektowania systemów baz danych w kontekście wymagań bezpieczeństwa | P6U_W | P6S_WG |
| K_W04 | zagadnienia dotyczące systemów informatycznych i sieci komputerowych oraz zasady ich organizacji i administracji | P6U_W | P6S_WG |
| K_W05 | zasady działania podstawowych narzędzi kryptograficznych w kontekście zapewnienia optymalnego zabezpieczenia struktur lokalnych i sieciowych | P6U_W | P6S_WG |

[1] Zgodnie z załącznikiem do ustawy z dnia 22 grudnia 2015 r. o Zintegrowanym Systemie Kwalifikacji (Dz. U. z 2016, poz.64).
[2] Zgodnie z załącznikiem do rozporządzenia Ministra Nauki i Szkolnictwa Wyższego z dnia 14 listopada 2018 r. w sprawie charakterystyk drugiego stopnia efektów uczenia się dla kwalifikacji na poziomach 6-8 Polskiej Ramy Kwalifikacji (Dz. U. z 2018 r., poz. 2218).

| | | | |
|---|---|---|---|
| K_W06 | zasady działania aplikacji i usług elektronicznych w Internecie i w sieciach lokalnych ze szczególnym uwzględnieniem aspektów bezpieczeństwa | P6U_W | P6S_WG |
| K_W07 | w zaawansowanym stopniu pojęcia, struktury i procesy z zakresu cyberbezpieczeństwa (w tym zagrożenia i szanse wynikające z funkcjonowania w świecie cyfrowym wpływające na współczesne państwa, społeczeństwa, podmioty prywatne), jak również przykłady je ilustrujące oraz zależności występujące w obrębie wiedzy dotyczącej bezpieczeństwa w cyberprzestrzeni | P6U_W | P6S_WG |
| K_W08 | w zaawansowanym stopniu prawne, techniczne, ekonomiczno-społeczne i inne uwarunkowania cyberbezpieczeństwa oraz polityki przeciwdziałania przestępczości w cyberprzestrzeni (w tym zaawansowane zasady tworzenia i rozwoju polityki bezpieczeństwa informacyjnego) | P6U_W | P6S_WK |
| K_W09 | istotę człowieka jako podmiotu kształtującego współczesne struktury i procesy w środowisku bezpieczeństwa narodowego i międzynarodowego oraz cyberbezpieczeństwa, generującym szanse i zagrożenia dla jego przyszłości | P6U_W | P6S_WK |
| K_W10 | główne tendencje rozwojowe, najistotniejsze nowe osiągnięcia oraz dylematy etyczne w obszarze cyberbezpieczeństwa | P6U_W | P6S_WK |
| **UMIEJĘTNOŚCI – ABSOLWENT potrafi:** | | | |
| K_U01 | korzystać z nowoczesnych narzędzi IT w zakresie planowania, budowania i eksploatacji sieci komputerowych o lokalnym i rozszerzonym zasięgu w oparciu o zasady bezpieczeństwa funkcjonowania tych struktur | P6U_U | P6S_UW |
| K_U02 | wykorzystywać nowoczesne narzędzia technologii informacyjno-komunikacyjnych w zakresie obsługi (instalacji, konfiguracji i eksploatacji) systemów operacyjnych | P6U_U | P6S_UW |
| K_U03 | używać dedykowanych środowisk programistycznych wraz z wybranymi bibliotekami w celu efektywnego i bezpiecznego tworzenia aplikacji desktopowych, mobilnych czy internetowych | P6U_U | P6S_UW |
| K_U04 | konstruować algorytmy i pisać pojedyncze aplikacje oraz większe projekty programistyczne, w oparciu o języki programowania niskiego i wysokiego poziomu, z uwzględnieniem zasad bezpieczeństwa | P6U_U | P6S_UW |
| K_U05 | indywidualnie lub w zespole pracować (m.in. opracować dokumentację, przedstawić prezentację i prowadzić dyskusję na temat zadania, projektu lub zagadnień w szczególności zw. z cyberbezpieczeństwem, również w jęz. obcym) lub planować pracę, a także komunikować się przy użyciu technik właściwych dla branży IT | P6U_U | P6S_UO |
| K_U06 | zaplanować i przeprowadzać testy, eksperymenty i badania z dziedziny telekomunikacji i informatyki, w szczególności związane z cyberbeczpieczeństwem | P6U_U | P6S_UO |
| K_U07 | analizować i projektować protokoły, sieci i systemy teleinformatyczne, stosując właściwe metody, techniki i narzędzia oraz biorąc pod uwagę aspekty związane z bezpieczeństwem ich użytkowania | P6U_U | P6S_UW |

