| Sylabus przedmiotu / modułu kształcenia | | |
|---|---|---|
| **Nazwa przedmiotu/modułu kształcenia:** | Problemy bezpieczeństwa komputerowego w systemach informatycznych | |
| **Nazwa w języku angielskim:** | Contemporary Computer Security Issues in Information Systems | |
| **Język wykładowy:** | polski | |
| **Kierunek studiów, dla którego przedmiot jest oferowany:** | informatyka | |
| **Jednostka realizująca:** | Wydział Nauk Ścisłych i Przyrodniczych | |
| **Rodzaj przedmiotu/modułu kształcenia (obowiązkowy/fakultatywny):** | fakultatywny | |
| **Poziom modułu kształcenia (np. pierwszego lub drugiego stopnia, jednolitych magisterskich):** | drugiego stopnia | |
| **Rok studiów:** | pierwszy | |
| **Semestr:** | drugi | |
| **Liczba punktów ECTS:** | 4 | |
| **Imię i nazwisko koordynatora przedmiotu:** | dr Piotr Świtalski | |
| **Imię i nazwisko prowadzących zajęcia:** | dr Piotr Świtalski | |
| **Założenia i cele przedmiotu:** | Założeniem tego przedmiotu jest znajomość przez słuchaczy zagadnień związanych z podstawami bezpieczeństwa komputerowego.<br><br>Celem przedmiotu jest pogłębienie wiedzy o bezpieczeństwie systemów komputerowych. W założeniu ma również usystematyzowanie wiedzy w zakresie najnowszych technologii i systemów bezpieczeństwa komputerowego. | |

| **Symbol efektu** | **Efekty uczenia się** | **Symbol efektu kierunkowego** |
|---|---|---|
| | **WIEDZA**<br>**Student zna i rozumie:** | |
| **W_01** | technologie oraz systemy służące do zapewnienia bezpieczeństwa komputerowego | **W_S01, W_S05** |
| **W_02** | jaki wpływ na bezpieczeństwo komputerowe mają zastosowane technologie i rozwiązania informatyczne | **W_S05** |
| | **UMIEJĘTNOŚCI**<br>**Student potrafi:** | |
| **U_01** | wdrożyć technologie bezpieczeństwa komputerowego w istniejącym oprogramowaniu | **U_S01, U_S04** |
| **U_02** | zastosować bezpieczne protokoły uwierzytelniania w systemie komputerowym | **U_S04** |
| **U_03** | skonfigurować oprogramowanie służące bezpieczeństwu komputerowemu | **U_S04** |

| | |
|---|---|
| **Forma i typy zajęć:** | • studia stacjonarne: wykłady (20 godz.), ćwiczenia laboratoryjne (24 godz.)<br>• studia niestacjonarne: wykłady (10 godz.), ćwiczenia laboratoryjne (15 godz.) |

| **Wymagania wstępne i dodatkowe:** |
|---|
| Warunkiem uczestnictwa w zajęciach jest znajomość podstaw bezpieczeństwa komputerowego. |

