**Syllabus modułu 6: Kompleksowe zabezpieczenie sieci**

**Obciążenie pracą i ECTS**

Zajęcia wideo: 8 godzin

Praca autonomiczna: 67 godz.

ECTS: 3

**Efekty kształcenia (wiedza, umiejętności i kompetencje)**

Moduł Comprehensive Network Security dostarcza teoretycznej i praktycznej wiedzy na temat technologii cyberbezpieczeństwa, a mianowicie o Firewallach, systemach wykrywania włamań (IDS), systemach zapobiegania włamaniom (IPS) oraz malware i antivirusach. Rozwijane umiejętności to:

1. Zrozumienie roli Firewalla w technologiach cyberbezpieczeństwa, jego typów i cech, topologii i architektur oraz wspólnych rozwiązań;

2. Zrozumienie roli systemów detekcji włamań w zakresie technologii cyberbezpieczeństwa, ich rodzajów i cech charakterystycznych, architektur wdrożeniowych i powszechnie stosowanych rozwiązań;

3. Zrozumienie roli systemów zapobiegania włamaniom w zakresie technologii cyberbezpieczeństwa, ich rodzajów i cech charakterystycznych, architektur wdrożeniowych i powszechnie stosowanych rozwiązań;

4. Zrozumienie roli Anti-Malware w technologiach Cyberbezpieczeństwa, jak rozprzestrzenia się złośliwe oprogramowanie, różne rodzaje złośliwego oprogramowania, jak wykryć, usunąć i zapobiec przed infekcjami złośliwym oprogramowaniem, jak działa specyficzny przypadek oprogramowania anty-malware - antywirus - i jego wspólne rozwiązania.

**Spis treści**

1. Zapory ogniowe

1.1 Wprowadzenie do zapór ogniowych

1.2 Potrzeba zapory ogniowej

1.3 Rodzaje i charakterystyka zapór ogniowych

1.4 Topologie i architektury firewalli

1.5 Przykłady firewalli

2. Systemy wykrywania włamań

2.1 Wprowadzenie do systemów wykrywania włamań

2.2 Rodzaje i charakterystyka systemów wykrywania włamań

2.3 Architektury implementacji systemów wykrywania włamań

2.4 Systemy wykrywania włamań wspólne rozwiązania i przykłady

3. Systemy zapobiegania włamaniom

3.1 Wprowadzenie do systemów zapobiegania włamaniom

3.2 Rodzaje i charakterystyka systemów zapobiegania włamaniom

3.3 Architektury wdrażania systemów zapobiegania włamaniom

4. Malware i Antivirus

4.1 Wprowadzenie do złośliwego oprogramowania

4.2 Jak dochodzi do infekcji złośliwym oprogramowaniem

4.3 Najczęstsze typy złośliwego oprogramowania

4.4 Jak wykrywać, usuwać i zapobiegać infekcjom złośliwego oprogramowania

4.5 Szczególny przypadek programu antywirusowego

4.6 Jak działa program antywirusowy

4.7 Wybór dobrego oprogramowania antywirusowego

**Metodyka nauczania**

Książka kursowa i lekcja wideo z wyjaśnieniem treści kursu, zestaw ćwiczeń do ćwiczenia i zastosowania wiedzy z książki kursowej i lekcji wideo oraz zestaw gier dla uzupełniającego podejścia pedagogicznego do nauki. W zestawie znajduje się również test końcowy do osobistej oceny.

**Bibliografia główna**

[1] Chris Sandres, "Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems", 3rd Edition, ISBN: 978-1-59327-802-1, NO STARCH PRESS, 2017.

[2] Andrew S. Tanenbaum, Nick Feamster, David J. Wetherall, "Sieci komputerowe", 6th Edition, ISBN-13: 9780137523214, Pearson, 2021

[4] Behrouz A. Forouzan, "TCP/IP Protocol Suite", 4th Edition, ISBN: 978-0070166783, McGraw-Hill Higher Education, 2009.