**Nazwa przedmiotu:**

Wprowadzenie do cyberbezpieczeństwa

**Koordynator przedmiotu:**

dr hab. inż. Krzysztof Szczypiorski, prof. PW

**Status przedmiotu:**

Obowiązkowy

**Poziom kształcenia:**

Studia II stopnia

**Program:**

Matematyka

**Grupa przedmiotów:**

Wspólne

**Kod przedmiotu:**

.

**Semestr nominalny:**

3 / rok ak. 2021/2022

**Liczba punktów ECTS:**

4

**Liczba godzin pracy studenta związanych z osiągnięciem efektów uczenia się:**

1. godziny kontaktowe – 50 h; w tym
 a) obecność na wykładach – 30 h
 b) obecność na laboratoriach –15 h
 c) konsultacje – 5 h
2. praca własna studenta – 55 h; w tym
 a) przygotowanie do laboratoriów i do kolokwium – 50 h
 b) zapoznanie się z literaturą – 5 h
Razem 105 h, co odpowiada 4 pkt. ECTS

**Liczba punktów ECTS na zajęciach wymagających bezpośredniego udziału nauczycieli akademickich:**

a) obecność na wykładach – 30 h
b) obecność na laboratoriach – 15 h
c) konsultacje – 5 h
Razem 50 h, co odpowiada 2 pkt. ECTS

**Język prowadzenia zajęć:**

polski

**Liczba punktów ECTS, którą student uzyskuje w ramach zajęć o charakterze praktycznym:**

.

**Formy zajęć i ich wymiar w semestrze:**

|  |  |
| --- | --- |
| Wykład:  | 30h |
| Ćwiczenia:  | 0h |
| Laboratorium:  | 15h |
| Projekt:  | 0h |
| Lekcje komputerowe:  | 0h |

**Wymagania wstępne:**

brak

**Limit liczby studentów:**

Bez limitu

**Cel przedmiotu:**

Głównym celem przedmiotu jest wprowadzenie studentów do dziedziny inżynierii cyberbezpieczeństwa. W ramach przedmiotu omówione zostaną fundamentalne zagadnienia dotyczące bezpieczeństwa sieci, systemów i użytkowników wzajemnie na siebie oddziałowujących w świecie cyfrowym. Kontekstem wprowadzenia tych zagadnień będzie metodyka modelowania zagrożeń w cyberprzestrzeni poprzez identyfikację Łańcucha Śmierci (ang. Kill Chain). W dalszej kolejności zostanie dokonany przegląd głównych obszarów zapewniania bezpieczeństwa w cyberprzestrzeni. Każdy obszar zostanie scharakteryzowany właściwymi środkami technicznymi i nietechnicznymi.

