Wojskowa Akademia Techniczna

**Uchwała**
**Senatu Wojskowej Akademii Technicznej**
**im. Jarosława Dąbrowskiego**

**nr 100/WAT/2025 z dnia 27 listopada 2025 r.**

**w sprawie ustalenia programu studiów podyplomowych „Techniczne i organizacyjne aspekty cyberbezpieczeństwa”**

Na podstawie art. 28 ust. 1 pkt. 11 *ustawy z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce* (Dz. U. z 2024 poz. 1571, z późn. zm.) uchwala się, co następuje:

§ 1

Ustala się program studiów podyplomowych „Techniczne i organizacyjne aspekty cyberbezpieczeństwa”, stanowiący załącznik do uchwały.

§ 2

Uchwała wchodzi w życie z dniem podpisania.

**Przewodniczący Senatu**

**(-) gen. bryg. prof. dr hab. inż. Przemysław WACHULAK**

Załącznik
do Uchwały Senatu WAT nr 100/WAT/2025
z dnia 27 listopada 2025 r.

**WOJSKOWA AKADEMIA TECHNICZNA**
**im. Jarosława Dąbrowskiego**

# PROGRAM STUDIÓW PODYPLOMOWYCH

# „TECHNICZNE I ORGANIZACYJNE ASPEKTY CYBERBEZPIECZEŃSTWA”

**Ustalony uchwałą Senatu WAT Nr 100/WAT/2025 z dnia 27 listopada 2025 r.**

**Obowiązuje od 2025 roku**

**WARSZAWA 2025**

**SPIS TREŚCI** **Strona**


| | | |
|---|---|---|
| 1. | ZAŁOŻENIA PROGRAMU STUDIÓW PODYPLOMOWYCH …….. | 3 |
| 1.1. | ZAKŁADANE EFEKTY UCZENIA SIĘ ……. | 4 |
| 1.2. | KODY PRZEDMIOTÓW ORAZ LICZBA PUNKTÓW ECTS …… | 8 |
| 1.3. | PLAN STUDIÓW PODYPLOMOWYCH …… | 9 |
| 1.4. | SPOSOBY WERYFIKACJI I OCENY OSIĄGANIA PRZEZ SŁUCHACZA ZAKŁADANYCH EFEKTÓW UCZENIA SIĘ …….. | 10 |
| 1.5. | FORMA ZAKOŃCZENIA STUDIÓW PODYPLOMOWYCH ……. | 10 |
| 1.6. | WARUNKI OTRZYMANIA ŚWIADECTWA UKOŃCZENIA STUDIÓW PODYPLOMOWYCH …….. | 10 |
| 2. | PRZEDMIOTOWA CZĘŚĆ PROGRAMU …… | 11 |
| 2.1. | Wprowadzenie do cyberbezpieczeństwa ……. | 11 |
| 2.2. | Prawne aspekty cyberbezpieczeństwa ……. | 14 |
| 2.3. | Strategia cyberbezpieczeństwa ……. | 16 |
| 2.4. | Techniczne aspekty cyberbezpieczeństwa ……. | 19 |
| 2.5. | Nowe wyzwania cyberbezpieczeństwa …… | 23 |
| 2.6. | Zarządzanie cyberbezpieczeństwem ……... | 26 |

# 1. ZAŁOŻENIA PROGRAMU STUDIÓW PODYPLOMOWYCH

## „Techniczne i organizacyjne aspekty cyberbezpieczeństwa”

**Studia prowadzone w** Wydziale Elektroniki i Wydziale Cybernetyki Wojskowej Akademii Technicznej

**Kod studiów:** WELECCNP

Studia podyplomowe prowadzone są przy współudziale Eksperckiego Centrum Szkolenia Cyberbezpieczeństwa na mocy porozumienia pomiędzy Eksperckim Centrum Szkolenia Cyberbezpieczeństwa a Wojskową Akademią Techniczną z dnia 18 listopada 2020 roku.

**Obowiązuje od:** roku 2025.

**Język studiów podyplomowych:** polski

**Wymagania kwalifikacyjne kandydatów na studia podyplomowe:** na studia może być przyjęta osoba posiadająca kwalifikację pełną co najmniej na poziomie 6 Polskiej Ramy Kwalifikacji.

**Określenie kwalifikacji nadawanych absolwentom studiów podyplomowych z przypisaniem odpowiedniego poziomu kwalifikacji cząstkowych Polskiej Ramy Kwalifikacji:** kwalifikacja cząstkowa na poziomie 7 Polskiej Ramy Kwalifikacji.

**Czas trwania studiów podyplomowych:** dwa semestry

**Łączna liczba godzin programowych:** 234 godziny zajęć audytoryjnych w ciągu 16 dwudniowych (weekendowych) zjazdów i jeden dodatkowy zjazd przewidziany na egzamin końcowy.

**Liczba punktów ECTS:** 30.

**Określenie formy zakończenia studiów podyplomowych:** Studia kończą się egzaminem końcowym, który przeprowadza komisja powołana decyzją Dziekana Wydziału Elektroniki lub Dziekana Wydziału Cybernetyki.

**Warunki otrzymania świadectwa ukończenia studiów podyplomowych:** Warunkiem otrzymania świadectwa ukończenia studiów podyplomowych jest zdanie egzaminu końcowego.

## 1.1. ZAKŁADANE EFEKTY UCZENIA SIĘ

Opis zakładanych efektów uczenia się uwzględnia:
- uniwersalne charakterystyki pierwszego stopnia określone w załączniku do ustawy z dnia 22 grudnia 2015 r. o Zintegrowanym Systemie Kwalifikacji,
- charakterystyki drugiego stopnia określone w załączniku 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,
- charakterystyki drugiego stopnia określone w załączniku do rozporządzenia Ministra Edukacji Narodowej z dnia 13 kwietnia 2016 r. w sprawie charakterystyk drugiego stopnia Polskiej Ramy Kwalifikacji typowych dla kwalifikacji o charakterze zawodowym - poziomy 1-8.

**i jest ujęty w trzech kategoriach:**
- kategoria **wiedzy (W)**, która określa:
  - zakres i głębię (**G**) – kompletność perspektywy poznawczej i zależności,
  - kontekst (**K**) – uwarunkowania, skutki;
- kategoria **umiejętności (U)**, która określa:
  - w zakresie wykorzystania wiedzy (**W**) – rozwiązywane problemy i wykonywane zadania,
  - w zakresie komunikowania się (**K**) – odbieranie i tworzenie wypowiedzi, upowszechnianie wiedzy w środowisku naukowym i posługiwanie się językiem obcym,
  - w zakresie organizacji pracy (**O**) – planowanie i pracę zespołową,
  - w zakresie uczenia się (**U**) – planowanie własnego rozwoju i rozwoju innych osób;
- kategoria **kompetencji społecznych (K)**, która określa:
  - w zakresie ocen (**K**) – krytyczne podejście,
  - w zakresie odpowiedzialności (**O**) – wypełnianie zobowiązań społecznych i działanie na rzecz interesu publicznego,
  - w odniesieniu do roli zawodowej (**R**) – niezależność i rozwój etosu.

Objaśnienie oznaczeń:
1) w kolumnie *symbol i numer efektu*:
   a) P – podyplomowe efekty uczenia się,
   b) W, U, K (po podkreślniku) – kategoria (odpowiednio): wiedzy, umiejętności, kompetencji społecznych,
   c) 01, 02, 03, …. – numer efektu uczenia się;
2) w kolumnie kod składnika opisu o charakterze obszarowym – P7S_WG – kod składnika opisu charakterystyk drugiego stopnia Polskiej Ramy Kwalifikacji dla poziomu 7;
3) w kolumnie kod składnika opisu o charakterze zawodowym – P7Z_WT – kod składnika opisu charakterystyki drugiego stopnia Polskiej Ramy Kwalifikacji typowe dla kwalifikacji o charakterze zawodowym (Z – kompetencje zawodowe).

| symbol i numer efektu | opis zakładanych efektów uczenia się | kod składnika opisu o charakterze: | |
|---|---|---|---|
| **WIEDZA** | **Absolwent:** | **obszarowym** | **zawodowym** |
| P_W01 | Zna i rozumie szczegółowo wybrane fakty, obiekty i zjawiska, a także metody i teorie, które wyjaśniają skomplikowane zależności w obszarze cyberbezpieczeństwa. Posiada zaawansowaną, dobrze uporządkowaną i teoretycznie ugruntowaną wiedzę, obejmującą najważniejsze zagadnienia z tego obszaru. | P7S_WG | |
| P_W02 | Zna i rozumie główne tendencje rozwojowe dyscyplin naukowych z obszaru kryptologii, technologii informacyjnych oraz cyberbezpieczeństwa. | P7S_WG | |
| P_W03 | Zna i rozumie podstawowe procesy zachodzące w cyklu życia urządzeń, obiektów i systemów technicznych. | P7S_WG | |
| P_W04 | Zna i rozumie ekonomiczne, prawne, etyczne i inne uwarunkowania różnych rodzajów działalności zawodowej w obszarze kryptologii, technologii informacyjnych oraz cyberbezpieczeństwa. | P7S_WK | |
| P_W05 | Zna i rozumie w pogłębiony sposób podstawy teoretyczne kryptologii, technologii informacyjnych oraz cyberbezpieczeństwa. | | P7Z_WT |
| P_W06 | Zna i rozumie trendy rozwojowe w dziedzinie działalności zawodowej w obszarze kryptologii, technologii informacyjnych oraz cyberbezpieczeństwa. | | P7Z_WT |
| P_W07 | Zna i rozumie teorie dotyczące zjawisk i procesów zachodzących w cyberprzestrzeni w sposób, umożliwiający skuteczne stosowanie metod i technologii z obszaru kryptologii, technologii informacyjnych oraz cyberbezpieczeństwa. | | P7Z_WZ |
| P_W08 | Zna i rozumie różnorodne, złożone metody i technologie z obszaru cyberbezpieczeństwa oraz ich wpływ na inne dziedziny | | P7Z_WO |
| P_W09 | Zna i rozumie różnorodne, złożone rozwiązania organizacyjne w obszarze cyberbezpieczeństwa oraz ich wpływ na inne dziedziny | | P7Z_WO |
| **UMIEJĘTNOŚCI** | **Absolwent:** | | |
| P_U01 | Potrafi wykorzystywać posiadaną wiedzę, formułować i rozwiązywać złożone i nietypowe problemy oraz innowacyjnie wykonywać zadania w nieprzewidywalnych warunkach przez właściwy dobór źródeł i informacji z nich pochodzących w obszarze kryptologii, technologii informacyjnych oraz cyberbezpieczeństwa. | P7S_UW | |
| P_U02 | Potrafi wykorzystywać posiadaną wiedzę, formułować i rozwiązywać złożone i nietypowe problemy oraz innowacyjnie wykonywać zadania w nieprzewidywalnych warunkach przez dokonywanie oceny, krytycznej analizy, syntezy, twórczej interpretacji i prezentacji tych informacji w obszarze kryptologii, technologii informacyjnych oraz cyberbezpieczeństwa. | P7S_UW | |

