Sylabus przedmiotu / modułu kształcenia – studia podyplomowe	
Nazwa przedmiotu/modułu kształcenia:	**Bezpieczeństwo systemów informatycznych**
Nazwa w języku angielskim:	Security of information systems
Język wykładowy:	polski
Studia podyplomowe dla których oferowany jest przedmiot/moduł kształcenia:	Podyplomowe studia cyberbezpieczeństwa
Dziedzina/dziedziny nauki, w ramach których prowadzone są studia podyplomowe:	informatyka
Jednostka realizująca:	Instytut Informatyki
Rodzaj przedmiotu/modułu kształcenia (obowiązkowy/fakultatywny):	obowiązkowy
Rok studiów:	1
Semestr:	2
Liczba punktów ECTS:	2
Imię i nazwisko koordynatora przedmiotu:	dr Piotr Świtalski
Imię i nazwisko prowadzących zajęcia:	dr Piotr Świtalski
Założenia i cele przedmiotu:	Celem przedmiotu jest zaznajomienie studentów z problematyką bezpieczeństwa systemów komputerowych. Przedmiot ma za zadanie zapoznanie z klasycznymi technikami bezpieczeństwa w systemach komputerowych. W założeniach do tego przedmiotu przewiduje się zajęcia praktyczne z użyciem komputerów, podczas których studenci nabędą umiejętności z atakami na systemy komputerowe i również metody przeciwdziałania im. Dodatkowo studenci poznają techniki zabezpieczania baz danych. Ma również usystematyzować wiedzę w zakresie standardów bezpieczeństwa.
Efekty uczenia się (wiedza, umiejętności, kompetencje społeczne):	WIEDZA: • Student zna i rozumie zagadnienia z zakresu bezpieczeństwa systemów komputerowych • Student zna i rozumie mechanizmy bezpieczeństwa komputerowego i potrafi je wykorzystać w przedstawionym środowisku
	UMIEJĘTNOŚCI: • Student potrafi sprawnie wykorzystać narzędzia bezpieczeństwa systemów komputerowych

	• Student potrafi dobrać adekwatne zabezpieczenia w stosunku do zagrożenia w systemie komputerowym
Forma i typy zajęć:	wykłady (10 godz.), ćwiczenia laboratoryjne (18 godz.)

Wymagania wstępne i dodatkowe:

Warunkiem uczestnictwa w zajęciach jest posiadanie podstawowej wiedzy i umiejętności z zakresu obsługi systemu operacyjnego Linuks

Treści modułu kształcenia:

1. **Charakterystyka zagrożeń w systemach informatycznych oraz przestępczość komputerowa.** Podstawowe zasady. Właściwości i klasyfikacja koncepcji bezpieczeństwa: integralność, dostępność, poufność, niezaprzeczalność, odpowiedzialność. Podstawowe pojęcia. Model bezpieczeństwa sieciowego. Minimalne standardy bezpieczeństwa. Polityka bezpieczeństwa. Specyfika systemów informatycznych. Klasyfikacja zagrożeń. Zagrożenia związane z DNS. Złośliwe oprogramowanie. Sieci botnet. Statystyka typowych zagrożeń Przestępstwa ujawnione i nieujawnione. Obiekty, typy i sprawcy przestępstw. Piractwo komputerowe, sabotaż, wywiad gospodarczy, szpiegostwo, przestępstwa bankowe. Inżynieria społeczna. Phising. Inżynieria odwrotna. Organizacje przeciwdziałające przestępczości komputerowej.
2. **Podpis cyfrowy.** Idea podpisu cyfrowego. Wymagania stawiane podpisom cyfrowym. Mechanizm uwierzytelniania komunikatów. Kody uwierzytelnienia komunikatów MAC. Podpis cyfrowy ElGamal. Standard DSS. Algorytm DSA. Kryptograficzne funkcje haszujące. Algorytm SHA-512. Paradoks urodzin.
3. **Uwierzytelnianie.** Pojęcie uwierzytelniania. Uwierzytelnianie przez hasło. Strategie wyboru haseł. Inne metody uwierzytelniania. Protokoły uwierzytelniania: protokół challenge and response. Atak „człowiek pośrodku”. Dowód z wiedzą zerową. Uwierzytelnianie dwuskładnikowe. Hasło jednorazowe. Generowanie haseł jednorazowych – protokół S/KEY.
4. **Szkodliwe oprogramowanie.** Problemy związane z nieautoryzowanym dostępem do systemów komputerowych. Infekcje systemów komputerowych. Bezpieczny system operacyjny. Podatność systemów operacyjnych. Charakterystyka szkodliwego oprogramowania: tylne drzwi, bomby logiczne, konie trojańskie, wirusy, robaki, eksploity i rootkity, keyloggery. Przeciwdziałanie szkodliwemu oprogramowaniu.
5. **Zapory sieciowe (firewalle).** Model ogólny zapory sieciowej. Charakterystyka firewalli. Ograniczenia firewalli. Firewall filtrujący pakiety. Firewall filtrujący pakiety z badaniem stanu pakietu. Brama aplikacyjna, brama transmisyjna. Implementacja firewalla. Strefa zdemilitaryzowana (DMZ). Przykładowa konfiguracja firewalla z DMZ.
6. **Systemy wykrywania intruzów.** Zachowania intruzywne. Wzorce zachowań intruzów. Wykrywanie intruzów. Statystyczna analiza zachowania. Wykrywanie intruzów w oparciu o reguły. Systemy IDPS. Audyt w systemach IDPS. Pułapki (Honeypoty).
7. **Bezpieczeństwo systemów internetowych.** Ataki w warstwie aplikacji. Przepełnienie bufora. Wstrzykiwanie kodu. Ataki SQL Injection. Błędy w uwierzytelnianiu użytkownika i zarządzania jego sesją. Atak XSS. Błędy w konfiguracji oprogramowania. Niewłaściwe zabezpieczenie wrażliwych danych. Atak Cross-Site Request Forgery (CSRF).
8. **Zapewnianie dostępności danych.** Utrzymanie ciągłości zasilania. Sposoby zapobiegania problemom zasilania, zasilacze awaryjne UPS. Ochrona danych przed utratą. Systemy macierzowe RAID. Kopie bezpieczeństwa.

Literatura podstawowa:

1. Stallings W., Brown L.: Bezpieczeństwo systemów informatycznych. Zasady i praktyka, Wydanie IV. Tom 1, Wyd. Helion, Gliwice, 2023.
2. Khawaja G.: Kali Linux i testy penetracyjne. Biblia. Wyd. Helion, Gliwice, 2022.

Literatura dodatkowa:

1. Stallings W., Brown L.: Bezpieczeństwo systemów informatycznych. Zasady i praktyka, Wydanie IV. Tom 2, Wyd. Helion, Gliwice, 2023.
2. Janca T.: Alicja i Bob. Bezpieczeństwo aplikacji w praktyce. Wyd. Helion, Gliwice, 2021.
3. Tevault D. A.: Bezpieczeństwo systemu Linux. Hardening i najnowsze techniki zabezpieczania przed cyberatakami, Wyd. Helion, Gliwice, 2024.

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:

Efekty z zakresu wiedzy weryfikowane będą poprzez egzamin pisemny, a także w toku weryfikacji przygotowania do kolejnych zajęć laboratoryjnych. Na egzaminie pisemnym pytania będą dotyczyły poznanych technik ataków i sposobów zabezpieczania systemów komputerowych. Przykładowe pytania:

- Przedstaw schemat działania podpisu cyfrowego.
- Na czym polega uwierzytelnianie dwuskładnikowe?
- W jaki sposób przeprowadzany jest atak DDoS?

Przed egzaminem studenci będą mieli dostęp do przykładowych pytań na egzamin.

Efekty związane z umiejętnościami będą sprawdzane systematycznie na zajęciach laboratoryjnych. Materiały na następne laboratorium będą dostępne na dwa dni przed zajęciami.

Forma i warunki zaliczenia (wraz z kryteriami oceniania):

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 40 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. Można na nim uzyskać maksymalnie 60 pkt. Egzamin będzie zaliczony w przypadku uzyskania co najmniej 51% liczby punktów z tej formy zaliczenia. Ocena końcowa z przedmiotu, 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:	
Aktywność	Obciążenie studenta
Udział w wykładach	10 godz.
Udział w ćwiczeniach laboratoryjnych	18 godz.
Przygotowanie się do egzaminu	12 godz.
Przygotowanie się do ćwiczeń laboratoryjnych	8 godz.
Udział w konsultacjach z przedmiotu	2 godz.
Sumaryczne obciążenie pracą studenta	**50 godz.**
Punkty ECTS za przedmiot	**2 ECTS**