

## KARTA KURSU

<b>Nazwa</b>	<b>Wstęp do cyberbezpieczeństwa</b>
Nazwa w j. ang.	Introduction to Cybersecurity

Koordynator	prof. dr hab. inż. Anna Korchenko	Zespół dydaktyczny
		prof. dr hab. inż. Anna Korchenko
Punktacja ECTS*	2	

### Opis kursu (cele kształcenia)

Przedmiot „Wstęp do cyberbezpieczeństwa” ma na celu zapoznanie studentów z podstawowymi zasadami, pojęciami i praktykami cyberbezpieczeństwa, a także rodzajami cyberataków i specyfiką zagrożeń pojawiających się w cyberprzestrzeni. W trakcie kursu omawiane będą zagadnienia związane ze świadomością użytkowników dotyczącą wykrywania naruszeń bezpieczeństwa oraz kształtowanie zrozumienia znaczenia ochrony informacji we współczesnym cyfrowym świecie.

### Warunki wstępne

Wiedza	Podstawowa wiedza z zakresu obsługi komputera i technologii informatycznych
Umiejętności	Umiejętność analizowania i samodzielnego korzystania z literatury przedmiotu, a także obsługi podstawowych programów komputerowych
Kursy	Nie są wymagane żadne kursy wstępne

### Efekty uczenia się

	Efekt uczenia się dla kursu	Odniesienie do efektów kierunkowych
Wiedza	<p>Po zakończeniu kursu student:</p> <p>W01: podstawy i historia bezpieczeństwa informacji, pojęcia cyberbezpieczeństwa, cyberprzestrzeni.</p> <p>W02: potencjalne zagrożenia, podatności, cyberataki oraz inne destabilizujące czynniki w cyberprzestrzeni wpływające na współczesne państwa, społeczeństwa, podmioty prywatne.</p> <p>W03: pojęcie identyfikacji, metod uwierzytelniania, autoryzacji i kontrola dostępu, a także współczesne usługi i technologie internetowe.</p>	K_W06 K_W07

	Efekt uczenia się dla kursu	Odniesienie do efektów kierunkowych
Umiejętności	<p>Po zakończeniu kursu student:</p> <p>U01: stosować wiedzę z zakresu cyberbezpieczeństwa w działalności praktycznej (identyfikować potencjalne zagrożenia lub ataki, klasyfikować podstawowe zasady działania i typy złośliwego oprogramowania).</p> <p>U02: opisać zasady poufności, integralności i dostępności, związane ze stanem danych oraz środki zaradcze wobec zagrożeń cyberbezpieczeństwa.</p> <p>U03: rozpoznawać nowoczesne podejścia inżynierii społecznej, a także opisać taktyki, metody i procedury stosowane przez cyberprzestępców.</p> <p>U04: planować i realizować proces samokształcenia i rozwój zawodowy w sektorze cyberbezpieczeństwa, korzystać się literaturą z zakresu cyberbezpieczeństwa.</p>	K_U08 K_U11 K_U14

	Efekt uczenia się dla kursu	Odniesienie do efektów kierunkowych
Kompetencje społeczne	<p>Po zakończeniu kursu student:</p> <p>K01: wykazuje się wrażliwością na kwestię cyberbezpieczeństwa informacji w organizacji.</p> <p>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.</p> <p>K03: respektowania zasad etycznych i prawnych w cyberprzestrzeni oraz zobowiązań płynących z wykonywanego zawodu.</p>	K_K01 K_K02 K_K03

#### Studia stacjonarne

Organizacja											
Forma zajęć	Wykład (W)	Ćwiczenia w grupach									
		A		K		L		S		P	E
Liczba godzin	15	15									

#### Studia niestacjonarne

Organizacja											
Forma zajęć	Wykład (W)	Ćwiczenia w grupach									
		A		K		L		S		P	E
Liczba godzin	10	10									

