POLSKO-JAPOŃSKA AKADEMIA TECHNIK KOMPUTEROWYCH

SYLABUS PRZEDMIOTU

Nazwa przedmiotu:	**Analiza Incydentów Cyberbezpieczeństwa**
Kod przedmiotu:	AIC
Kierunek / Profil:	Informatyka / praktyczny
Tryb studiów:	stacjonarny
Rok / Semestr:	3 / 5
Charakter:	obowiązkowy
Odpowiedzialny:	mgr inż. Paweł Lelental
Wersja z dnia:	19.02.2026

1. Godziny zajęć i punkty ECTS

Wykłady	Ćwiczenia	Laboratori	Z prowa-dzącym	Praca własna	Łącznie	ECTS
30 h	—	30 h	60 h	40 h	100 h	**4**

2. Forma zajęć

Forma zajęć	Sposób zaliczenia
Laboratorium	Zaliczenie z oceną
Wykład	Nieoceniany

3. Cel dydaktyczny

Analiza incydentów cyberbezpieczeństwa to proces badania i oceny zdarzeń, które mogą stanowić naruszenie cyberbezpieczeństwa. Celem jest zrozumienie, jak doszło do incydentu, jakie są jego skutki, jak można go zażegnać i jak zapobiegać podobnym incydentom w przyszłości. W całym tym procesie kluczowe jest posiadanie odpowiednich umiejętności analizy systemów i sieci, a także do podejmowania szybkich i skutecznych działań w celu zminimalizowania wpływu incydentów na cyberbezpieczeństwo.

4. Treści programowe

1. Wykład:
2. Anatomia zagrożenia – Ransomware (wg. ENISA)
3. Anatomia zagrożenia – Malware (wg. ENISA)
4. Anatomia zagrożenia – Cryptojacking (wg. ENISA)
5. Anatomia zagrożenia - E-mail related threats (wg. ENISA)
6. Anatomia zagrożenia - Threats against data (wg. ENISA)
7. Anatomia zagrożenia - Threats against availability and integrity (wg. ENISA)
8. Anatomia zagrożenia - Disinformation – misinformation (wg. ENISA)
9. Anatomia zagrożenia - Non-malicious threats (wg. ENISA)
10. Laboratoria:
11. Zapoznanie się z organizacją oraz utworzenie Zespołów SOC
12. Atak 1: Atak typu Ransomware, Poziom 1– Reakcja i prewencja
13. Atak 2: Atak typu Malware. Poziom 1 – Reakcja i prewencja
14. Atak 3: Atak typu Cryptojacking, Poziom 1 – Reakcja i prewencja
15. Atak 4: Atak typu E-mail related threats, Poziom 1 – Reakcja i prewencja
16. Atak 5: Atak typu Threats against data, Poziom 1 – Reakcja i prewencja
17. Atak 6: Atak typu Threats against availability and integrity, Poziom 1 – Reakcja i prewencja
18. Atak 7: Atak typu Disinformation – misinformation, Poziom 1 – Reakcja i prewencja
19. Atak 8: Atak typu Non-malicious threats, Poziom 1 – Reakcja i prewencja
20. Atak 9: Atak typu Zaawansowany wektor ataku 1, Poziom 2 – Reakcja i prewencja
21. Atak 10: Atak typu Zaawansowany wektor ataku 2, Poziom 2 – Reakcja i prewencja
22. Atak 11: Atak typu Zaawansowany wektor ataku 3, Poziom 2 – Reakcja i prewencja
23. Atak 12 : Atak typu Zaawansowany wektor ataku 4, Poziom 2 – Reakcja i prewencja

5. Efekty kształcenia

Wiedza

- Student zna i rozumie anatomię kluczowych zagrożeń Cyber
- Student zna i rozumie podstawowe środki ochrony i reakcji na kluczowe zagrożenia Cyber

Umiejętności

- Student potrafi przygotować zestaw środków ochrony informacji odpowiednich dla różnych typów zagrożeń
- Student potrafi wskazać mocne i słabe strony systemów ochrony informacji

Kompetencje społeczne

- Student jest gotów do pracy zespołowej w dziale SOC

6. Kryteria oceny

- burza mózgów
- warsztaty
- Kryteria oceny
- Laboratorium/Projekt
- rezultaty gry strategicznej, kolokwium końcowe
- Kryteria oceny:niedostateczny: < 50% możliwych do zdobycia punktów dostateczny : 50%-60% możliwych do zdobycia punktów dostateczny+ : 61%- 70% możliwych do zdobycia punktówdobry : 71%-80% możliwych do zdobycia punktówdobry +: 81%-90% możliwych do zdobycia punktów bardzo dobry : >90% możliwych do zdobycia punktów
- Zaliczenie – kolokwium końcowe z Laboratoriów

7. Metody dydaktyczne

Wykład, laboratoria, praca własna studenta.

8. Literatura

Podstawowa:

- William Stallings, Lawrie Brown - Bezpieczeństwo systemów informatycznych. Zasady i praktyka. (ang. Computer Security: Principles and Practice), Wydanie IV. Tom 1 i 2, Helion 2019

Uzupełniająca:

- Brak danych.