**Treści kształcenia:**

1. Systemy cyber-fizyczne, cyberprzestrzeń i cyberbezpieczeństwo (2 godz.) Cyberprzestrzeń; sieci, systemy i użytkownicy; systemy cyber-fizyczne; modelowanie systemów; współczesne sieci i systemy; trendy; wprowadzenie do dziedziny cyberbezpieczeństwa; co to znaczy „zajmuję się cyberbezpieczeństwem?”, w kontekście: technicznym, naukowym, biznesowym, prawnym, ekonomicznym; model obszarów cyberbezpieczeństwa – zagadnienia, kompetencje i zawody; cyberbezpieczeństwo a bezpieczeństwo cybernetyczne.
2. Podstawowe zagadnienia z dziedziny cyberbezpieczeństwa (2 godz.)
Pojęcia fundamentalne dla dziedziny – CIA (Confidentiality, Integrity, Availability); podatność, zagrożenie, skutek, ryzyko; systemowe podejście do cyberbezpieczeństwa; modelowanie zagrożeń i ocena ryzyka; podejście klasyczne do modelowania zagrożeń; nowe metodyki modelowania i testowania bezpieczeństwa w kontekście Advanced Persisent Threats; wprowadzenie do modelowania bezpieczeństwa cyberprzestrzeni metodyką Kill Chain.
3. Zagrożenia w cyberprzestrzeni – metodyka Kill Chain: Rekonesans (2 godz.) Pozyskiwanie informacji o celach – podejścia, techniki, biały wywiad; wprowadzenie do wyszukiwania podatności (Vulnerability Assesment) sieci i systemów; planowanie ataków – podejścia, techniki, wektory ataku; wpływ ataków; metody in.
4. Zagrożenia w cyberprzestrzeni – metodyka Kill Chain: Techniki przygotowywania ataków i przełamywania zabezpieczeń; dystrybucja malware (2 godz.) Złośliwe oprogramowanie (malware): rodzaje, podstawowe pojęcia, architektura; metody dystrybucji złośliwego oprogramowania, w tym odniesienie do socjotechniki; warsztat analityka malware; wprowadzenie do klasycznych technik detekcji i analizy malware; nowe techniki detekcji i analizy malware; techniki unikania detekcji i utrudniania analizy malware.
5. Zagrożenia w cyberprzestrzeni – metodyka Kill Chain: Eksploitacja systemów, utrzymywanie dostępu i sterowanie atakami (2 godz.)
Podstawowe techniki przełamywania zabezpieczeń systemów operacyjnych i systemów komputerowych; przejmowanie kontroli i wykonywanie arbitralnego oprogramowania; techniki utrzymywania złośliwego oprogramowania w systemie; tylne furtki; sieci Malware, czyli botnety: podstawowe pojęcia, elementy, architektura; komunikacja i sterowanie atakami.
6. Zagrożenia w cyberprzestrzeni – metodyka Kill Chain: Ataki – case studies. (2 godz.) Cele atakujących; trendy i case study: ransomware, IoT botnets, cryptojacking, steganografia, botnet-as-a-service; Cyber Warfare; grupy APT i ich metody działania; wpływ społeczno-ekonomiczny ataków w cyberprzestrzeni; prawo a cyberprzestępstwa; etyka a cyberprzestrzępstwa.
7. Metody i środki obrony przed współczesnymi atakami na sieci, systemy i użytkowników: bezpieczeństwo systemów i oprogramowania (4 godz.) Mechanizmy bezpieczeństwa w systemach: uwierzytelnienie, kontrola dostępu; polityki bezpieczeństwa; monitorowanie, utrzymywanie i odzyskiwanie systemów; projektowanie, modelowanie, testowanie, audyt systemów i oprogramowania w kontekście cyberbezpieczeństwa; test penetracyjny, audyt bezpieczeństwa; etapy testu penetracyjnego, techniki i warsztat pentestera; tworzenie raportu z pentestów; Red Teaming, Blue Teaming, Purple Teaming; inżynieria odwrotna.
8. Metody i środki obrony przed współczesnymi atakami na sieci, systemy i użytkowników: bezpieczeństwo danych (4 godz.)
Kryptografia i kryptoanaliza; integralność i autentyczność danych; kontrola dostępu; protokoły bezpiecznej komunikacji; bezpieczeństwo przechowywania danych; prywatność; zastosowanie kryptografii w bezpieczeństwie systemów.
9. Metody i środki obrony przed współczesnymi atakami na sieci, systemy i użytkowników: bezpieczeństwo komunikacji (2 godz.)
Dobre praktyki zabezpieczenia sieci teleinformatycznych; sprzęt i oprogramowanie dla bezpieczeństwa teleinformatycznego: IDS/IPS, firewall, secure gateways, systemy kontroli dostępu, systemy bezpiecznej łączności; monitoring komunikacji sieciowej; analiza ruchu sieciowego dla cyberbezpieczeństwa; honeypots/honeynets; aplikacje analityczne, systemy SIEM.
10. Metody i środki obrony przed współczesnymi atakami na sieci, systemy i użytkowników: kryminalistyka cyfrowa (4 godz.)
Pojęcia podstawowe; pozyskiwanie danych śledczych z urządzeń cyfrowych: metody, zabezpieczanie materiału dowodowego, praca z materiałem dowodowym, akwizycja danych; pozyskiwanie danych śledczych jako strumieni komunikacji: kontekst sieci, systemów i użytkowników, przechwytywanie i analiza sieciowych strumieni komunikacji, przechwytywanie i analiza danych cyfrowych; techniki poszukiwań atakujących: biały wywiad, Dark Web, wywiad gospodarczy; Digital Forensics jako element zarządzania cyberbezpieczeństwem; aspekty prawne dochodzenia śledczego z dowodami cyfrowymi; metody kryminalistyki cyfrowej w kontekście prywatnym, compliance, spory prywatne.
11. Metody i środki obrony przed współczesnymi atakami na sieci, systemy i użytkowników: bezpieczeństwo organizacyjne, społeczne i zarządzanie cyberbepieczeństwem (2 godz.) Organizacja systemów bezpieczeństwa i zarządzanie incydentami; zarządzanie ryzykiem; strategia i planowanie polityk bezpieczeństwa organizacji; zarządzanie ryzykiem; Threat Intelligence i bezpieczeństwo oparte o analitykę danych; zarządzanie tożsamością użytkowników i systemów; inżyniera społeczna; prywatność zachowania i danych użytkowników; normy w zakresie cyberbezpieczeństwa.
12. Podsumowanie (2 godz.) Cyberbezpieczeństwo sieci, systemów i użytkowników jako wielowymiarowy proces; podsumowanie przedmiotu jako analizy bezpieczeństwa cyberprzestrzeni metodyką Kill Chain; metody zarządzania obroną przed atakiem typu APT: rodzaje reakcji na poszczególne ataki, formułowanie strategii koncentrującej się na coraz wcześniejszym przerywaniu łańcucha; orientacja rozwoju kompetencji inżyniera cyberbezpieczeństwa na kierunku Cyberbezpieczeństwo.