| | | | |
|---|---|---|---|
| P_U03 | Potrafi wykorzystywać posiadaną wiedzę, formułować i rozwiązywać złożone i nietypowe problemy oraz innowacyjnie wykonywać zadania w nieprzewidywalnych warunkach przez dobór oraz stosowanie właściwych metod i narzędzi dedykowanych kryptologii, technologii informacyjnych oraz cyberbezpieczeństwa. | P7S_UW | |
| P_U04 | Potrafi wykorzystywać posiadaną wiedzę, formułować i rozwiązywać problemy oraz wykonywać zadania typowe dla działalności zawodowej w obszarze kryptologii, technologii informacyjnych oraz cyberbezpieczeństwa. | P7S_UW | |
| P_U05 | Potrafi wykorzystywać posiadaną wiedzę, formułować i testować hipotezy związane z problemami wdrożeniowymi w obszarze kryptologii, technologii informacyjnych oraz cyberbezpieczeństwa | P7S_UW | |
| P_U06 | Potrafi komunikować się na tematy specjalistyczne szczególnie odnoszących się do kryptologii, technologii informacyjnych oraz cyberbezpieczeństwa ze zróżnicowanymi kręgami odbiorców oraz prowadzić debatę | P7S_UK | |
| P_U07 | Potrafi kierować pracą zespołu, współdziałać z innymi osobami w ramach prac zespołowych i podejmować wiodącą rolę w zespołach. | P7S_UO | |
| P_U08 | Potrafi samodzielnie planować i realizować własne uczenie się przez całe życie i ukierunkowywać innych w tym zakresie. | P7S_UU | |
| P_U09 | Potrafi planować i przeprowadzać eksperymenty, w tym pomiary i symulacje komputerowe, interpretować uzyskane wyniki i wyciągać wnioski. | P7S_UW | |
| P_U10 | Potrafi dokonywać krytycznej analizy sposobu funkcjonowania istniejących rozwiązań technicznych z obszaru kryptologii, technologii informacyjnych oraz cyberbezpieczeństwa oraz oceniać te rozwiązania | P7S_UW | |
| P_U11 | Potrafi projektować - zgodnie z zadaną specyfikacją - oraz wykonywać typowe dla kierunku studiów rozwiązania, obiekty, systemy lub realizować procesy, używając odpowiednio dobranych metod, technik, narzędzi i materiałów. | P7S_UW | |
| P_U12 | Potrafi rozwiązywać praktyczne zadania inżynierskie wymagające korzystania ze standardów i norm inżynierskich oraz stosowania technologii z obszaru kryptologii, technologii informacyjnych oraz cyberbezpieczeństwa. | P7S_UW | |
| P_U13 | Potrafi wykorzystywać zdobyte w środowisku zajmującym się zawodowo działalnością inżynierską doświadczenie związane z utrzymaniem urządzeń, obiektów i systemów z obszaru kryptologii, technologii informacyjnych oraz cyberbezpieczeństwa | P7S_UW | |
| P_U14 | Potrafi monitorować kierunki rozwoju technologii w obszarze kryptologii, IT oraz cyberbezpieczeństwa i dziedzin powiązanych oraz jej międzynarodowe uwarunkowania i konteksty | | P7Z_UI |

| | | | |
|---|---|---|---|
| P_U15 | Potrafi prognozować kierunki rozwoju technologii w obszarze kryptologii, IT oraz cyberbezpieczeństwa. | | P7Z_UI |
| P_U16 | Potrafi opracowywać plan strategiczny dla zespołu pracowniczego / organizacji w dziedzinie cyberbezpieczeństwa. | | P7Z_UO |
| P_U17 | Potrafi kierować zespołem pracowniczym / organizacją realizującą złożone i nietypowe zadania zawodowe w obszarze kryptologii, technologii informacyjnych oraz cyberbezpieczeństwa w zmiennych i nieprzewidywalnych warunkach | | P7Z_UO |
| P_U18 | Potrafi analizować i oceniać prowadzoną działalność zawodową w perspektywie trendów rozwojowych w dziedzinie kryptologii, technologii informacyjnych oraz cyberbezpieczeństwa. | | P7Z_UO |
| P_U19 | Potrafi modyfikować metody i technologie oraz procedury w działalności zawodowej w obszarze kryptologii, technologii informacyjnych oraz cyberbezpieczeństwa. | | P7Z_UN |
| P_U20 | Potrafi ukierunkować rozwój kompetencji zawodowych podległych pracowników. | | P7Z_UU |
| P_U21 | Potrafi przekazywać wiedzę zawodową w różnych formach. | | P7Z_UU |
| **KOMPETENCJE SPOŁECZNE Absolwent:** | | | |
| P_K01 | Jest gotów do krytycznej oceny posiadanej wiedzy i odbieranych treści. | P7S_KK | |
| P_K02 | Jest gotów do uznawania znaczenia wiedzy w rozwiązywaniu problemów poznawczych i praktycznych oraz zasięgania opinii ekspertów w przypadku trudności z samodzielnym rozwiązaniem problemu. | P7S_KK | |
| P_K03 | Jest gotów do inicjowania działań na rzecz interesu publicznego. | P7S_KO | |
| P_K04 | Rozumie potrzebę i zna możliwości ciągłego dokształcania się – podnoszenia kompetencji zawodowych, osobistych i społecznych. | P7S_KO | |
| P_K05 | Rozumie potrzebę wymagania od innych przestrzegania zasad obowiązujących w działalności zawodowej, w obszarze kryptologii, technologii informacyjnych oraz cyberbezpieczeństwa dotyczących utrzymywania jakości prowadzonej działalności. | | P7Z_KP |
| P_K06 | Jest gotów do promowania kultury projakościowej w działalności zawodowej w obszarze kryptologii, technologii informacyjnych oraz cyberbezpieczeństwa. | | P7Z_KO |

## 1.2. KODY PRZEDMIOTÓW ORAZ LICZBA PUNKTÓW ECTS:

| Lp. | Nazwa przedmiotu | Kod przedmiotu[1] | Liczba punktów ECTS |
|---|---|---|---|
| 1 | Wprowadzenie do cyberbezpieczeństwa | **WELECCNP – WDC** | 3 |
| 2 | Prawne aspekty cyberbezpieczeństwa | **WELECCNP – PAC** | 0,5 |
| 3 | Strategia cyberbezpieczeństwa | **WELECCNP – SC** | 1 |
| 4 | Techniczne aspekty cyberbezpieczeństwa | **WELECCNP – TAC** | 10 |
| 5 | Nowe wyzwania cyberbezpieczeństwa | **WELECCNP – NWC** | 1,5 |
| 6 | Zarządzanie cyberbezpieczeństwem | **WELECCNP – ZC** | 6 |
| 7 | Egzamin końcowy | **WELECCNP – EK** | 8 |
| **Razem punkty ECTS** | | | **30** |

[1] *zgodny z kodem nadawanym przez USOS*

## 1.3. PLAN STUDIÓW PODYPLOMOWYCH

Wojskowa Akademia Techniczna

**PLAN STUDIÓW PODYPLOMOWYCH**

**Wydział Elektroniki / Wydział Cybernetyki / Eksperckie Centrum Szkolenia Cyberbezpieczeństwa**

**TECHNICZNE I ORGANIZACYJNE ASPEKTY CYBERBEZPIECZEŃSTWA**

| PRZEDMIOTY | | Ogółem godzin / punkty ECTS | | w tym godzin: | | | | | liczba godzin, rygorów, punktów ECTS w semestrze | | | | | | Jednostka organizacyjna odpowiedzialna za przedmiot |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | I | | | II | | | |
| | | godz. | ECTS | wykł. | ćwicz. | proj. | lab. | sem. | godz. | rygor | ECTS | godz. | rygor | ECTS | |
| **1** | Wprowadzenie do cyberbezpieczeństwa | 28 | 3 | 20 | 8 | | | | 28 | Zo | 3 | | | | **WCY** |
| **2** | Prawne aspekty cyberbezpieczeństwa | 8 | 0,5 | 8 | | | | | 8 | Z | 0,5 | | | | **WEL / ECSC** |
| **3** | Strategia cyberbezpieczeństwa | 12 | 1 | 8 | 4 | | | | 12 | Zo | 1 | | | | **WEL / ECSC** |
| **4** | Techniczne aspekty cyberbezpieczeństwa | 100 | 10 | 8 | 4 | | 88 | | 72 | Zo | 7 | 28 | Zo | 3 | **WEL / WCY** |
| **5** | Nowe wyzwania cyberbezpieczeństwa | 14 | 1,5 | 14 | | | | | | | | 14 | Z | 1,5 | **WEL** |
| **6** | Zarządzanie cyberbezpieczeństwem | 64 | 6 | 8 | 24 | | 32 | | | | | 64 | Zo | 6 | **WEL / WCY / ECSC** |
| **7** | Egzamin końcowy | 8 | 8 | | | | | | | | | 8 | E | 8 | **WEL / WCY / ECSC** |
| **OGÓŁEM** | | **234** | **30** | **66** | **40** | | **120** | | **120** | | **11,5** | **114** | | **18,5** | |
| **Rodzaje i liczba rygorów** | | | | | | **Egzamin – E** | | | **0** | | | **1** | | | |
| | | | | | | **Zaliczenie bez oceny – Z** | | | **1** | | | **1** | | | |
| | | | | | | **Zaliczenie z oceną – Zo** | | | **3** | | | **2** | | | |

## 1.4. SPOSOBY WERYFIKACJI I OCENY OSIĄGANIA PRZEZ SŁUCHACZA ZAKŁADANYCH EFEKTÓW UCZENIA SIĘ

Weryfikacja zakładanych efektów uczenia się prowadzona jest na poziomie przedmiotu kształcenia. Dla każdej formy realizacji przedmiotu (wykłady, ćwiczenia audytoryjne, ćwiczenia laboratoryjne, seminarium, projekt) zostały zdefiniowane zakładane efekty uczenia się w zakresie wiedzy, umiejętności i kompetencji społecznych oraz metody i sposoby ich weryfikacji. Szczegółowe sposoby weryfikacji efektów uczenia się są zawarte w przedmiotowej części programu. Ostateczną formą weryfikacji nabytej wiedzy i umiejętności jest egzamin końcowy.

## 1.5. FORMA ZAKOŃCZENIA STUDIÓW PODYPLOMOWYCH

Studia kończą się egzaminem końcowym, który przeprowadza komisja powołana decyzją Dziekana Wydziału Elektroniki lub Dziekana Wydziału Cybernetyki. Zakres działalności komisji, jej skład, zadania oraz sposób oceny słuchacza są określone w regulaminie studiów podyplomowych Wojskowej Akademii Technicznej im. Jarosława Dąbrowskiego.
Warunkiem przystąpienia słuchacza do egzaminu końcowego jest uzyskanie pozytywnych ocen/zaliczeń ze wszystkich przedmiotów występujących w planie studiów.

## 1.6. WARUNKI OTRZYMANIA ŚWIADECTWA UKOŃCZENIA STUDIÓW PODYPLOMOWYCH

Warunkiem otrzymania świadectwa ukończenia studiów podyplomowych jest zdanie egzaminu końcowego. Na świadectwie studiów wpisuje się słownie wynik ukończenia studiów podyplomowych, ustalony zgodnie z obowiązującym regulaminem studiów podyplomowych Wojskowej Akademii Technicznej im. Jarosława Dąbrowskiego.
Dokumentem formalizującymi i nadającym moc prawną uzyskania świadectwa ukończenia studiów podyplomowych jest decyzja Rektora.
Świadectwo ukończenia studiów podyplomowych wykonywane jest /wypisywane jest/ w WAT, centralnie przez Dział Organizacji Kształcenia. Świadectwo podlega ewidencji w rejestrze wydanych świadectw.