| | | | |
|---|---|---|---|
| K_U08 | konfigurować urządzenia i protokoły sieciowe oraz nimi zarządzać, mając na uwadze bezpieczeństwo danych | P6U_U | P6S_UW |
| K_U09 | dokonać analizy pod kątem bezpieczeństwa struktur krytycznych z zakresu sieci komputerowych i systemów operacyjnych | P6U_U | P6S_UW |
| K_U10 | formułować i rozwiązywać złożone, typowe i nietypowe problemy zw. z bezpieczeństwem w cyberprzestrzeni, dobierając odpowiednie źródła informacji (również w języku obcym) oraz krytycznie je analizując i syntetyzując, a także wybierając stosowne narzędzia programistyczne, sprzętowe i sieciowe | P6U_U | P6S_UW |
| K_U11 | prawidłowo dostrzec, ocenić i interpretować zjawiska w zakresie cyberbezpieczeństwa oraz rozwoju nowych technologii w ujęciu historycznym, politycznym, społecznym, gospodarczym, militarnym, prawnym (w tym w zakresie ochrony własności intelektualnej) i etycznym. | P6U_U | P6S_UW |
| K_U12 | posługiwać się co najmniej jednym językiem obcym na poziomie B2 Europejskiego Systemu Opisu Kształcenia Językowego oraz terminologią w zakresie cyberbezpieczeństwa | P6U_U | P6S_UK |
| K_U13 | samodzielnie planować i realizować własne uczenie się oraz swój dalszy rozwój zawodowy w branży IT, w szczególności w sektorze cyberbezpieczeństwa. | P6U_U | P6S_UU |
| **KOMPETENCJE SPOŁECZNE – ABSOLWENT jest gotów do:** | | | |
| K_K01 | inicjowania działań na rzecz współdziałania z innymi osobami w ramach prac zespołowych i podejmowania różnych wiodących ról w interdyscyplinarnych zespołach zajmujących się analizowaniem cyberbezpieczeństwa oraz myślenia i działania w sposób przedsiębiorczy | P6U_K | P6S_KO |
| K_K02 | krytycznej oceny poziomu swojej wiedzy oraz ciągłego dokształcania się i konsultacji z innymi ekspertami z branży IT w szczególności związanej z cyberbezpieczeństwem, a także planowania własnego rozwoju zawodowego | P6U_K | P6S_KK |
| K_K03 | respektowania zasad etycznych i prawnych w cyberprzestrzeni oraz zobowiązań płynących z wykonywanego zawodu (w tym poszanowania prawa własności intelektualnej) | P6U_K | P6S_KR |
| K_K04 | uznawania znaczenia tworzenia i wdrażania rozwiązań z obszaru cyberbezpieczeństwa w podnoszeniu jakości życia na świecie (na poziomie jednostki oraz zbiorowości) | P6U_K | P6S_KO |
| K_K05 | inicjowania działań w złożonym ekosystemie podmiotów związanych z zapewnianiem cyberbezpieczeństwa – zarówno z punktu widzenia sektora prywatnego jak i publicznego | P6U_K | P6S_KO |