## Opis metod prowadzenia zajęć

1. Wykłady: Podczas wykładów prowadzący przedstawiają materiał teoretyczny, wyjaśniają kluczowe koncepcje i metody oraz prezentują przykłady, ilustracje, slajdy i filmy. Wykłady mogą być prowadzone w auli lub online, a nagrania z nich mogą być udostępniane do późniejszego obejrzenia.
2. Ćwiczenia laboratoryjne: Ćwiczenia laboratoryjne pozwalają studentom przeprowadzać praktyczne eksperymenty z rzeczywistymi danymi, które pomagają studentom utrwalić wiedzę teoretyczną.
3. Dyskusje i zadania grupowe: Dyskusje i zadania grupowe promują wymianę wiedzy między studentami i zachęcają do wspólnego uczenia się. Metody te mogą obejmować forum dyskusyjne, grupowe projekty oraz wspólne rozwiązywanie zadań.
4. Samodzielne uczenie się: Dodatkowo, studentom mogą być udostępniane materiały do samodzielnego uczenia się, takie jak podręczniki, artykuły i kursy online. To pozwala studentom na pogłębienie swojej wiedzy i badanie tematów, które ich szczególnie interesują.
5. Testy i ocena: W trakcie kursu studenci mogą przechodzić testy i prace kontrolne w celu oceny swojego poziomu wiedzy i osiągnięć. Oceny te mogą obejmować zarówno egzaminy pisemne, jak i ocenę wyników ćwiczeń laboratoryjnych.

## Formy sprawdzania efektów uczenia się

	E – learning	Gry dydaktyczne	Ćwiczenia w szkole	Zajęcia terenowe	Praca laboratoryjna	Projekt indywidualny	Projekt grupowy	Udział w dyskusji	Referat	Praca pisemna (esej)	Egzamin ustny	Egzamin pisemny	Inne
W01	X				X			X					
W02	X				X			X					
W03	X				X			X					
U01	X				X			X					
U02	X				X			X					
U03	X				X			X					
U04	X				X			X					
K01	X				X			X					
K02	X				X			X					
K03	X				X			X					

### Kryteria oceny

Ocena końcowa jest zależna od ocen cząstkowych, systematyczności realizowanych zadań oraz oceny uzyskanej za realizację projektu zespołowego (indywidualnego). W szczególności ocenę dobrą i bardzo dobrą z ćwiczeń może uzyskać student, który: na podstawie zdobytej wiedzy samodzielnie identyfikuje potencjalne zagrożenia dla systemów informatycznych oraz potrafi analizować warunki, w jakich krążą odpowiednie ataki.

### Uwagi

Brak

## Treści merytoryczne (wykaz tematów)

1. Pojęcia cyberbezpieczeństwa i cyberprzestrzeni
  - Wartość cyberbezpieczeństwa dla różnych kierunków
  - Pojęcia cyberprzestrzeni
  - Pojęcia cyberbezpieczeństwa
2. Podstawy i historia bezpieczeństwa informacji
  - Znaczenie i definicja informacji
  - Cykl życia informacji
  - Istota bezpieczeństwa informacji
  - Modele bezpieczeństwa
3. Rodzaje ataków cybernetycznych.
  - Kategorie ataków
  - Zagrożenia, podatności i ryzyko

- Główne rodzaje cyberataków
4. Identyfikacja, uwierzytelnianie i zarządzanie hasłami
    - Identyfikacja
    - Uwierzytelnianie
    - Uwierzytelnianie wieloskładnikowe
    - Uwierzytelnianie wzajemne
    - Popularne metody identyfikacji i uwierzytelniania
  5. Autoryzacja i kontrola dostępu
    - Zasady procesu autoryzacji
    - Urządzenia kontroli dostępu
    - Wdrażanie kontroli dostępu
    - Modele kontroli dostępu
    - Fizyczna kontrola dostępu
  6. Zapobieganie atakom socjotechnicznym
    - Gromadzenie informacji na potrzeby ataków socjotechnicznych
    - Rodzaje ataków socjotechnicznych
    - Sześć zasad wykorzystywanych przez socjotechników
    - Rozpowszechnianie nadmiernych informacji w sieciach społecznościowych
    - Budowanie świadomości bezpieczeństwa użytkowników
  7. Zagrożenia bezpieczeństwa informacji
    - Zagrożenia dla bezpieczeństwa informacji w systemach informatycznych
    - Klasyfikacja zagrożeń bezpieczeństwa
    - Zarządzanie ryzykiem bezpieczeństwa informacji
    - Nowe technologie, nowe zagrożenia
  8. Identyfikowanie naruszeń bezpieczeństwa
    - Identyfikowanie jawnych włamań
    - Wykrywanie ukrytych włamań