## 2. PRZEDMIOTOWA CZĘŚĆ PROGRAMU

### 2.1 Wprowadzenie do cyberbezpieczeństwa

| **Nazwa przedmiotu** | **Wprowadzenie do cyberbezpieczeństwa** |
|---|---|
| Kod przedmiotu | *WELECCNP – WDC* |
| Forma zajęć,<br>liczba godzin / rygor,<br>razem godz., pkt ECTS | *W-20/Zo, C-8/Z,* ***razem: 28 godz. / Zo, 3 pkt ECTS*** |
| Jednostka organizacyjna odpowiedzialna za przedmiot | *WCY* |
| Skrócony opis przedmiotu /zajęć | *W ramach przedmiotu zostaną omówione zagadnienia związane z ochroną systemów i sieci komputerowych, systemów teleinformatycznych, danych oraz użytkowników przed zagrożeniami występującymi w cyberprzestrzeni. Zaprezentowane zostaną rodzaje, techniki i narzędzia przeprowadzania ataków w cyberprzestrzeni oraz zagrożenia, podatności sprzętu i oprogramowania, ryzyko z nimi związane oraz metody przeciwdziałania tym zagrożeniom.*<br>*Przedstawiona zostanie architektura globalnego i krajowego systemu cyberbezpieczeństwa.* |
| Zakładane przedmiotowe efekty uczenia się | Symbol i nr efektu przedmiotu / efekt uczenia się / odniesienie do efektu:<br>W01/ Zna i rozumie szczegółowo wybrane fakty, obiekty i zjawiska, a także metody i teorie, które wyjaśniają skomplikowane zależności między nimi. Posiada zaawansowaną wiedzę ogólną z danej dziedziny naukowej, dobrze uporządkowaną i teoretycznie ugruntowaną, obejmującą najważniejsze zagadnienia oraz wybrane szczegółowe tematy. / P_W01<br>W02/ Zna i rozumie główne tendencje rozwojowe dyscyplin naukowych z obszaru kryptologii, technologii informacyjnych oraz cyberbezpieczeństwa. / P_W02<br>W03/ Zna i rozumie podstawowe procesy zachodzące w cyklu życia urządzeń, obiektów i systemów technicznych. / P_W03<br>W06/ Zna i rozumie trendy rozwojowe w dziedzinie działalności zawodowej w obszarze kryptologii, technologii informacyjnych oraz cyberbezpieczeństwa. / P_W06<br>W08/ Zna i rozumie różnorodne, złożone metody i technologie w dziedzinie działalności zawodowej w kontekście rozwiązań stosowanych w innych dziedzinach w obszarze kryptologii, technologii informacyjnych oraz cyberbezpieczeństwa. / P_W08<br>U01/ Potrafi wykorzystywać posiadaną wiedzę, formułować i rozwiązywać złożone i nietypowe problemy oraz innowacyjnie wykonywać zadania w nieprzewidywalnych warunkach przez właściwy dobór źródeł i informacji z nich pochodzących w obszarze kryptologii, technologii informacyjnych oraz cyberbezpieczeństwa. / P_U01<br>U03/ Potrafi wykorzystywać posiadaną wiedzę, formułować i rozwiązywać złożone i nietypowe problemy oraz innowacyjnie wykonywać zadania w nieprzewidywalnych warunkach przez dobór oraz stosowanie właściwych metod i narzędzi dedykowanych kryptologii, technologii informacyjnych oraz cyberbezpieczeństwa. / P_U03<br>U10/ Potrafi dokonywać krytycznej analizy sposobu funkcjonowania istniejących rozwiązań technicznych z obszaru kryptologii, technologii informacyjnych oraz cyberbezpieczeństwa oraz oceniać te rozwiązania. / P_U10<br>U12/ Potrafi rozwiązywać praktyczne zadania inżynierskie wymagające korzystania ze standardów i norm inżynierskich oraz stosowania technologii z obszaru kryptologii, technologii informacyjnych oraz cyberbezpieczeństwa. / P_U12 |

| | |
|---|---|
| | U13/ Potrafi wykorzystywać zdobyte w środowisku zajmującym się zawodowo działalnością inżynierską doświadczenie związane z utrzymaniem urządzeń, obiektów i systemów z obszaru kryptologii, technologii informacyjnych oraz cyberbezpieczeństwa. / P_U13<br>U14/ Potrafi monitorować rozwój dziedziny działalności zawodowej w obszarze kryptologii, technologii informacyjnych oraz cyberbezpieczeństwa i dziedzin powiązanych oraz jej międzynarodowe uwarunkowania i konteksty. / P_U14<br>U18/ Potrafi analizować i oceniać prowadzoną działalność zawodową w perspektywie trendów rozwojowych w dziedzinie kryptologii, technologii informacyjnych oraz cyberbezpieczeństwa. / P_U18<br>U19/ Potrafi modyfikować metody i technologie oraz procedury w działalności zawodowej w obszarze kryptologii, technologii informacyjnych oraz cyberbezpieczeństwa. / P_U19 |
| Pełny opis przedmiotu (treści programowe) | Wykłady<br>**1. Podstawy cyberbezpieczeństwa** / 16 godz. /<br>*Podstawowe pojęcia z zakresu cyberbezpieczeństwa, typy i rodzaje zagrożeń w cyberprzestrzeni, analiza podatności i ryzyka oraz skutków zaistnienia cyberataków, źródła informacji o bieżących cyberzagrożeniach oraz lukach bezpieczeństwa, złośliwe oprogramowanie, techniki detekcji i analizy, zabezpieczenia jako środek kontrolowania możliwości realizacji zagrożenia – klasyfikacja i właściwości, przegląd mechanizmów bezpieczeństwa sieci, systemów i użytkowników.*<br><br>**2. Globalny i Krajowy System Cyberbezpieczeństwa** / 4 godz. /<br>*Uregulowania prawne Globalnego i Krajowego Systemu Cyberbezpieczeństwa, architektura i zasady funkcjonowania Globalnego Systemy Cyberbezpieczeństwa, architektura i zasady funkcjonowania Krajowego Systemy Cyberbezpieczeństwa oraz jego miejsce w Globalnym Systemie Cyberbezpieczeństwa, przykładowe systemy cyberbezpieczeństwa wybranych państw członkowskich UE i NATO.*<br><br>Ćwiczenia audytoryjne<br>**3. Tworzenie dokumentacji systemu cyberbezpieczeństwa** / 8 godz. /<br>*Polityka bezpieczeństwa informacji, analiza ryzyka, planowanie i zarządzanie incydentami, zarządzanie dostępem, ochrona danych osobowych, zabezpieczenie techniczne, system szkoleń i budowanie świadomości użytkowników, zarządzanie ciągłością działania organizacji, audyt i monitoring, współpraca wewnętrzna i zewnętrzna, aktualizacja dokumentacji i polityk.* |
| Literatura | Podstawowa:<br>1. *Charles J. Brooks, Philip Craig, Donald Short, Cybersecurity essentials, John Wiley & Sons Inc, 2018*<br>2. *Robin Sharp, Introduction to Cybersecurity, Springer, 2023*<br>3. *Ajay Singh, Introduction to Cybersecurity, Orient Blackswan Pvt Ltd, 2023*<br>4. *Anand Shinde, Introduction to Cyber Security: Guide to the World of Cyber Security, HARPERCOLLINS 360, 2021*<br>5. *Krzysztof Liderman, "Wprowadzenie do cyberbezpieczeństwa - Podstawowe pojęcia", e-book wydanie ECSC, 2024*<br>6. *Raef Meeuwisse, Cybersecurity for Beginners 2nd edition, Cyber Simplicity Ltd., 2017*<br><br>Uzupełniająca:<br>1. *Touhill Gregory J., Touhill C. Joseph, Cybersecurity for Executives: A Practical Guide", John Wiley & Sons Inc, 2014*<br>2. *Diogenes Yuri, Erdal Ozkaya, Cybersecurity - Attack and Defense Strategies - Second Edition: Counter modern threats and employ state-of-the-art tools and techniques to protect your organisation against cybercriminals, Packt Pub, 2020* |

| | |
|---|---|
| | 3. *William Stallings, Network Security Essentials: Applications and Standards, Global Edition, PEARSON Education Limited, 2016*<br>*4. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa* |
| Metody i kryteria oceniania (sposób sprawdzania osiągnięcia przez słuchacza zakładanych efektów uczenia się) | Przedmiot zakończony jest: zaliczeniem z oceną.<br>Ćwiczenia audytoryjne zaliczane są na podstawie: zaliczenia<br>Zaliczenie przedmiotu jest prowadzone w formie pisemnego testu.<br>Warunkiem przystąpienia słuchacza do zaliczenia jest pozytywne zaliczenie ćwiczeń audytoryjnych.<br><br>Osiągnięcie efektu W01, W02, W03, W06 oraz W08 weryfikowane jest podczas zaliczenia.<br>Osiągnięcie efektu U01, U03, U10, U12, U13, U14, U18 oraz U19 sprawdzane jest w czasie ćwiczeń audytoryjnych.<br><br>Ocenę **bardzo dobrą** otrzymuje słuchacz, który osiągnął zakładane efekty uczenia się na poziomie 91-100%.<br>Ocenę **dobrą plus** otrzymuje słuchacz, który osiągnął zakładane efekty uczenia się na poziomie 81-90%.<br>Ocenę **dobrą** otrzymuje słuchacz, który osiągnął zakładane efekty uczenia się na poziomie 71-80%.<br>Ocenę **dostateczną plus** otrzymuje słuchacz, który osiągnął zakładane efekty uczenia się na poziomie 61-70%.<br>Ocenę **dostateczną** otrzymuje słuchacz, który osiągnął zakładane efekty uczenia się na poziomie 51-60%.<br>Ocenę **niedostateczną** otrzymuje słuchacz, który osiągnął zakładane efekty uczenia się na poziomie równym lub niższym niż 50%. |
| Bilans ECTS<br>(nakład pracy słuchacza) | Aktywność / obciążenie słuchacza w godz.<br>*Udział w wykładach / 20*<br>*Udział w ćwiczeniach laboratoryjnych / 0*<br>*Udział w ćwiczeniach audytoryjnych / 8*<br>*Udział w seminariach / 0*<br>*Samodzielne studiowanie tematyki wykładów / 15*<br>*Samodzielne przygotowanie do ćwiczeń laboratoryjnych / 0*<br>*Samodzielne przygotowanie do ćwiczeń audytoryjnych / 8*<br>*Samodzielne przygotowanie do seminarium / 0*<br>*Realizacja projektu / 0*<br>*Udział w konsultacjach / 2*<br>*Przygotowanie do egzaminu / 0*<br>*Przygotowanie do zaliczenia / 22*<br>*Udział w egzaminie / 0*<br><br>Sumaryczne obciążenie pracą słuchacza: 75 godz. / 3 ECTS |

## 2.2 Prawne aspekty cyberbezpieczeństwa

| **Nazwa przedmiotu** | **Prawne aspekty cyberbezpieczeństwa** |
|---|---|
| Kod przedmiotu | *WELECCNP – PAC* |
| Forma zajęć, liczba godzin / rygor, razem godz., pkt ECTS | *W-8/Z,* ***razem: 8 godz. / Z, 0,5 pkt ECTS*** |
| Jednostka organizacyjna odpowiedzialna za przedmiot | *WEL / ECSC* |
| Skrócony opis przedmiotu /zajęć | *W ramach przedmiotu omówione zostanie prawodawstwo krajowe w zakresie cyberbezpieczeństwa z uwzględnieniem operacji w cyberprzestrzeni w czasie pokoju, kryzysu i konfliktu zbrojnego, ramy prawne działalności bussinesowej w kontekście cyberbezpieczeństwa oraz wyzwania etyczne związane z rozwojem technologii w kontekście cyberbezpieczeństwa.* |
| Zakładane przedmiotowe efekty uczenia się | Symbol i nr efektu przedmiotu / efekt uczenia się / odniesienie do efektu:<br>W01/ Zna i rozumie ekonomiczne, prawne, etyczne i inne uwarunkowania różnych rodzajów działalności zawodowej w obszarze kryptologii, technologii informacyjnych oraz cyberbezpieczeństwa. / P_W04<br>W02/ Zna i rozumie różnorodne, złożone rozwiązania organizacyjne w dziedzinie działalności zawodowej w kontekście rozwiązań stosowanych w innych dziedzinach w obszarze kryptologii, technologii informacyjnych oraz cyberbezpieczeństwa. / P_W09<br>U01/ Potrafi wykorzystywać posiadaną wiedzę, formułować i rozwiązywać złożone i nietypowe problemy oraz innowacyjnie wykonywać zadania w nieprzewidywalnych warunkach przez właściwy dobór źródeł i informacji z nich pochodzących w obszarze kryptologii, technologii informacyjnych oraz cyberbezpieczeństwa. / P_U01<br>U02/ Potrafi rozwiązywać praktyczne zadania inżynierskie wymagające korzystania ze standardów i norm inżynierskich oraz stosowania technologii z obszaru kryptologii, technologii informacyjnych oraz cyberbezpieczeństwa. / P_U12<br>U03/ Potrafi opracowywać plan strategiczny dla zespołu pracowniczego organizacji w dziedzinie cyberbezpieczeństwa. / P_U16<br>K01/ Jest gotów do inicjowania działań na rzecz interesu publicznego. / P_K03<br>K02/ Jest gotów do wymagania od innych przestrzegania zasad obowiązujących w działalności zawodowej, w obszarze kryptologii, technologii informacyjnych oraz cyberbezpieczeństwa dotyczących utrzymywania jakości prowadzonej działalności. / P_K05 |
| Pełny opis przedmiotu (treści programowe) | Wykłady<br>**1. Prawodawstwo krajowe i międzynarodowe w zakresie cyberbezpieczeństwa** / 4 godz. /<br>*Przegląd regulacji krajowych i międzynarodowych w zakresie cyberbezpieczeństwa, prawne aspekty ochrony informacji, ochrona danych osobowych, wolność słowa i prawa człowieka a cyberbezpieczeństwo, cyberprzestępczość w ujęciu polskiego prawodawstwa, uregulowania prawne operacji defensywnych i ofensywnych w cyberprzestrzeni w czasie pokoju, kryzysu i konfliktu zbrojnego.*<br>**2. Ramy prawne działalności bussinesowej w kontekście cyberbezpieczeństwa** / 4 godz. /<br>*Krajowe prawodawstwo w odniesieniu do umów o świadczenie usług z zakresu cyberbezpieczeństwa, zamówienia publiczne w sektorze cyberbezpieczeństwa, ubezpieczenie ryzyk cybernetycznych, prawne aspekty kryptografii, technologii blockchain, podpisów cyfrowych, tzw. „shadow IT", ocena wyzwań etycznych w sektorze cyberbezpieczeństwa.* |