Zakres laboratorium:
1. Podstawy systemów operacyjnych i sieci teleinformatycznych
2. Pozyskiwanie informacji: rekonesans, skanowanie,
3. Testowanie bezpieczeństwa danych, aplikacji i systemów z wykorzystaniem specjalistycznych narzędzi.
4. Podstawy bezpieczeństwa systemów i oprogramowania
5. Wykorzystanie wirtualnej sieci komputerowej do wykonania ćwiczeń związanych zapewnianiem bezpieczeństwa cyberprzestrzeni. Realizacja zadania będzie obejmowała monitorowanie sieci i systemów, implementację mechanizmów bezpieczeństwa sieci i systemów oraz modelowania i symulowania zagrożeń w celu przetestowania wprowadzonych mechanizmów i zebrania dowodów wykonania ataków.

**Metody oceny:**

Regulamin zaliczenia przedmiotu

**Egzamin:**

nie

**Literatura:**

1. J. White, B. Clark: Blue Team Field Manual; 2017; CreateSpace Independent Publishing Platform.
2. Clark: Red Team Field Manual; 2014; CreateSpace Independent Publishing Platform.
3. Harper et al.: Gray Hat Hacking: The Ethical Hacker's Handbook, 5th Ed.; 2018; McGraw-Hill Education.
3. J. Luttgens, M. Pepe, K. Mandia: Incident Response & Computer Forensics, 3rd Ed.; 2014; McGraw-Hill Education.
4. SP 800-61: Computer Security Incident Handling Guide; Rev.2; 2012; US NIST.
5. Hadnagy: Social Engineering: The Art of Human Hacking; John Wiley & Sons; 1 edition (17 Dec. 2010).
Oprogramowanie:
1. Systemy operacyjne Windows, Linux, macOS – wersje klienckie i serwerowe.
2. Oprogramowanie open source i komercyjne do realizacji zadań praktycznych z zakresu przedmiotu:
 - emulacji sieci i systemów;
 - narzędzia do analizy, detekcji cyber zagrożeń;
 - narzędzia do monitoringu systemów, sieci i użytkowników;
 - narzędzia do wykonywania aktywnych testów bezpieczeństwa systemów, sieci i użytkowników.

**Witryna www przedmiotu:**

brak

**Uwagi:**

.