#### Wykaz literatury podstawowej

1. Gańko, Katarzyna, Diana Kania, Emilia Troszczyńska-Roszczyk. *ABC cyberbezpieczeństwa*. Warszawa: NASK – Państwowy Instytut Badawczy, 2021. ISBN 978-83-65448-49-1. 104 s.
2. Bravo, Cesar. *Cyberbezpieczeństwo dla zaawansowanych. Skuteczne zabezpieczenia systemu Windows, Linux, IoT i infrastruktury w chmurze*. Gliwice: Helion, 2023. ISBN 978-83-283-9833-7. 456 s.
3. *Cyberbezpieczeństwo. Zarys wykładu*. Red. nauk. Cezary Banasiński ; Cezary Banasiński, Cezary Błaszczak, Jacek M. Chmielewski, Władysław Hydzik, Dariusz Jagiełło, Zuzanna Krauzowicz, Filip Krzyżankiewicz, Arwid Mednis, Włodzimierz Nowak, Marcin Rojszczak, Adam Szafranski, Ryszard Szpyra, Kazimierz Waćkowski, Paweł Widawski, Joanna Worona-Vlugt, Zofia Zawadzka. — Warszawa: Wolters Kluwer Polska, 2023. — Wydanie 2. — 588 s. — ISBN 978-83-8328-821-5.

#### Wykaz literatury uzupełniającej

1. *Wprowadzenie do bezpieczeństwa IT*. Tom 1 / red. Michał Sajdak ; Gynvael Coldwind, Michał Sajdak, Marek Rzepecki, Marcin Piosek, Bartosz Jerzman, Łukasz Basa, Wiktor Sędkowski, Wojciech Lesicki, Iwona Polak, Marcin Dudek, Krzysztof Wosiński, Tomasz Turba, Tomasz Dacka, Marek Zmysłowski, Grzegorz Trawiński, Konrad Jędrzejczyk, Piotr Ptaszek, Paweł Maziarz. — Warszawa: Wydawnictwo Securitum, 2023. — 942 s. — ISBN 978-83-968874-0-5.
2. *Wprowadzenie do bezpieczeństwa IT*. Tom 2 / red. nauk. Michał Sajdak ; Łukasz Olejnik, Grzegorz Tworek, Robert Przybylski, Karol Szafranski, Piotr Wojciechowski, Łukasz Bromirski, Maciej Szymczak, Arkadiusz Siczek, Kamil Jarosiński, Paweł Łąka, Mateusz Wójcik, Tomasz Turba, Piotr Rzeszut. — Warszawa: Wydawnictwo Securitum, 2024. — 814 s. — ISBN 978-83-968874-7-4.
3. Andress, Jason. *Podstawy bezpieczeństwa informacji. Praktyczne wprowadzenie*. Tłumaczenie: Grzegorz Kowalczyk. Warszawa: Helion, 2021. — 264 s. — ISBN: 978-83-283-8351-7.

Bilans godzinowy zgodny z CNPS (Całkowity Nakład Pracy Studenta) **studia stacjonarne**

liczba godzin w kontakcie z prowadzącymi	Wykład	15
	Konwersatorium (ćwiczenia, laboratorium itd.)	15
	Pozostałe godziny kontaktu studenta z prowadzącym	5
liczba godzin pracy studenta bez kontaktu z prowadzącymi	Lektura w ramach przygotowania do zajęć	10
	Przygotowanie krótkiej pracy pisemnej lub referatu po zapoznaniu się z niezbędną literaturą przedmiotu	0
	Przygotowanie projektu lub prezentacji na podany temat (praca w grupie)	0
	Przygotowanie do egzaminu/zaliczenia	5
Ogółem bilans czasu pracy		50
Liczba punktów ECTS w zależności od przyjętego przelicznika		2

Bilans godzinowy zgodny z CNPS (Całkowity Nakład Pracy Studenta) **studia niestacjonarne**

liczba godzin w kontakcie z prowadzącymi	Wykład	10
	Konwersatorium (ćwiczenia, laboratorium itd.)	10
	Pozostałe godziny kontaktu studenta z prowadzącym	5
liczba godzin pracy studenta bez kontaktu z prowadzącymi	Lektura w ramach przygotowania do zajęć	20
	Przygotowanie krótkiej pracy pisemnej lub referatu po zapoznaniu się z niezbędną literaturą przedmiotu	0
	Przygotowanie projektu lub prezentacji na podany temat (praca w grupie)	5
	Przygotowanie do egzaminu/zaliczenia	2
Ogółem bilans czasu pracy		50
Liczba punktów ECTS w zależności od przyjętego przelicznika		2