KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu
Bezpieczeństwo sektora finansowego [S1Cybez1>BSF]

Przedmiot

Kierunek studiów
Cyberbezpieczeństwo

Rok/Semestr
4/7

Studia w zakresie (specjalność)
–

Profil studiów
ogólnoakademicki

Poziom studiów
pierwszego stopnia

Język oferowanego przedmiotu
polski

Forma studiów
stacjonarne

Wymagalność
obieralny

Liczba godzin

Wykład
16

Laboratorium
0

Inne
0

Ćwiczenia
0

Projekty/seminaria
16

Liczba punktów ECTS

2,00

Koordynatorzy

prof. dr hab. inż. Mariusz Głąbowski
mariusz.glabowski@put.poznan.pl

Wykładowcy

Wymagania wstępne

Podstawowa znajomość zasad funkcjonowania systemów informatycznych oraz ogólna wiedza z zakresu cyberbezpieczeństwa.

Cel przedmiotu

Celem przedmiotu jest rozwinięcie wiedzy i umiejętności związanych z bezpieczeństwem w sektorze finansowym, ze szczególnym uwzględnieniem elektronicznych systemów płatności. Studenci poznają najnowsze technologie, metody ataków oraz środki ich zapobiegania, a także specyfikę przestępczości finansowej.

Przedmiotowe efekty uczenia się

Wiedza • Student zna mechanizmy funkcjonowania elektronicznych systemów płatności i form płatności bezgotówkowych. [K1_W05]
• Rozumie zagrożenia związane z bankowością elektroniczną i systemami płatności w e-commerce. [K1_W17]
• Zna podstawowe metody i narzędzia używane w atakach socjotechnicznych oraz sposoby ich identyfikacji. [K1_W20]

• Posiada wiedzę o przestępstwach finansowych, takich jak phishing, malware i pranie pieniędzy. [K1_W20]
• Zna zasady zarządzania tożsamością i dostępem (IAM) w sektorze finansowym. [K1_W17]
Umiejętności • Student potrafi identyfikować symptomy wskazujące na przygotowanie ataku na elektroniczne systemy płatności. [K1_U04]
• Umie analizować przypadki ataków na bankowość elektroniczną oraz projektować odpowiednie środki zapobiegawcze. [K1_U06]
• Tworzy procedury uwierzytelniania wieloskładnikowego oraz zarządza dostępem do zasobów krytycznych. [K1_U02]
• Wykorzystuje narzędzia i metody analizy behawioralnej w wykrywaniu zagrożeń. [K1_U08]
Kompetencje społeczne • Student rozumie znaczenie ochrony finansowej i technologicznej w kontekście bezpieczeństwa publicznego. [K1_K03]
• Jest świadomy dynamicznego charakteru zagrożeń w sektorze finansowym i konieczności stałego aktualizowania wiedzy.[K1_K01]
• Współpracuje w zespole, realizując zadania związane z analizą i zapobieganiem przestępstwom finansowym.[K1_K05]

Umiejętności:
-

Kompetencje społeczne:
-

Metody weryfikacji efektów uczenia się i kryteria oceny

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:

Test pisemny (wiedza): Test oraz pytania otwarte sprawdzające znajomość mechanizmów systemów płatności, zagrożeń i metod przeciwdziałania.
• Projekt zespołowy (umiejętności i kompetencje społeczne): Opracowanie planu ochrony systemu finansowego z uwzględnieniem analizy ryzyka.
W każdej formie zaliczenia przedmiotu ocena zależy od liczby zdobytych przez studenta punktów w stosunku do maksymalnej liczby punktów obowiązkowych. Warunkiem pozytywnego zaliczenia jest otrzymanie co najmniej 50% punktów możliwych do zdobycia. Zależność oceny od liczby punktów definiuje Regulamin Studiów. Dodatkowo zasady zaliczania przedmiotu i dokładne progi zaliczeniowe zostaną przekazane studentom na początku semestru z wykorzystaniem uczelnianych systemów elektronicznych oraz na pierwszych zajęciach (w każdej formie zajęć).