## Charakterystyki przedmiotowe

### Profil ogólnoakademicki - wiedza

**Charakterystyka WCB\_W01:**

Ma wiedzę dotyczącą fundamentalnych pojęć z zakresu cyberbezpieczeństwa

Weryfikacja:

Kolokwium pisemne

**Powiązane charakterystyki kierunkowe:** M2\_W04, M2MCB\_W02

**Powiązane charakterystyki obszarowe:**

**Charakterystyka WCB\_W02:**

Ma wiedzę z zakresu mechanizmów stosowanych w złośliwym oprogramowaniu i sieciach botnet

Weryfikacja:

Kolokwium pisemne

**Powiązane charakterystyki kierunkowe:** M2MCB\_W02

**Powiązane charakterystyki obszarowe:**

**Charakterystyka WCB\_W03:**

Ma podstawową wiedzę z zakresu testów penetracyjnych

Weryfikacja:

Kolokwium pisemne, zajęcia laboratoryjne

**Powiązane charakterystyki kierunkowe:** M2MCB\_W02

**Powiązane charakterystyki obszarowe:**

**Charakterystyka WCB\_W04:**

Ma podstawową wiedzę z zakresu kryminalistyki cyfrowej

Weryfikacja:

Kolokwium pisemne

**Powiązane charakterystyki kierunkowe:** M2MCB\_W02

**Powiązane charakterystyki obszarowe:**

**Charakterystyka WCB\_W05:**

Ma podstawową wiedzę z obszaru środków technicznych zapewniających cyberbezpieczeństwo sieci, systemów i użytkowników

Weryfikacja:

Kolokwium pisemne, zajęcia laboratoryjne

**Powiązane charakterystyki kierunkowe:** M2MCB\_W02

**Powiązane charakterystyki obszarowe:**

**Charakterystyka WCB\_W06:**

Ma podstawową wiedzę z obszaru bezpieczeństwa komunikacji w sieciach teleinformatycznych

Weryfikacja:

Kolokwium pisemne, zajęcia laboratoryjne

**Powiązane charakterystyki kierunkowe:** M2MCB\_W02

**Powiązane charakterystyki obszarowe:**

**Charakterystyka WCB\_W07:**

Ma podstawową wiedzę z zakresu modelowania zagrożeń w cyberprzestrzeni

Weryfikacja:

Kolokwium pisemne, zajęcia laboratoryjne

**Powiązane charakterystyki kierunkowe:** M2MCB\_W02

**Powiązane charakterystyki obszarowe:**

**Charakterystyka WCB\_W08:**

Ma podstawową wiedzę z zakresu zarządzania cyberbezpieczeństwem i aspektów społecznych w cyberprzestrzeni

Weryfikacja:

Kolokwium pisemne

**Powiązane charakterystyki kierunkowe:** M2MCB\_W02, M2\_W04

**Powiązane charakterystyki obszarowe:**

### Profil ogólnoakademicki - umiejętności

**Charakterystyka WCB\_U01:**

Potrafi przygotować środowisko pracy badacza cyberbezpieczeństwa systemów i sieci

Weryfikacja:

Zajęcia laboratoryjne, sprawozdanie

**Powiązane charakterystyki kierunkowe:** M2MCB\_U05

**Powiązane charakterystyki obszarowe:**

**Charakterystyka WCB\_U02:**

Potrafi przeprowadzić podstawowy test bezpieczeństwa zgodnie z przyjętą metodyką

Weryfikacja:

Zajęcia laboratoryjne, sprawozdanie

**Powiązane charakterystyki kierunkowe:** M2MCB\_U05

**Powiązane charakterystyki obszarowe:**

**Charakterystyka WCB\_U03:**

Potrafi stworzyć dokumentację z testów bezpieczeństwa zgodnie z przyjętą metodyką i wymaganiami

Weryfikacja:

Zajęcia laboratoryjne, sprawozdanie

**Powiązane charakterystyki kierunkowe:** M2MCB\_U05

**Powiązane charakterystyki obszarowe:**

**Charakterystyka WCB\_U04:**

Potrafi modelować zagrożenia w cyberprzestrzeni zgodnie z metodyką Cyber Kill Chain

Weryfikacja:

Zajęcia laboratoryjne, sprawozdanie

**Powiązane charakterystyki kierunkowe:** M2MCB\_U05

**Powiązane charakterystyki obszarowe:**

**Charakterystyka WCB\_U05:**

Potrafi stosować środki techniczne zapewniające cyberbezpieczeństwo sieci, systemów i użytkowników

Weryfikacja:

Zajęcia laboratoryjne, sprawozdanie

**Powiązane charakterystyki kierunkowe:** M2MCB\_U05

**Powiązane charakterystyki obszarowe:**

**Charakterystyka WCB\_U06:**

Potrafi skonfigurować i zabezpieczyć system końcowy lub oprogramowanie przed zagrożeniami w cyberprzestrzeni

Weryfikacja:

Zajęcia laboratoryjne, sprawozdanie

**Powiązane charakterystyki kierunkowe:** M2MCB\_U05

**Powiązane charakterystyki obszarowe:**

**Charakterystyka WCB\_U07:**

Potrafi zweryfikować w podstawowym zakresie czy system końcowy lub oprogramowanie mogą być zagrożone cyberatakami

Weryfikacja:

Zajęcia laboratoryjne, sprawozdanie

**Powiązane charakterystyki kierunkowe:** M2MCB\_U05

**Powiązane charakterystyki obszarowe:**

**Charakterystyka WCB\_U08:**

Potrafi w podstawowym zakresie przeprowadzić analizę zdarzeń w sieci i systemach w kierunku odkrycia niepożądanych akcji i anomalii

Weryfikacja:

Zajęcia laboratoryjne, sprawozdanie

**Powiązane charakterystyki kierunkowe:** M2MCB\_U05

**Powiązane charakterystyki obszarowe:**

**Charakterystyka WCB\_U09:**

Potrafi rozwiązywać zadania formułowane na bieżąco, komunikować wnioski i opinie, prowadzić na ich temat dyskusję i przekonywać innych

Weryfikacja:

Zajęcia laboratoryjne, sprawozdanie, prezentacja

**Powiązane charakterystyki kierunkowe:** M2MCB\_U05

**Powiązane charakterystyki obszarowe:**

**Charakterystyka WCB\_U10:**

Potrafi przygotować i przeprowadzić prezentację dotyczącą zagadnień technicznych związanych z problemem rozwiązywanym na bieżąco

Weryfikacja:

Zajęcia laboratoryjne, sprawozdanie, prezentacja

**Powiązane charakterystyki kierunkowe:** M2MCB\_U05

**Powiązane charakterystyki obszarowe:**

**Charakterystyka WCB\_U11:**

Potrafi krytycznie analizować dostępną literaturę z zakresu domeny wiedzy

Weryfikacja:

Zajęcia laboratoryjne, sprawozdanie, prezentacja

**Powiązane charakterystyki kierunkowe:** M2MCB\_U05

**Powiązane charakterystyki obszarowe:**

### Profil ogólnoakademicki - kompetencje społeczne

**Charakterystyka WCB\_K01:**

Ma świadomość konieczności komunikowania się z otoczeniem, także pozazawodowym, w sposób zrozumiały dla odbiorcy

Weryfikacja:

Zajęcia laboratoryjne, wykład

**Powiązane charakterystyki kierunkowe:** M2MCB\_K01

**Powiązane charakterystyki obszarowe:**

**Charakterystyka WCB\_K02:**

Ma orientację zawodową w obszarze inżynierii cyberbepieczeństwa i jest świadomy procesu uczenia się w kierunku zwiększania kompetencji w tym obszarze

Weryfikacja:

Zajęcia laboratoryjne, wykład

**Powiązane charakterystyki kierunkowe:** M2\_K01, M2\_K03

**Powiązane charakterystyki obszarowe:**

**Charakterystyka WCB\_K03:**

Ma świadomość uwarunkowań etycznych i prawnych związanych z działalnością naukową, dydaktyczną, wdrożeniową i biznesową.

Weryfikacja:

Zajęcia laboratoryjne, wykład

**Powiązane charakterystyki kierunkowe:** M2\_K04

**Powiązane charakterystyki obszarowe:**