| | |
|---|---|
| Literatura | Podstawowa:<br>1. *Ustawa z dnia 11 marca 2022 r. o obronie Ojczyzny*<br>2. *Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa*<br>3. *Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych*<br>4. *Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych*<br>5. *Ustawa z dnia 6 czerwca 1997 r. Kodeks karny*<br>6. *Ustawa z dnia 11 września 2019 r. Prawo zamówień publicznych*<br>7. *Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną*<br>8. *Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne*<br>9. *CDiSZ, DD 3.20 Operacje w cyberprzestrzeni – szkol. 977/2020, CDiSZ, 2020, CDiSZ, 2020*<br>10. *NSO, Allied Joint Doctrine 3.20 for cyberspace operations, Edition A, Version 1, NSO, 2020, NSO, 2020*<br><br>Uzupełniająca:<br>1. *Damian Robert Jaworski, Paweł Opitek, Cyberprzestępczość w prawie karnym i kryminalistyce: Kompendium wiedzy, Difin, 2025*<br>2. *Theodoros Karathanasis, Cybersecurity and EU law, Taylor & Francis Ltd, 2024*<br>3. *Joe Gray, Socjotechniki w praktyce. Podręcznik etycznego hakera, Helion, 2022* |
| Metody i kryteria oceniania (sposób sprawdzania osiągnięcia przez słuchacza zakładanych efektów uczenia się) | Przedmiot zakończony jest: zaliczeniem bez oceny.<br>Warunkiem zaliczenia przedmiotu jest obecność na wykładach.<br><br>Osiągnięcie efektów W01, W02, U01, U02, U03, K01 oraz K02 weryfikowane jest podczas wykładów.<br><br>Ocenę **uogólnioną zal.** otrzymuje słuchacz, który osiągnął zakładane efekty uczenia się na poziomie wyższym niż 50%.<br>Ocenę **uogólnioną nzal.** otrzymuje słuchacz, który osiągnął zakładane efekty uczenia się na poziomie równym lub niższym niż 50%. |
| Bilans ECTS (nakład pracy słuchacza) | Aktywność / obciążenie słuchacza w godz.<br>*Udział w wykładach / 8*<br>*Udział w ćwiczeniach laboratoryjnych / 0*<br>*Udział w ćwiczeniach audytoryjnych / 0*<br>*Udział w seminariach / 0*<br>*Samodzielne studiowanie tematyki wykładów / 5*<br>*Samodzielne przygotowanie do ćwiczeń laboratoryjnych / 0*<br>*Samodzielne przygotowanie do ćwiczeń audytoryjnych / 0*<br>*Samodzielne przygotowanie do seminarium / 0*<br>*Realizacja projektu / 0*<br>*Udział w konsultacjach / 2*<br>*Przygotowanie do egzaminu / 0*<br>*Przygotowanie do zaliczenia / 0*<br>*Udział w egzaminie / 0*<br><br>Sumaryczne obciążenie pracą słuchacza: 15 godz. / 0,5 ECTS |

## 2.3 Strategia cyberbezpieczeństwa

| **Nazwa przedmiotu** | **Strategia cyberbezpieczeństwa** |
|---|---|
| Kod przedmiotu | *WELECCNP – SC* |
| Forma zajęć,<br>liczba godzin / rygor,<br>razem godz., pkt ECTS | *W-8/Zo, C-4/Z,* ***razem: 12 godz. / Zo, 1 pkt ECTS*** |
| Jednostka organizacyjna odpowiedzialna za przedmiot | *WEL / ECSC* |
| Skrócony opis przedmiotu /zajęć | *W ramach przedmiotu omówione zostaną zagadnienia odnoszące się do planowania, wdrażania i egzekwowania strategii cyberbezpieczeństwa w skali macro (w państwie) i mikro (w organizacji), w ujęciu cywilnym i wojskowym. Przedstawione zostaną strategie (w tym polityki, taktyki, techniki i procedury) obniżające ryzyko dla bezpieczeństwa informacji.* |
| Zakładane przedmiotowe efekty uczenia się | Symbol i nr efektu przedmiotu / efekt uczenia się / odniesienie do efektu:<br>W01/ Zna i rozumie różnorodne, złożone rozwiązania organizacyjne w dziedzinie działalności zawodowej w kontekście rozwiązań stosowanych w innych dziedzinach w obszarze kryptologii, technologii informacyjnych oraz cyberbezpieczeństwa. / P_W09<br>U01/ Potrafi wykorzystywać posiadaną wiedzę, formułować i rozwiązywać złożone i nietypowe problemy oraz innowacyjnie wykonywać zadania w nieprzewidywalnych warunkach przez właściwy dobór źródeł i informacji z nich pochodzących w obszarze kryptologii, technologii informacyjnych oraz cyberbezpieczeństwa. / P_U01<br>U02/ Potrafi samodzielnie planować i realizować własne uczenie się przez całe życie i ukierunkowywać innych w tym zakresie. / P_U08<br>U03/ Potrafi prognozować rozwój sytuacji w dziedzinie działalności zawodowej w obszarze kryptologii, technologii informacyjnych oraz cyberbezpieczeństwa. / P_U15<br>U04/ Potrafi opracowywać plan strategiczny dla zespołu pracowniczego / organizacji w dziedzinie cyberbezpieczeństwa. / P_U16<br>K01/ Jest gotów do promowania kultury projakościowej w działalności zawodowej w obszarze kryptologii, technologii informacyjnych oraz cyberbezpieczeństwa. / P_K06 |
| Pełny opis przedmiotu (treści programowe) | Wykłady<br>**1. Strategiczna rola cyberbezpieczeństwa** / 4 godz. /<br>*Strategia cyberbezpieczeństwa Rzeczypospolitej Polskiej, strategia cyberbezpieczeństwa w skali organizacji, cele szczegółowe i misja strategii cyberbezpieczeństwa, znaczenie cyberprzestrzeni dla bezpieczeństwa państwa i organizacji, źródła wymagań, architektura i aspekty ekonomiczne w kontekście długoterminowego rozwoju organizacji i państwa, strategia cyberbezpieczeństwa w dobie transformacji cyfrowej.*<br><br>**2. Obrona cyberprzestrzeni państwa w sytuacji konfliktów zbrojnych** / 4 godz. /<br>*Strategia cyberbezpieczeństwa w kontekście kryzysu i konfliktu, w ujęciu cywilnym i wojskowym, , miejsce krajowego systemu cyberbezpieczeństwa w strategii cyberbezpieczeństwa, cyberbezpieczeństwo infrastruktury krytycznej i wojskowej, zdolności ofensywne w cyberprzestrzeni i zasady wykorzystania w świetle prawa międzynarodowego, międzynarodowa współpraca w obronie cyberprzestrzeni, przyszłość ochrony cyberprzestrzeni w kontekście rozwoju nowych technologii.* |

| | |
|---|---|
| | Ćwiczenia audytoryjne<br>**1. Kryzysowy "PR" w tematyce cyberbezpieczeństwa** / 4 godz. /<br>*Wojna kognitywna i jej wykorzystanie do uzyskiwania przewagi strategicznej, znaczenie komunikacji strategicznej we współczesnym świecie, media społecznościowe i ich znaczenie, nowe technologie i ich znaczenie w kontekście wojny informacyjnej.* |
| Literatura | Podstawowa:<br>1. *Katarzyna Chałubińska-Jentkiewicz, Agnieszka Brzostek, Strategie cyberbezpieczeństwa współczesnego świata, Wydawnictwo Towarzystwa Wiedzy Obronnej, 2021*<br>2. *Kshetri Nir, Cybersecurity Management: An Organizational and Strategic Approach, Univ of Toronto Pr, 2021*<br>3. *Ibp Inc - praca zbiorowa, EU Cyber Security Strategy and Programs Handbook Volume 1 Strategic Information and Regulations, Intl Business Pubn, 2018*<br>4. *Allison Cerra, The Cybersecurity Playbook: How Every Leader and Employee Can Contribute to a Culture of Security, John Wiley & Sons Inc, 2019*<br><br>Uzupełniająca:<br>1. *Charles J. Brooks, Philip Craig, Donald Short, Cybersecurity essentials, John Wiley & Sons Inc, 2018*<br>2. *Anand Shinde, Introduction to Cyber Security: Guide to the World of Cyber Security, HARPERCOLLINS 360, 2021*<br>3. *Lester Nichols, Cybersecurity Architect's Handbook, Packt Publishing, 2024*<br>4. *Trim Peter, Strategic Cyber Security Management, Routledge, 2022*<br>5. *Mary Aiken, Cyber Effect, John Murray Press, 2017* |
| Metody i kryteria oceniania (sposób sprawdzania osiągnięcia przez słuchacza zakładanych efektów uczenia się) | Przedmiot zakończony jest: zaliczeniem z oceną.<br>Ćwiczenia audytoryjne zaliczane są na podstawie: zaliczenia<br>Zaliczenie przedmiotu jest prowadzone w formie pisemnego testu.<br>Warunkiem przystąpienia słuchacza do zaliczenia jest pozytywne zaliczenie ćwiczeń audytoryjnych.<br><br>Osiągnięcie efektu W01 weryfikowane jest podczas zaliczenia.<br>Osiągnięcie efektu U01, U02, U03, U04 oraz K01 sprawdzane jest w czasie ćwiczeń audytoryjnych.<br><br>Ocenę **bardzo dobrą** otrzymuje słuchacz, który osiągnął zakładane efekty uczenia się na poziomie 91-100%.<br>Ocenę **dobrą plus** otrzymuje słuchacz, który osiągnął zakładane efekty uczenia się na poziomie 81-90%.<br>Ocenę **dobrą** otrzymuje słuchacz, który osiągnął zakładane efekty uczenia się na poziomie 71-80%.<br>Ocenę **dostateczną plus** otrzymuje słuchacz, który osiągnął zakładane efekty uczenia się na poziomie 61-70%.<br>Ocenę **dostateczną** otrzymuje słuchacz, który osiągnął zakładane efekty uczenia się na poziomie 51-60%.<br>Ocenę **niedostateczną** otrzymuje słuchacz, który osiągnął zakładane efekty uczenia się na poziomie równym lub niższym niż 50%. |
| Bilans ECTS<br>(nakład pracy słuchacza) | Aktywność / obciążenie słuchacza w godz.<br>*Udział w wykładach / 8*<br>*Udział w ćwiczeniach laboratoryjnych / 0*<br>*Udział w ćwiczeniach audytoryjnych / 4*<br>*Udział w seminariach / 0*<br>*Samodzielne studiowanie tematyki wykładów / 4*<br>*Samodzielne przygotowanie do ćwiczeń laboratoryjnych / 0*<br>*Samodzielne przygotowanie do ćwiczeń audytoryjnych / 4*<br>*Samodzielne przygotowanie do seminarium / 0*<br>*Realizacja projektu / 0* |

| | |
|---|---|
| | *Udział w konsultacjach / 2*<br>*Przygotowanie do egzaminu / 0*<br>*Przygotowanie do zaliczenia / 8*<br>*Udział w egzaminie / 0*<br><br>Sumaryczne obciążenie pracą słuchacza: 30 godz. / 1 ECTS |