**Treści modułu kształcenia:**

1. **Zarządzanie kluczami i ich dystrybucja.** Dystrybucja kluczy (symetryczna/asymetryczna). Transparentne zarządzanie kluczami. Zdecentralizowana organizacja kluczy. Publiczne ogłoszenie klucza. Certyfikaty kluczy publicznych. Standard X.509. Infrastruktura klucza publicznego (PKI).
2. **Uwierzytelnianie użytkowników i protokoły bezpieczeństwa**. Uwierzytelnianie jednokierunkowe i wzajemne. Uwierzytelnianie zdalne (symetryczne i asymetryczne). Kerberos. Protokoły uwierzytelniania w sieciach. PAKE (Password-Authenticated Key Exchange). SAML, OAuth, OpenID Connect.
3. **Współczesne technologie uwierzytelniania użytkowników.** Statyczne uwierzytelnienie. Hasła jednorazowe. Wieloetapowe uwierzytelnianie (MFA). Tokeny sprzętowe. Proces uwierzytelniania i asercje. TPM jako element uwierzytelniania. FIDO, UAF, FDO. Passkeys (FIDO 2). Problemy tożsamości: MFA fatigue, token theft. Ciągłe uwierzytelnianie.
4. **Biometria i identyfikacja użytkowników.** Biometria statyczna. Biometria behawioralna. Biometria multimodalna. Algorytmy i modele biometryczne. Bezpieczeństwo metod biometrycznych. Ataki na biometrię (spoofing, deepfake). Ochrona danych biometrycznych: biometria anulowalna. Integracja biometrii z systemami uwierzytelniania. Biometria w kryptografii.
5. **Łańcuchy bloków i decentralizacja w bezpieczeństwie.** Historia. Typy łańcuchów bloków. Algorytmy konsensusu. Metody decentralizacji. Smart contracts. Platformy blockchain. Bezpieczeństwo łańcuchów bloków. Zdecentralizowana tożsamość (DID).
6. **Bezpieczeństwo sprzętowe.** Trusted Computing. Hardsec. Ataki kanałów bocznych. Ataki elektromagnetyczne i czasowe. Nowe warianty Spectre/Meltdown. Intel SGX (Software Guard Extensions). UEFI Secure Boot. Ataki na TPM i Secure Enclave. Fingerprinting urządzeń i użytkowników. Rowhammer i pokrewne ataki na pamięć.
7. **Bezpieczeństwo Internetu rzeczy i Edge Computing.** Uwierzytelnianie i autoryzacja w urządzeniach. Smart Home. Automatyczne aktualizacje. Ochrona danych osobowych. Ataki na IoT i Edge Computing. Cyfrowy bliźniak (Digital Twin) w IoT. Bezpieczeństwo protokołów przemysłowych: Modbus, OPC UA.
8. **Najnowsze ataki i współczesne zagrożenia bezpieczeństwa komputerowego.** Ataki wspierane przez sztuczną inteligencję. Zaawansowana socjotechnika. Ransomware 3.0. Ataki na chmurę i SaaS. Ataki na łańcuchy CI/CD: dependency confusion, artifact poisoning. Ataki na modele sztucznej inteligencji: prompt injection, model extraction.
9. **Inteligentne systemy wykrywania zagrożeń.** Metody wykrywania anomalii. Architektura inteligentnych systemów detekcji. Sztuczna inteligencja w systemach detekcji. Automatyzacja reakcji na incydenty: SIEM + SOAR. Graph-based anomaly detection (GBAD). Uczenie federacyjne w detekcji zagrożeń.
10. **Projektowanie uniwersalne w systemach inteligentnych.** Zasady projektowania uniwersalnego. Identyfikacja potrzeb osób ze szczególnymi potrzebami. Dostępność wspierana przez sztuczną inteligencję. Bezpieczeństwo a dostępność.

**Literatura podstawowa:**


1. Stallings W., Brown L.: Bezpieczeństwo systemów informatycznych. Zasady i praktyka, Wydanie IV. Tom I i II, Helion, Gliwice, 2023.
2. Bashir I.: Blockchain. Zaawansowane zastosowania łańcucha bloków. Wydanie II, Helion, 2019
3. McIlwraith D., Marmanis H., Babenko D.: Inteligentna sieć. Algorytmy przyszłości. Wydanie II, Helion, 2017


**Literatura dodatkowa:**

1. Khawaja G.: Kali Linux i testy penetracyjne. Biblia. Wyd. Helion, Gliwice, 2022.
2. Prasad P.: Testy penetracyjne nowoczesnych serwisów. Kompendium inżynierów bezpieczeństwa, Helion, 2017.

**Planowane formy/działania/metody dydaktyczne:**

Wykład tradycyjny wspomagany jest technikami multimedialnymi. Ćwiczenia laboratoryjne – zajęcia praktyczne z wykorzystaniem wybranych narzędzi programowych. Na stronie internetowej prowadzącego zamieszczane są materiały z problemami i zadaniami laboratoryjnymi.