Treści programowe

Elektroniczne systemy płatności
2. Zagrożenia dla systemów finansowych
3. Ataki na systemy finansowe
4. Zarządzanie bezpieczeństwem sektora finansowego
5. AI w sektorze finansowym

Tematyka zajęć

1: Wprowadzenie do elektronicznych systemów płatności (90 minut)
- Historia i ewolucja płatności elektronicznych.
- Rodzaje i formy płatności bezgotówkowych: karty płatnicze, przelewy elektroniczne, płatności mobilne.
- Przegląd systemów e-commerce: platformy i mechanizmy płatności.
- Portfele elektroniczne: funkcjonalność, przykłady (np. PayPal, Google Pay, Apple Pay).
2: Zagrożenia związane z bankowością elektroniczną (90 minut)
- Podstawowe zagrożenia dla użytkowników prywatnych i instytucjonalnych.
- Przegląd metod ataków: keylogger, man-in-the-middle, credential stuffing.
- Omówienie działań prewencyjnych w kontekście ochrony bankowości elektronicznej.
- Case study: typowe błędy użytkowników skutkujące utratą środków.
4
3: Przestępstwa w obrocie bezgotówkowym (90 minut)
- Definicje i klasyfikacja przestępstw finansowych: phishing, malware, pranie pieniędzy.
- Analiza zagrożeń związanych z oprogramowaniem złośliwym dedykowanym systemom finansowym.

- Mechanizmy prania pieniędzy z wykorzystaniem systemów płatności elektronicznych.
- Studium przypadku: analiza wykrytych przypadków nadużyć.
4: Ataki na systemy finansowe – etapy i metody (90 minut)
- Etapy przygotowania ataku: rozpoznanie, identyfikacja luk w zabezpieczeniach.
- Analiza zabezpieczeń i możliwości ich obejścia.
- Socjotechnika w praktyce: phishing, spear phishing, vishing – definicje i różnice.
- Przykłady rzeczywistych incydentów z sektora finansowego.
5: Zarządzanie bezpieczeństwem w sektorze finansowym (cz. 1) (90 minut)
- Zarządzanie tożsamością i dostępem (IAM): mechanizmy i standardy.
- Uwierzytelnianie wieloskładnikowe (MFA): techniki, wady i zalety.
- Zarządzanie krytycznymi zasobami i systemami.
- Praktyczne aspekty ochrony danych klientów w instytucjach finansowych.
6: Zarządzanie bezpieczeństwem w sektorze finansowym (cz. 2) (90 minut)
- Analiza behawioralna jako narzędzie wykrywania nietypowych działań w systemach finansowych.
- Bezpieczeństwo sieci w instytucjach finansowych: segmentacja, monitoring, systemy IDS/IPS.
- Standardy i regulacje dotyczące bezpieczeństwa w sektorze finansowym (np. PSD2, RODO).
- Praktyczne aspekty zarządzania incydentami w sektorze finansowym.
7: Sztuczna inteligencja w sektorze finansowym (90 minut)
- Wprowadzenie do zastosowania AI w analizie transakcji finansowych.
- Mechanizmy wykrywania oszustw z użyciem algorytmów uczenia maszynowego.
- Wpływ AI na automatyzację procesów zabezpieczeń finansowych.
- Przykłady narzędzi wykorzystujących AI w ochronie systemów finansowych.
8: Przyszłość bezpieczeństwa sektora finansowego (90 minut)
- Rozwój technologii blockchain i jego wpływ na bezpieczeństwo transakcji finansowych.
- Trendy i wyzwania w zabezpieczeniach systemów finansowych.
- Przegląd innowacyjnych technologii wspierających ochronę sektora finansowego.
- Podsumowanie i dyskusja na temat integracji technologii i procesów zabezpieczeń.

Metody dydaktyczne

Wykłady teoretyczne z elementami prezentacji multimedialnych, prowadzone online
• Laboratoria praktyczne: analiza przypadków, projektowanie zabezpieczeń.
• Dyskusje i symulacje sytuacji kryzysowych.

Literatura

Podstawowa:
Krzysztof Jajuga, Zarządzanie ryzykiem, Wydawnictwo Naukowe PWN, Warszawa 2016.
ksiegarnia.pwn.pl
• William Stallings, Cryptography and Network Security: Principles and Practice, 8. wydanie, Pearson, 2020.
pearson.com
• Dokumentacja i raporty dotyczące przestępczości finansowej, np. raporty Narodowego Banku Polskiego (NBP) oraz Komisji Nadzoru Finansowego (KNF).
Uzupełniająca • J. Czapska, Z. Rau, Policja w społeczeństwie obywatelskim, Kraków: Zakamycze, 1997.
• A. Tyburska, Zarządzanie kryzysowe. Organizacja, planowanie, reagowanie, Warszawa: Wydawnictwo Naukowe PWN, 2012.
• C. Hadnagy, Socjotechnika. Sztuka zdobywania władzy nad umysłami, Gliwice: Wydawnictwo Helion, 2012.
• Artykuły i raporty z zakresu cyberbezpieczeństwa publikowane przez CERT Polska, ENISA (European Union Agency for Cybersecurity) itp.

Bilans nakładu pracy przeciętnego studenta

	Godzin	ECTS
Łączny nakład pracy	57	2,00
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	32	1,00
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych/ćwiczeń, przygotowanie do kolokwiów/egzaminu, wykonanie projektu)	25	1,00