## 2.4 Techniczne aspekty cyberbezpieczeństwa

| **Nazwa przedmiotu** | **Techniczne aspekty cyberbezpieczeństwa** |
|---|---|
| Kod przedmiotu | *WELECCNP – TAC* |
| Forma zajęć,<br>liczba godzin / rygor,<br>razem godz., pkt ECTS | *W-8/Zo, C-4/Z, L-88/Zo,* ***razem: 100 godz. / Zo, 10 pkt ECTS*** |
| Jednostka organizacyjna odpowiedzialna za przedmiot | *WEL / WCY* |
| Skrócony opis przedmiotu /zajęć | *W ramach przedmiotu zostaną omówione zagadnienia związane z bezpieczeństwem fizycznym w obszarze cyberbezpieczeństwa, bezpieczeństwem kryptograficznym, zasadami budowania bezpieczeństwa systemów informacyjnych z uwzględnieniem bezpieczeństwa sieci komputerowych i systemów operacyjnych, aplikacji mobilnych i webowych, bezpieczeństwa infrastruktury centrów przetwarzania danych "on-premise" oraz opartych na rozwiązaniach chmurowych, jak również bezpieczeństwo urządzeń mobilnych. Zaprezentowane zostaną najlepsze praktyki budowania cyberodporności w organizacji, w tym modele bazujące na ryzyku (risk-based).* |
| Zakładane przedmiotowe efekty uczenia się | Symbol i nr efektu przedmiotu / efekt uczenia się / odniesienie do efektu:<br>W01/ Zna i rozumie podstawowe procesy zachodzące w cyklu życia urządzeń, obiektów i systemów technicznych. / P_W03<br>W02/ Zna i rozumie w pogłębiony sposób podstawy teoretyczne metod i technologii w dziedzinie działalności zawodowej w powiązaniu z innymi dziedzinami z obszaru kryptologii, technologii informacyjnych oraz cyberbezpieczeństwa. / P_W05<br>W03/ Zna i rozumie teorie dotyczące zjawisk i procesów w pogłębiony sposób, umożliwiający przezwyciężanie ograniczeń wynikających z właściwości stosowanych materiałów, metod i technologii w obszarze kryptologii, technologii informacyjnych oraz cyberbezpieczeństwa. / P_W07<br>W04/ Zna i rozumie różnorodne, złożone metody i technologie w dziedzinie działalności zawodowej w kontekście rozwiązań stosowanych w innych dziedzinach w obszarze kryptologii, technologii informacyjnych oraz cyberbezpieczeństwa. / P_W08<br>U01/ Potrafi wykorzystywać posiadaną wiedzę, formułować i rozwiązywać złożone i nietypowe problemy oraz innowacyjnie wykonywać zadania w nieprzewidywalnych warunkach przez właściwy dobór źródeł i informacji z nich pochodzących w obszarze kryptologii, technologii informacyjnych oraz cyberbezpieczeństwa. / P_U01<br>U02/ Potrafi wykorzystywać posiadaną wiedzę, formułować i rozwiązywać złożone i nietypowe problemy oraz innowacyjnie wykonywać zadania w nieprzewidywalnych warunkach przez dokonywanie oceny, krytycznej analizy, syntezy, twórczej interpretacji i prezentacji tych informacji w szczególności w obszarze kryptologii, technologii informacyjnych oraz cyberbezpieczeństwa. / P_U02<br>U03/ Potrafi wykorzystywać posiadaną wiedzę, formułować i rozwiązywać złożone i nietypowe problemy oraz innowacyjnie wykonywać zadania w nieprzewidywalnych warunkach przez dobór oraz stosowanie właściwych metod i narzędzi dedykowanych kryptologii, technologii informacyjnych oraz cyberbezpieczeństwa. / P_U03 |
| Pełny opis przedmiotu (treści programowe) | Wykłady<br>**1. Bezpieczeństwo fizyczne** / 1 godz. /<br>*Bezpieczeństwo fizyczne infrastruktury krytycznej, zagrożenia wewnętrzne i zewnętrzne, zasady i najlepsze praktyki budowania bezpieczeństwa fizycznego centrów danych, ochrona przed nieautoryzowanym dostępem do urządzeń IT, zabezpieczenie sieci kablowych i infrastruktury komunikacyjnej* |

| | |
|---|---|
| | *w skali mikro i makro, zarządzanie dostępem do pomieszczeń "technicznych", przechowywanie nośników danych, zabezpieczanie urządzeń końcowych przed kradzieżą, znaczenie szkolenia z zakresu bezpieczeństwa fizycznego.*<br><br>**2. Bezpieczeństwo kryptograficzne** / 1 godz. /<br>*Znaczenie kryptografii dla cyberbezpieczeństwa, zagrożenia dla bezpieczeństwa kryptograficznego, rodzaje ataków, metody i algorytmy szyfrowania, infrastruktura klucza publicznego i zarządzanie kluczami kryptograficznymi, bezpieczeństwo kryptograficzne w chmurze, ochrona prywatności w płatnościach online, podpis cyfrowy, kryptografia kwantowa.*<br><br>**3. Bezpieczeństwo systemów informacyjnych** / 6 godz. /<br>*Wprowadzenie do bezpieczeństwa sieci, bezpieczeństwo systemów operacyjnych, bezpieczeństwo aplikacji mobilnych i webowych, bezpieczeństwo infrastruktury on-premise, bezpieczeństwo Cloud Computing.*<br><br>Ćwiczenia audytoryjne<br>**1. Bezpieczeństwo urządzeń mobilnych** / 4 godz. /<br>*Przegląd zagrożeń i ataków typowych dla urządzeń mobilnych, zabezpieczanie systemów operacyjnych urządzeń mobilnych (na przykładzie MS Windows, Unix/Linux, Android, iOS), zarządzanie aplikacjami oraz aktualizacjami OS i aplikacji, bezpieczeństwo przechowywanych danych, zarządzanie dostępem do danych, uwierzytelnienie i autoryzacja, zabezpieczenie przed kradzieżą i zgubieniem, zabezpieczanie komunikacji na urządzeniach mobilnych.*<br><br>Ćwiczenia laboratoryjne<br>**1. Bezpieczeństwo sieci** / 20 godz. /<br>*Testy penetracyjne (skanowanie, enumeracja, identyfikacja podatności). Ataki sieciowe i przeciwdziałanie atakom. Kryptograficzne mechanizmy zabezpieczania danych. Ochrona kanałów komunikacji w sieci.*<br><br>**2. Bezpieczeństwo systemów operacyjnych** / 32 godz. /<br>*Podstawy systemów operacyjnych – Windows i Linux (budowa, wersjonowanie, licencjonowanie, podstawowe narzędzia i obsługa). Testy penetracyjne (skanowanie, enumeracja, identyfikacja podatności). Analiza incydentów i korelacja zdarzeń. Utwardzanie systemów – zapora sieciowa. Utwardzanie systemów – zabezpieczanie usług. Utwardzanie systemów – zabezpieczanie kont użytkowników.*<br><br>**3. Bezpieczeństwo aplikacji** / 24 godz. /<br>*Definiowanie wymagań bezpieczeństwa dla aplikacji, anatomia ataków na aplikacje, planowanie i przeprowadzanie testów penetracyjnych, skanowanie i analiza sieci. Ataki na aplikacje, metody przeciwdziałania zagrożeniom dla aplikacji, warsztaty bezpieczeństwa aplikacji, systemy wykrywania intruzów, zabezpieczanie transmisji danych.*<br><br>**4. Bezpieczeństwo infrastruktury on-premise** / 4 godz. /<br>*Zagrożenia dla infrastruktury "on-prem", zasady i najlepsze praktyki zabezpieczania fizycznego centrów danych, zarządzanie dostępem do serwerów i urządzeń sieciowych, najlepsze praktyki w budowaniu redundancji, zapewnieniu ciągłości działania i odporności świadczonych usług na zagrożenia, zarządzanie i monitorowanie logów bezpieczeństwa, zarządzanie tożsamością i kryptografia w infrastrukturze on-prem, system aktualizacji, kopia zapasowa i odzyskiwanie danych w infrastrukturze on-prem.* |

| | |
|---|---|
| | **5. Bezpieczeństwo Cloud Computing** / 8 godz. /<br>*Zagrożenia dla rozwiązań chmurowych (poziom dostawcy usług) oraz usług (poziom klienta). Tworzenie środowisk cloud computing. Maszyny wirtualne, zarządzanie maszynami wirtualnymi. Redundancja i bezpieczeństwo środowisk chmurowych. Mechanizmy HA dla maszyn wirtualnych.* |
| Literatura | Podstawowa:<br>1. *Mary Aiken, Cyber Effect, John Murray Press, 2017*<br>2. *Joe Gray, Socjotechniki w praktyce. Podręcznik etycznego hakera, Helion, 2022*<br>3. *Diogenes Yuri, Erdal Ozkaya, Cybersecurity - Attack and Defense Strategies - Second Edition: Counter modern threats and employ state-of-the-art tools and techniques to protect your organisation against cybercriminals, Packt Publishing, 2020*<br>4. *Gerard Johansen, Digital Forensics and Incident Response - Third Edition, Packt Publishing, 2022*<br>5. *Gerard Johansen, Digital Forensics and Incident Response. Incident response techniques and procedures to respond to modern cyber threats, 2nd Edition, Packt Publishing, 2020*<br>6. *Khanna Deepanshu, Digital Forensics and Incident Response: A practical guide to using Kali Linux for cyber investigations (English Edition), Independent Cat, 2024*<br>7. *Darren R. Hayes, Practical Guide to Digital Forensics Investigations, A, Pearson Education, 2020*<br>8. *Michael Sikorski, Practical Malware Analysis, No Starch Press, 2022*<br>9. *Gus Khawaja, Kali Linux Penetration Testing Bible, John Wiley & Sons Inc, 2021*<br>10. *Chris Dotson, Practical Cloud Security: A Guide for Secure Design and Deployment, OREILLY MEDIA, 2024*<br>11. *Daniel Graham, Ethical Hacking, No Starch Press, 2021*<br><br>Uzupełniająca:<br>1. *Jon Erickson, Hacking: The Art Of Exploitation 2nd Edition, No Starch Press, 2008*<br>2. *William Stallings, Network Security Essentials: Applications and Standards, Global Edition, PEARSON Education Limited, 2016*<br>3. *Georgia Weidman, Penetration Testing, No Starch Press,US, 2014*<br>4. *Peter Kim, The Hacker Playbook 3: Practical Guide to Penetration Testing, LIGHTNING SOURCE INC, 2018* |
| Metody i kryteria oceniania (sposób sprawdzania osiągnięcia przez słuchacza zakładanych efektów uczenia się) | Przedmiot zakończony jest: zaliczeniem z oceną.<br>Ćwiczenia audytoryjne zaliczane są na podstawie: zaliczenia.<br>Ćwiczenia laboratoryjne zaliczane są zaliczeniem z oceną na podstawie sprawozdań wykonanych po każdym ćwiczeniu laboratoryjnym.<br>Zaliczenie przedmiotu jest prowadzone w formie pisemnego testu.<br>Warunkiem przystąpienia słuchacza do zaliczenia jest pozytywne zaliczenie ćwiczeń audytoryjnych oraz pozytywna ocena z ćwiczeń laboratoryjnych.<br><br>Osiągnięcie efektu W01, W02, W03 oraz W04 weryfikowane jest podczas zaliczenia.<br>Osiągnięcie efektu U01, U02 oraz U03 sprawdzane jest w czasie ćwiczeń audytoryjnych oraz ćwiczeń laboratoryjnych.<br><br>Ocenę **bardzo dobrą** otrzymuje słuchacz, który osiągnął zakładane efekty uczenia się na poziomie 91-100%.<br>Ocenę **dobrą plus** otrzymuje słuchacz, który osiągnął zakładane efekty uczenia się na poziomie 81-90%.<br>Ocenę **dobrą** otrzymuje słuchacz, który osiągnął zakładane efekty uczenia się na poziomie 71-80%. |