**Sposoby weryfikacji efektów uczenia się osiąganych przez studenta:**

| Symbol efektu | Metody weryfikacji efektów uczenia się |
|---|---|
| **W_01** | Efekt realizowany na egzaminie w formie pisemnej. Przykładowe pytanie: „Na czym polega zdecentralizowana organizacja kluczy?”. |
| **W_02** | Efekt realizowany na egzaminie w formie pisemnej. Przykładowe pytanie: „Przedstaw rodzaje ataków wymierzonych na modele sztucznej inteligencji”. |
| **U_01** | Efekt realizowany w trakcie zajęć laboratoryjnych. Przykładowe zadanie: „Skonfiguruj urząd certyfikacji. Wygeneruj certyfikat przez ten urząd. Unieważnij ten certyfikat i utwórz listę CRL”. |
| **U_02** | Efekt realizowany w trakcie zajęć laboratoryjnych. Przykładowe zadanie: „Zaimplementuj JSON Web Token”. |
| **U_03** | Efekt realizowany w trakcie zajęć laboratoryjnych. Przykładowe zadanie: „Utwórz konfigurację Kerberosa dla domeny uws.edu.pl. Utwórz bazę danych Kerberosa dla tej domeny”. |

**Forma i warunki zaliczenia:**

Ocena z przedmiotu składa się z dwóch ocen cząstkowych:

- oceny z zajęć laboratoryjnych,
- oceny z egzaminu końcowego.

Na ocenę z zajęć laboratoryjnych składają się oceny cząstkowe uzyskane na regularnych zajęciach z nauczycielem akademickim, za które można uzyskać sumarycznie 50 pkt. Zaliczenie zajęć laboratoryjnych możliwe po uzyskaniu co najmniej 51% liczby punktów z tej formy zaliczenia

Egzamin jest egzaminem pisemnym. Do egzaminu mogą przystąpić osoby, które uzyskały zaliczenie laboratorium. Na egzaminie można uzyskać maksymalnie 50 pkt. Egzamin będzie zaliczony w przypadku uzyskania co najmniej 51% liczby punktów z tej formy zaliczenia.

Ocena końcowa, w zależności od sumy uzyskanych punktów (maksymalnie 100 pkt) jest następująca (w nawiasach ocena wg skali ECTS):

- 0 – 50 pkt: niedostateczna (F),
- 51 – 60 pkt: dostateczna (E),
- 61 – 70 pkt: dostateczna plus (D),
- 71 – 80 pkt: dobra (C),
- 81 – 90 pkt: dobra plus (B),
- 91 – 100 pkt: bardzo dobra (A).

**Bilans punktów ECTS:**

| Studia stacjonarne | |
|---|---|
| Aktywność | Obciążenie studenta |
| Udział w wykładach | 20 godz. |
| Udział w ćwiczeniach laboratoryjnych | 24 godz. |
| Przygotowanie się i udział w egzaminie | 16 godz. |
| Przygotowanie się do ćwiczeń laboratoryjnych | 38 godz. |
| Udział w konsultacjach z przedmiotu | 2 godz. |
| **Sumaryczne obciążenie pracą studenta** | **100 godz.** |
| **Punkty ECTS za przedmiot** | **4 ECTS** |

| Studia niestacjonarne | |
|---|---|
| Aktywność | Obciążenie studenta |
| Udział w wykładach | 10 godz. |
| Udział w ćwiczeniach laboratoryjnych | 15 godz. |
| Przygotowanie się i udział w egzaminie | 30 godz. |
| Przygotowanie się do ćwiczeń laboratoryjnych | 43 godz. |
| Udział w konsultacjach z przedmiotu | 2 godz. |
| **Sumaryczne obciążenie pracą studenta** | **100 godz.** |
| **Punkty ECTS za przedmiot** | **4 ECTS** |