

KARTA KURSU

Nazwa	Wstęp do cyberbezpieczeństwa
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>K_W06: zasady działania aplikacji i usług elektronicznych w Internecie i w sieciach lokalnych ze szczególnym uwzględnieniem aspektów bezpieczeństwa.</p> <p>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.</p>	K_W06 K_W07
Umiejętności	<p>Po zakończeniu kursu student:</p> <p>K_U08: konfigurować urządzenia i protokoły sieciowe oraz nimi zarządzać, mając na uwadze bezpieczeństwo danych.</p> <p>K_U11: prawidłowo dostrzec, ocenić i interpretować zjawiska w zakresie cyberbezpieczeństwa oraz rozwoju nowych technologii w ujęciu historycznym, politycznym, społecznym, gospodarczym, militarnym, etycznym, prawnym (w tym w zakresie ochrony własności intelektualnej).</p> <p>K_U14: planować i realizować proces samokształcenia i rozwój zawodowy w branży IT, w szczególności w sektorze cyberbezpieczeństwa.</p>	K_U08 K_U11 K_U14

Kompetencje społeczne	Efekt uczenia się dla kursu	Odniesienie do efektów kierunkowych
	<p>Po zakończeniu kursu student:</p> <p>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.</p> <p>K_K02: krytycznej oceny poziomu swojej wiedzy oraz ciągłego doskonalenia się i konsultacji z innymi ekspertami z branży IT w szczególności związanej z cyberbezpieczeństwem, a także planowania własnego rozwoju zawodowego.</p> <p>K_K03: respektowania zasad etycznych i prawnych w cyberprzestrzeni oraz zobowiązań płynących z wykonywanego zawodu.</p>	<p>K_K01</p> <p>K_K02</p> <p>K_K03</p>

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
K_W06	X				X			X					
K_W07	X				X			X					
K_U08	X				X			X					
K_U11	X				X			X					
K_U14	X				X			X					
K_K01	X				X			X					
K_K02	X				X			X					
K_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)

- Pojęcia cyberbezpieczeństwa i cyberprzestrzeni
 - Wartość cyberbezpieczeństwa dla różnych kierunków
 - Pojęcia cyberprzestrzeni
 - Pojęcia cyberbezpieczeństwa
- Podstawy i historia bezpieczeństwa informacji
 - Znaczenie i definicja informacji
 - Cykl życia informacji
 - Istota bezpieczeństwa informacji
 - Modele bezpieczeństwa
- Rodzaje ataków cybernetycznych.
 - Kategorie ataków
 - Zagrożenia, podatności i ryzyko
 - Główne rodzaje cyberataków
- Identyfikacja, uwierzytelnianie i zarządzanie hasłami
 - Identyfikacja
 - Uwierzytelnianie
 - Uwierzytelnianie wieloskładnikowe
 - Uwierzytelnianie wzajemne
 - Popularne metody identyfikacji i uwierzytelniania
- Autoryzacja i kontrola dostępu
 - Zasady procesu autoryzacji
 - Urządzenia kontroli dostępu
 - Wdrażanie kontroli dostępu
 - Modele kontroli dostępu
 - Fizyczna kontrola dostępu
- Zapobieganie atakom socjotechnicznym
 - Gromadzenie informacji na potrzeby ataków socjotechnicznych
 - Rodzaje ataków socjotechnicznych
 - Sześć zasad wykorzystywanych przez socjotechników
 - Rozpowszechnianie nadmiernych informacji w sieciach społecznościowych

<ul style="list-style-type: none"> • Budowanie świadomości bezpieczeństwa użytkowników
7. Zagrożenia bezpieczeństwa informacji
<ul style="list-style-type: none"> • Zagrożenia dla bezpieczeństwa informacji w systemach informatycznych • Klasyfikacja zagrożeń bezpieczeństwa • Zarządzanie ryzykiem bezpieczeństwa informacji • Nowe technologie, nowe zagrożenia
8. Identyfikowanie naruszeń bezpieczeństwa
<ul style="list-style-type: none"> • Identyfikowanie jawnych włamań • Wykrywanie ukrytych włamań

Wykaz literatury podstawowej

1. Buchanan, Ben, The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations, Oxford University Press, New York 2017.
2. Klimburg, Alexander, The Darkening Web: The War for Cyberspace, Penguin Press, New York 2017.
3. Goodman, Marc, Future Crimes: Inside the Digital Underground and the Battle for Our Connected World, Anchor, New York 2016.

Wykaz literatury uzupełniającej

1. Liedel K., Piasecka P., Aleksandrowicz T.R. (red.), Sieciocentryczne bezpieczeństwo. Wojna, pokój i terroryzm w epoce informacji, Warszawa 2014.
2. Żywiołek, Justyna (2017) Bezpieczeństwo informacyjne: teoria i praktyka. Częstochowa: Oficyna Wydawnicza Stowarzyszenia Menedżerów Jakości i Produkcji, 2017.

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