| | |
|---|---|
| | Ocenę **dostateczną plus** otrzymuje słuchacz, który osiągnął zakładane efekty uczenia się na poziomie 61-70%.<br>Ocenę **dostateczną** otrzymuje słuchacz, który osiągnął zakładane efekty uczenia się na poziomie 51-60%.<br>Ocenę **niedostateczną** otrzymuje słuchacz, który osiągnął zakładane efekty uczenia się na poziomie równym lub niższym niż 50%. |
| Bilans ECTS<br>(nakład pracy słuchacza) | Aktywność / obciążenie słuchacza w godz.<br>*Udział w wykładach / 8*<br>*Udział w ćwiczeniach laboratoryjnych / 88*<br>*Udział w ćwiczeniach audytoryjnych / 4*<br>*Udział w seminariach / 0*<br>*Samodzielne studiowanie tematyki wykładów / 4*<br>*Samodzielne przygotowanie do ćwiczeń laboratoryjnych / 132*<br>*Samodzielne przygotowanie do ćwiczeń audytoryjnych / 4*<br>*Samodzielne przygotowanie do seminarium / 0*<br>*Realizacja projektu / 0*<br>*Udział w konsultacjach / 2*<br>*Przygotowanie do egzaminu / 0*<br>*Przygotowanie do zaliczenia / 8*<br>*Udział w egzaminie / 0*<br><br>Sumaryczne obciążenie pracą słuchacza: 250 godz. / 10 ECTS |

## 2.5 Nowe wyzwania cyberbezpieczeństwa

| **Nazwa przedmiotu** | **Nowe wyzwania cyberbezpieczeństwa** |
|---|---|
| Kod przedmiotu | *WELECCNP – NWC* |
| Forma zajęć,<br>liczba godzin / rygor,<br>razem godz., pkt ECTS | *W-14/Z,* ***razem: 14 godz. / Z, 1,5 pkt ECTS*** |
| Jednostka organizacyjna odpowiedzialna za przedmiot | *WEL* |
| Skrócony opis przedmiotu /zajęć | *W ramach przedmiotu zostaną omówione zagadnienia związane z technologią blockchain oraz jej zastosowaniem w cyberbezpieczeństwie, możliwościami i zagrożeniami jakie dla cyberbezpieczeństwa niesie sztuczna inteligencja i jej szybki rozwój. Zaprezentowane zostaną technologie kwantowe przez pryzmat kryptoanalizy, kryptografii kwantowej i postkwantowej w kontekście ich potencjału w obszarze cyberbezpieczeństwa. Omówione również będzie bezpieczeństwo komunikacji mobilnej (5G) w kontekście nowych, przełomowych technologii.* |
| Zakładane przedmiotowe efekty uczenia się | Symbol i nr efektu przedmiotu / efekt uczenia się / odniesienie do efektu:<br>W01/ Zna i rozumie główne tendencje rozwojowe dyscyplin naukowych z obszaru kryptologii, technologii informacyjnych oraz cyberbezpieczeństwa. / P_W02<br>W02/ Zna i rozumie trendy rozwojowe w dziedzinie działalności zawodowej w obszarze kryptologii, technologii informacyjnych oraz cyberbezpieczeństwa. / P_W06<br>U01/ Potrafi wykorzystywać posiadaną wiedzę, formułować i rozwiązywać złożone i nietypowe problemy oraz innowacyjnie wykonywać zadania w nieprzewidywalnych warunkach przez właściwy dobór źródeł i informacji z nich pochodzących w obszarze kryptologii, technologii informacyjnych oraz cyberbezpieczeństwa. / P_U01<br>U02/ Potrafi dokonywać krytycznej analizy sposobu funkcjonowania istniejących rozwiązań technicznych z obszaru kryptologii, technologii informacyjnych oraz cyberbezpieczeństwa oraz oceniać te rozwiązania. / P_U10<br>U03/ Potrafi monitorować rozwój dziedziny działalności zawodowej w obszarze kryptologii, technologii informacyjnych oraz cyberbezpieczeństwa i dziedzin powiązanych oraz jej międzynarodowe uwarunkowania i konteksty. / P_U14<br>U04/ Potrafi prognozować rozwój sytuacji w dziedzinie działalności zawodowej w obszarze kryptologii, technologii informacyjnych oraz cyberbezpieczeństwa. / P_U15<br>U05/ Potrafi analizować i oceniać prowadzoną działalność zawodową w perspektywie trendów rozwojowych w dziedzinie kryptologii, technologii informacyjnych oraz cyberbezpieczeństwa. / P_U18<br>U06/ Potrafi modyfikować metody i technologie oraz procedury w działalności zawodowej w obszarze kryptologii, technologii informacyjnych oraz cyberbezpieczeństwa. / P_U19<br>U07/ Potrafi ukierunkować rozwój kompetencji zawodowych podległych pracowników. / P_U20<br>K01/ Jest gotów do krytycznej oceny posiadanej wiedzy i odbieranych treści. / P_K01<br>K02/ Jest gotów do uznawania znaczenia wiedzy w rozwiązywaniu problemów poznawczych i praktycznych oraz zasięgania opinii ekspertów w przypadku trudności z samodzielnym rozwiązaniem problemu. / P_K02<br>K03/ Rozumie potrzebę i zna możliwości ciągłego dokształcania się – podnoszenia kompetencji zawodowych, osobistych i społecznych. / P_K04 |

| | |
|---|---|
| Pełny opis przedmiotu (treści programowe) | Wykłady<br>**1. Technologia blockchain – zastosowanie w cyberbezpieczeństwie** / 2 godz. /<br>*Zarządzanie tożsamością i dostępem, tworzenie zdecentralizowanych systemów tożsamości, ochrona integralności danych, zabezpieczenie przechowywania i udostępniania danych, zabezpieczenie komunikacji, implementacja Blockchain w protokołów komunikacyjnych, zarządzanie łańcuchem dostaw i śledzenie pochodzenia produktów, zabezpieczenie urządzeń IoT, zarządzanie danymi w chmurze, tworzenie rozproszonych systemów przechowywania danych, zabezpieczenie transakcji finansowych.*<br><br>**2. Sztuczna inteligencja a cyberbezpieczeństwo** / 4 godz. /<br>*Wykrywanie i analiza zagrożeń z wykorzystaniem dużych zbiorów danych w czasie rzeczywistym, rozpoznawanie nietypowych wzorców zachowań, automatyzacja reakcji na incydenty, uczenie maszynowe w analizie danych, działania proaktywne, wykrywanie anomalii, analityka predykcyjna, zarządzanie podatnościami w zabezpieczeniach, przeciwdziałanie zaawansowanym zagrożeniom, takim jak ataki zero-day, identyfikacja nowych technik ataków, zabezpieczenie urządzeń IoT, ochrona przed phishingiem i oszustwami, zarządzanie bezpieczeństwem w chmurze, monitorowanie i analiza środowisk chmurowych, wykrywanie zagrożeń specyficznych dla chmury, zarządzanie dostępem i tożsamością w chmurze*<br><br>**3. Technologie kwantowe – kryptoanaliza, kryptografia kwantowa i postkwantowa** / 4 godz. /<br>*Analiza potencjalnych zagrożeń dla obecnych systemów kryptograficznych, kryptografia postkwantowa, nowe algorytmy kryptograficzne odporne na ataki z wykorzystaniem technologii kwantowych, dystrybucja klucza kwantowego (QKD), zjawisko superpozycji i splątania, analiza wpływu komputerów kwantowych na istniejące algorytmy i systemy kryptograficzne, standaryzacja algorytmów kryptografii postkwantowej, postęp w pracach nad standardami kryptograficznymi odpornymi na ataki kwantowe, integracja kryptografii postkwantowej z istniejącymi systemami, metody migracji z klasycznych algorytmów do postkwantowych, zabezpieczenie blockchain przed atakami kwantowymi, wpływ komputerów kwantowych na bezpieczeństwo technologii blockchain, postkwantowe rozwiązania kryptograficzne dla zapewnienia integralności i autentyczności transakcji.*<br><br>**4. Bezpieczeństwo komunikacji mobilnej (5G)** / 4 godz. /<br>*Opis architektury bezpieczeństwa 5G razem z analizą domen bezpieczeństwa sieci 5G: (1) bezpieczeństwo dostępu do sieci: Security Associations, Authentication and Key Agreement (5G AKA, EAP-AKA), porównanie z siecią 4G; identyfikatorów (SUPI, SUCI, 5G-GUTI), ephemeral keys I szyfrowanie w dostępie do sieci 5G, Access Stratum security oraz Non-Access Stratum security, zarządzanie kluczami bezpieczeństwa; (2) bezpieczeństwo architektury Software-based: modele zabezpieczenia komunikacji w SBA, rola SCP, zarządzanie certyfikatami (#) bezpieczeństwo sieci: standardy 3GPP, użycie innych standardów: IPSec/IKEv2, TLS 1.2/TLS 1.3, bezpieczeństwo dostępu do sieci przez inne technologie sieci bezprzewodowych innych niż 3GPP (Non-3GPP Access security), bezpieczeństwo roamingu i sieci nie publicznych; (3) bezpieczeństwo domeny użytkownika: urządzenie mobilne oraz SIM (UICC), mobile ID application, Subscription management platform service (eUICC vs. UICC); (4) bezpieczeństwo domeny aplikacji: wsparcie 3GPP w EAP-based secondary authentication, slice-specific authentication and authorization, Authentication and Key Management for Applications (AKMA), Vehicle to Everything Services (V2X) security, CIoT (Cellular IoT) security enhancements.* |

| | |
|---|---|
| Literatura | Podstawowa:<br>1. *Rajneesh Gupta, Hands-On Cybersecurity with Blockchain, Packt Publishing, 2018*<br>2. *Alessandro Parisi, Hands-On Artificial Intelligence for Cybersecurity, Packt Publishing, 2019*<br>3. *Shyam R. Sihare, Quantum Computing and Cryptography in Future Computers, IGI Global/ Engineering Science Reference, 2024*<br>4. *Michio Kaku, Kwantowa dominacja. Jak komputery kwantowe odmienią nasz świat, Prószyński Media, 2023*<br>5. *Praca zbiorowa, Quantum Computing in Cybersecurity, Scrivener Publishing LLC, 2023*<br>6. *Simon Edwards, Quantum Computing and Modern Cryptography, 2+3D, 2020*<br><br>Uzupełniająca:<br>1. *Katarzyna Chałubińska-Jentkiewicz, Agnieszka Brzostek, Strategie cyberbezpieczeństwa współczesnego świata, Wydawnictwo Towarzystwa Wiedzy Obronnej, 2021*<br>2. *Andreas Antonopoulos, Mastering Bitcoin, O'Reilly Media, 2017*<br>3. *Joe Gray, Socjotechniki w praktyce. Podręcznik etycznego hakera, Helion, 2022*<br>4. *Noson S. Yanofsky, Mirco A. Mannucci, Quantum Computing for Computer Scientists, Cambridge University Press, 2012*<br>5. *Daniel J. Bernstein, Johannes Buchmann, Erik Dahmen, Post-Quantum Cryptography, Springer, 2008"* |
| Metody i kryteria oceniania (sposób sprawdzania osiągnięcia przez słuchacza zakładanych efektów uczenia się) | Przedmiot zakończony jest: zaliczeniem bez oceny.<br>Warunkiem zaliczenia przedmiotu jest obecność na wykładach.<br><br>Osiągnięcie efektów W01, W02, U03, U04, U05, U06, U07, U08, U09, K01 oraz K02 weryfikowane jest podczas wykładów.<br><br>Ocenę **uogólnioną zal.** otrzymuje słuchacz, który osiągnął zakładane efekty uczenia się na poziomie wyższym niż 50%.<br>Ocenę **uogólnioną nzal.** otrzymuje słuchacz, który osiągnął zakładane efekty uczenia się na poziomie równym lub niższym niż 50%. |
| Bilans ECTS (nakład pracy słuchacza) | Aktywność / obciążenie słuchacza w godz.<br>*Udział w wykładach / 14*<br>*Udział w ćwiczeniach laboratoryjnych / 0*<br>*Udział w ćwiczeniach audytoryjnych / 0*<br>*Udział w seminariach / 0*<br>*Samodzielne studiowanie tematyki wykładów / 20*<br>*Samodzielne przygotowanie do ćwiczeń laboratoryjnych / 0*<br>*Samodzielne przygotowanie do ćwiczeń audytoryjnych / 0*<br>*Samodzielne przygotowanie do seminarium / 0*<br>*Realizacja projektu / 0*<br>*Udział w konsultacjach / 2*<br>*Przygotowanie do egzaminu / 0*<br>*Przygotowanie do zaliczenia / 0*<br>*Udział w egzaminie / 0*<br><br>Sumaryczne obciążenie pracą słuchacza: 36 godz. / 1,5 ECTS |

## 2.6 Zarządzanie cyberbezpieczeństwem

| **Nazwa przedmiotu** | **Zarządzanie cyberbezpieczeństwem** |
|---|---|
| Kod przedmiotu | *WELECCNP – ZC* |
| Forma zajęć, liczba godzin / rygor, razem godz., pkt ECTS | *W-8/Zo, C-24/Zo, L-32/Zo,* ***razem: 64 godz. / Zo, 6 pkt ECTS*** |
| Jednostka organizacyjna odpowiedzialna za przedmiot | *WEL / WCY / ECSC* |
| Skrócony opis przedmiotu /zajęć | *W ramach przedmiotu zostaną omówione zagadnienia związane z zarządzaniem incydentami, metodyką modelowania ryzyka i oceny zagrożeń w cyberprzestrzeni, złośliwe oprogramowanie, techniki detekcji i analizy malware, botnety, rodzaje testów penetracyjnych, warsztat pentestera, test penetracyjny jako element zarządzania cyberbezpieczeństwem, model Intrusion Kill Chain, zarządzanie konfiguracją i testowaniem bezpieczeństwa systemu operacyjnego, zarządzanie testowaniem bezpieczeństwa z wykorzystaniem przykładowej sieci komputerowej, metodyki prowadzenia audytu, ataki APT (Advanced Persistent Threats), luki 0-day, zarządzanie projektami.* |
| Zakładane przedmiotowe efekty uczenia się | W01/ Zna i rozumie ekonomiczne, prawne, etyczne i inne uwarunkowania różnych rodzajów działalności zawodowej w obszarze kryptologii, technologii informacyjnych oraz cyberbezpieczeństwa. / P_W04<br>W02/ Zna i rozumie w pogłębiony sposób podstawy teoretyczne metod i technologii w dziedzinie działalności zawodowej w powiązaniu z innymi dziedzinami z obszaru kryptologii, technologii informacyjnych oraz cyberbezpieczeństwa. / P_W05<br>W03/ Zna i rozumie różnorodne, złożone rozwiązania organizacyjne w dziedzinie działalności zawodowej w kontekście rozwiązań stosowanych w innych dziedzinach w obszarze kryptologii, technologii informacyjnych oraz cyberbezpieczeństwa. / P_W09<br>U01/ Potrafi wykorzystywać posiadaną wiedzę, formułować i rozwiązywać złożone i nietypowe problemy oraz innowacyjnie wykonywać zadania w nieprzewidywalnych warunkach przez właściwy dobór źródeł i informacji z nich pochodzących w obszarze kryptologii, technologii informacyjnych oraz cyberbezpieczeństwa. / P_U01<br>U02/ Potrafi wykorzystywać posiadaną wiedzę, formułować i rozwiązywać złożone i nietypowe problemy oraz innowacyjnie wykonywać zadania w nieprzewidywalnych warunkach przez dokonywanie oceny, krytycznej analizy, syntezy, twórczej interpretacji i prezentacji tych informacji w szczególności w obszarze kryptologii, technologii informacyjnych oraz cyberbezpieczeństwa. / P_U02<br>U03/ Potrafi wykorzystywać posiadaną wiedzę, formułować i rozwiązywać złożone i nietypowe problemy oraz innowacyjnie wykonywać zadania w nieprzewidywalnych warunkach przez dobór oraz stosowanie właściwych metod i narzędzi dedykowanych kryptologii, technologii informacyjnych oraz cyberbezpieczeństwa. / P_U03<br>U04/ Potrafi wykorzystywać posiadaną wiedzę, formułować i rozwiązywać problemy oraz wykonywać zadania typowe dla działalności zawodowej w obszarze kryptologii, technologii informacyjnych oraz cyberbezpieczeństwa. / P_U04<br>U05/ Potrafi wykorzystywać posiadaną wiedzę, formułować i testować hipotezy związane z prostymi problemami wdrożeniowymi w obszarze kryptologii, technologii informacyjnych oraz cyberbezpieczeństwa. / P_U05<br>U06/ Potrafi komunikować się na tematy specjalistyczne szczególnie odnoszących się do kryptologii, technologii informacyjnych oraz cyberbezpieczeństwa ze zróżnicowanymi kręgami odbiorców oraz prowadzić debatę / P_U06 |

| | |
|---|---|
| | U07/ Potrafi kierować pracą zespołu, współdziałać z innymi osobami w ramach prac zespołowych i podejmować wiodącą rolę w zespołach. / P_U07<br>U08/ Potrafi samodzielnie planować i realizować własne uczenie się przez całe życie i ukierunkowywać innych w tym zakresie. / P_U08<br>U09/ Potrafi planować i przeprowadzać eksperymenty, w tym pomiary i symulacje komputerowe, interpretować uzyskane wyniki i wyciągać wnioski. / P_U09<br>U10/ Potrafi projektować - zgodnie z zadaną specyfikacją - oraz wykonywać typowe dla kierunku studiów proste rozwiązania, obiekty, systemy lub realizować procesy, używając odpowiednio dobranych metod, technik, narzędzi i materiałów. / P_U11<br>U11/ Potrafi wykorzystywać zdobyte w środowisku zajmującym się zawodowo działalnością inżynierską doświadczenie związane z utrzymaniem urządzeń, obiektów i systemów z obszaru kryptologii, technologii informacyjnych oraz cyberbezpieczeństwa. / P_U13<br>U12/ Potrafi kierować zespołem pracowniczym / organizacją realizującą złożone i nietypowe zadania zawodowe w obszarze kryptologii, technologii informacyjnych oraz cyberbezpieczeństwa w zmiennych i nieprzewidywalnych warunkach. / P_U17<br>U13/ Potrafi analizować i oceniać prowadzoną działalność zawodową w perspektywie trendów rozwojowych w dziedzinie kryptologii, technologii informacyjnych oraz cyberbezpieczeństwa. / P_U18<br>U14/ Potrafi modyfikować metody i technologie oraz procedury w działalności zawodowej w obszarze kryptologii, technologii informacyjnych oraz cyberbezpieczeństwa. / P_U19<br>U15/ Potrafi ukierunkować rozwój kompetencji zawodowych podległych pracowników. / P_U20<br>U16/ Potrafi przekazywać wiedzę zawodową w różnych formach. / P_U21<br>K01/ Jest gotów do krytycznej oceny posiadanej wiedzy i odbieranych treści. / P_K01<br>K02/ Jest gotów do wymagania od innych przestrzegania zasad obowiązujących w działalności zawodowej, w obszarze kryptologii, technologii informacyjnych oraz cyberbezpieczeństwa dotyczących utrzymywania jakości prowadzonej działalności. / P_K05<br>K03/ Jest gotów do promowania kultury projakościowej w działalności zawodowej w obszarze kryptologii, technologii informacyjnych oraz cyberbezpieczeństwa. / P_K06 |
| Pełny opis przedmiotu (treści programowe) | Wykłady<br>**1. Systemy zarządzania bezpieczeństwem informacji (SZBI) wg ISO/IEC 27001** / 1 godz. /<br>*Przegląd modeli zarządzania ryzykiem, przegląd rodziny norm ISO/IEC27000 ze szczególnym uwzględnieniem normy ISO/IEC 27001, planowanie, projektowanie i budowanie systemu zarządzania bezpieczeństwem informacji, modelowanie zagrożeń i zarządzanie ryzykiem, narzędzia wykorzystywane do zarządzania ryzykiem.*<br><br>**2. Psychologiczne aspekty cyberbezpieczeństwa** / 1 godz. /<br>*Definicja socjotechniki i jej znaczenie w cyberbezpieczeństwie, metody i narzędzia wykorzystywane w atakach socjotechnicznych (np. phishing, vishing, pretexting), psychologiczne mechanizmy wykorzystywane w atakach socjotechnicznych, techniki obrony przed atakami socjotechnicznymi, rola organizacji w przeciwdziałaniu atakom socjotechnicznym*<br><br>**3. Cyber Security Leadership** / 4 godz. /<br>*Definicja przywództwa w cyberbezpieczeństwie i przywództwo strategiczne, rola liderów w kształtowaniu kultury i strategii cyberbezpieczeństwa w organizacjach, kompetencje liderów w obszarze cyberbezpieczeństwa, strategie i podejście liderów w zarządzaniu cyberzagrożeniami, wyzwania dla liderów cyberbezpieczeństwa w erze cyfrowej transformacji (np. IoT, chmura, sztuczna inteligencja, technologie kwantowe), zarządzanie zespołami* |

| | |
|---|---|
| | *cyberbezpieczeństwa, przywództwo w sytuacjach kryzysowych (reagowanie na incydenty cyberbezpieczeństwa), planowanie i prowadzenie operacji w cyberprzestrzeni, zarządzanie budżetem i zasobami w dziedzinie cyberbezpieczeństwa, etyka i odpowiedzialność liderów, współpraca z zarządem i innymi interesariuszami, zarządzanie relacjami z partnerami i dostawcami zewnętrznymi, trendy i przyszłość przywództwa w cyberbezpieczeństwie.*<br><br>**4. Wstęp do zarządzania projektami** / 2 godz. /<br>*Definicja projektu i zarządzania projektem, kluczowe elementy zarządzania projektami (cele, zasoby, czas, budżet, jakość), rola menedżera projektu i jego zadania, cykl życia projektu, metodyki i podejścia do zarządzania projektami (tradycyjne np. Waterfall vs. metodyki zwinne Agile, Scrum, Kanban), zarządzanie zakresem, czasem, budżetem, jakością, zespołem, ryzykiem, interesariuszami, zmianą projektu, zarządzanie komunikacją w projekcie, technologie wspomagające zarządzanie projektami, zarządzanie projektem w kontekście międzynarodowym, etyka w zarządzaniu projektami, trendy i przyszłość zarządzania projektami.*<br><br>Ćwiczenia audytoryjne<br>**1. Budowa systemu zarządzania bezpieczeństwem informacji (SZBI) wg ISO/IEC 27001** / 6 godz. /<br>*Planowanie, projektowanie i budowanie systemu zarządzania bezpieczeństwem informacji, modelowanie zagrożeń i zarządzanie ryzykiem, narzędzia wykorzystywane do zarządzania ryzykiem.*<br><br>**2. Działania socjotechniczne** / 2 godz. /<br>*Czynniki wpływające na podatność użytkowników na ataki socjotechniczne, techniki obrony przed atakami socjotechnicznymi, rola organizacji w przeciwdziałaniu atakom socjotechnicznym, współpraca działów IT i HR w celu zmniejszenia ryzyka, przykłady ataków socjotechnicznych i ich psychologiczne aspekty, przyszłość cyberbezpieczeństwa i socjotechniki*<br><br>**3.** *Zarządzanie zespołami cyberbezpieczeństwa* **(Cyber Security Leadership)** / 4 godz. /<br>*Strategie i podejście liderów w zarządzaniu cyberzagrożeniami, praktyczne aspekty planowania, tworzenia i funkcjonowania działów cyberbezpieczeństwa, wymiarowanie zasobów, rekrutacja, przywództwo w sytuacjach kryzysowych (reagowanie na incydenty cyberbezpieczeństwa), planowanie i prowadzenie operacji w cyberprzestrzeni.*<br><br>**4. Zarządzanie ciągłością działania organizacji** / 4 godz. /<br>*Definicja ciągłości działania organizacji (Business Continuity Management – BCM), podstawowe zasady i elementy zarządzania ciągłością działania, kluczowe zasady i standardy BCM (np. ISO 22301), ocena ryzyka i analiza wpływu na działalność organizacji (Business Impact Analysis - BIA), BCM w kontekście zagrożeń w cyberprzestrzeni, tworzenie planu ciągłości działania, zarządzanie kryzysowe a zarządzanie ciągłością działania, zarządzanie zasobami i infrastrukturą w kontekście BCM, strategie odzyskiwania po awarii (Disaster Recovery – DR), zarządzanie łańcuchem dostaw monitorowanie i ocena skuteczności zarządzania ciągłością działania, przyszłość zarządzania ciągłością działania organizacji.*<br><br>**5. Audyt systemów teleinformatycznych** / 8 godz. /<br>*Definicja audytu systemów teleinformatycznych, rola audytu w zapewnieniu bezpieczeństwa i efektywności systemów teleinformatycznych, cele audytu teleinformatycznego, międzynarodowe standardy audytu (np. ISO/IEC 27001, ISO/IEC 27002, COBIT, NIST), rodzaje audytów systemów teleinformatycznych, planowanie i metodyka przeprowadzania audytu, testowanie odporności systemów IT na ataki (testy penetracyjne), ocena* |

| | |
|---|---|
| | *zarządzania incydentami i ciągłością działania, raportowanie wyników audytu.,*<br><br>Ćwiczenia laboratoryjne<br>**1. Zarządzanie operacjami w cyberprzestrzeni** / 32 godz. /<br>*Planowanie i prowadzenie operacji w cyberprzestrzeni, analiza zagrożeń (Threat Intelligence), zarządzanie podatnościami, informatyka śledcza, zarządzanie dostępem, zarządzanie incydentami* |
| Literatura | Podstawowa:<br>1. *Jason Edwards, Griffin Weaver, Cybersecurity Guide to Governance, Risk, and Compliance, John Wiley & Sons Inc, 2024*<br>2. *Douglas W. Hubbard, Richard Seiersen, Ryzyko w cyberbezpieczeństwie. Metody modelowania, pomiaru i szacowania ryzyka. Wydanie II, 2024*<br>3. *Hemang Doshi, CISA - Certified Information Systems Auditor Study Guide, Packt Publishing, 2024*<br>4. *Jakub Syta, Zarządzanie cyberbezpieczeństwem. Pracownicy, procesy, technologie, Wydawnictwo Naukowe PWN, 2025*<br>5. *Brumfield Cynthia, Cybersecurity Risk Management: Mastering the Fundamentals Using the Nist Cybersecurity Framework, John Wiley & Sons Inc, 2022*<br>6. *Lester Nichols, Cybersecurity Architect's Handbook, Packt Publishing, 2024*<br>7. *Allison Cerra, The Cybersecurity Playbook: How Every Leader and Employee Can Contribute to a Culture of Security, John Wiley & Sons Inc, 2019*<br>8. *Touhill Gregory J. ,Touhill C. Joseph, Cybersecurity for Executives: A Practical Guide", John Wiley & Sons Inc, 2014*<br>9. *Diogenes Yuri, Erdal Ozkaya, Cybersecurity - Attack and Defense Strategies - Second Edition: Counter modern threats and employ state-of-the-art tools and techniques to protect your organisation against cybercriminals, Packt Publishing, 2020*<br>10. *Joe Gray, Socjotechniki w praktyce. Podręcznik etycznego hakera, Helion, 2022*<br><br>Uzupełniająca:<br>1. *ISACA, The Risk IT Framework 2nd edition, ISACA, 2020*<br>2. *Normy ISO/IEC 27000 (27000, 27001:2022, 27003, 27005) - System Zarządzania Bezpieczeństwem Informacji*<br>3. *Norma ISO 31000:2018 - Zarządzanie ryzykiem*<br>4. *Norma ISO 9001 - System Zarządzania Jakością*<br>5. *Norma ISO 22301 - System Zarządzania Ciągłością Działania* |
| Metody i kryteria oceniania (sposób sprawdzania osiągnięcia przez słuchacza zakładanych efektów uczenia się) | Przedmiot zakończony jest: zaliczeniem z oceną.<br>Ćwiczenia audytoryjne zaliczane są zaliczeniem z oceną na podstawie zadań wykonanych w trakcie każdych ćwiczeń.<br>Ćwiczenia laboratoryjne zaliczane są zaliczeniem z oceną na podstawie sprawozdań wykonanych po każdym ćwiczeniu laboratoryjnym.<br>Zaliczenie przedmiotu jest prowadzone w formie pisemnego testu.<br>Warunkiem przystąpienia słuchacza do zaliczenia jest pozytywne zaliczenie ćwiczeń audytoryjnych oraz pozytywna ocena z ćwiczeń laboratoryjnych.<br><br>Osiągnięcie efektu W01, W02 oraz W03 weryfikowane jest podczas zaliczenia.<br>Osiągnięcie efektu U01, U02, U03, U04, U05, U06, U07, U08, U09, U10, U11, U12, U13, U14, U15, U16, K01, K02 oraz K03 sprawdzane jest w czasie ćwiczeń audytoryjnych oraz ćwiczeń laboratoryjnych. |

| | |
|---|---|
| | Ocenę **bardzo dobrą** otrzymuje słuchacz, który osiągnął zakładane efekty uczenia się na poziomie 91-100%.<br>Ocenę **dobrą plus** otrzymuje słuchacz, który osiągnął zakładane efekty uczenia się na poziomie 81-90%.<br>Ocenę **dobrą** otrzymuje słuchacz, który osiągnął zakładane efekty uczenia się na poziomie 71-80%.<br>Ocenę **dostateczną plus** otrzymuje słuchacz, który osiągnął zakładane efekty uczenia się na poziomie 61-70%.<br>Ocenę **dostateczną** otrzymuje słuchacz, który osiągnął zakładane efekty uczenia się na poziomie 51-60%.<br>Ocenę **niedostateczną** otrzymuje słuchacz, który osiągnął zakładane efekty uczenia się na poziomie równym lub niższym niż 50%. |
| Bilans ECTS<br>(nakład pracy słuchacza) | Aktywność / obciążenie słuchacza w godz.<br>*Udział w wykładach / 8*<br>*Udział w ćwiczeniach laboratoryjnych / 32*<br>*Udział w ćwiczeniach audytoryjnych / 24*<br>*Udział w seminariach / 0*<br>*Samodzielne studiowanie tematyki wykładów / 4*<br>*Samodzielne przygotowanie do ćwiczeń laboratoryjnych / 54*<br>*Samodzielne przygotowanie do ćwiczeń audytoryjnych / 18*<br>*Samodzielne przygotowanie do seminarium / 0*<br>*Realizacja projektu / 0*<br>*Udział w konsultacjach / 2*<br>*Przygotowanie do egzaminu / 0*<br>*Przygotowanie do zaliczenia / 8*<br>*Udział w egzaminie / 0*<br><br>Sumaryczne obciążenie pracą słuchacza: 150 godz. / 6 ECTS |

Wojskowa Akademia Techniczna

Wydział Elektroniki

**Opinia**
**Wydziałowej Rady ds. Kształcenia**
**Wydziału Elektroniki Wojskowej Akademii Technicznej**
**im. Jarosława Dąbrowskiego**

**Nr 91/RDK/WEL/2025 z dnia 26 sierpnia 2025 r.**

**w sprawie programu studiów podyplomowych**
**„Techniczne i organizacyjne aspekty cyberbezpieczeństwa"**
**dla naborów rozpoczynających się od r.a. 2025/2026**

Na podstawie § 92 ust. 1 pkt 1 Statutu WAT, stanowiącego załącznik do uchwały Senatu WAT nr 16/WAT/2019 z dnia 25 kwietnia 2019 r. w sprawie uchwalenia Statutu WAT (tj. obwieszczenie Rektora WAT nr 2/WAT/2024 z dnia 27 marca 2024 r.), wyraża się następującą opinię:

Wydziałowa Rada ds. Kształcenia Wydziału Elektroniki Wojskowej Akademii Technicznej im. Jarosława Dąbrowskiego wyraża pozytywną opinię o projekcie programu studiów podyplomowych „Techniczne i organizacyjne aspekty cyberbezpieczeństwa" dla naborów rozpoczynających się od r.a. 2025/2026, stanowiącym Załącznik do niniejszej opinii.

PRZEWODNICZĄCY
Wydziałowej Rady ds. kształcenia
WEL WAT
dr inż. Wiktor OLCHOWIK

Sporządziła Magdalena Grzybowska – Sekretarz Rady ds. Kształcenia

Wojskowa Akademia Techniczna

Wydział Cybernetyki

**Opinia**
**Wydziałowej Rady ds. Kształcenia**
**Wydziału Cybernetyki Wojskowej Akademii Technicznej**

**nr 37/WRdsK/2025 z dnia 14 października 2025 r.**

**w sprawie projektu programu Studiów Podyplomowych**
**„Techniczne i organizacyjne aspekty cyberbezpieczeństwa"**

Na podstawie § 92 ust. 1 pkt. 1 *Statutu WAT, stanowiącego załącznik do uchwały Senatu WAT nr 16/WAT/2019 z dnia 25 kwietnia 2019 r. w sprawie uchwalenia Statutu Wojskowej Akademii Technicznej im. Jarosława Dąbrowskiego* (tj. obwieszczenie Rektora WAT nr 2/WAT/2024 z dnia 27 marca 2024 r.) oraz § 17 ust. 1 pkt. 1 *Regulaminu Wydziałowej Rady do spraw Kształcenia Wydziału Cybernetyki Wojskowej Akademii Technicznej im. Jarosława Dąbrowskiego* stanowiącego załącznik *do decyzji Dziekana Wydziału Cybernetyki Wojskowej Akademii Technicznej im. Jarosława Dąbrowskiego nr 57/WCY/2019 z dnia 4 listopada 2019 r. w sprawie nadania regulaminu wydziałowej radzie do spraw kształcenia* ze zmianami wprowadzonymi *Decyzją Dziekana nr 32/WCY/2022 z dnia 28 czerwca 2022 r.* postanawia się, co następuje:

§ 1

Pozytywnie opiniuje się projekt programu Studiów Podyplomowych "Techniczne i organizacyjne aspekty cyberbezpieczeństawa" obowiązującego od roku 2025, stanowiący załącznik do niniejszej opinii.

PRZEWODNICZĄCY
Wydziałowej Rady ds. kształcenia
płk dr inż. Dariusz PIERZCHAŁA, prof. WAT