**Sylabus modulu 6: Komplexní zabezpečení sítě**

**Pracovní zátěž a ECTS**

Videotřídy: 8 hodin

Autonomní práce: 67 hodin

ECTS: 3

**Výsledky učení (znalosti, dovednosti a kompetence)**

Modul Komplexní síťová bezpečnost poskytuje teoretické a praktické znalosti o technologiích kybernetické bezpečnosti, konkrétně o firewallech, systémech detekce narušení (IDS), systémech prevence narušení (IPS) a o malwaru a antivirech. Dovednosti, které je třeba rozvíjet, jsou následující:

1. Porozumět úloze firewallů v technologiích kybernetické bezpečnosti, jejich typům a vlastnostem, topologiím a architekturám a běžným řešením;

2. Porozumět úloze systémů detekce narušení v technologiích kybernetické bezpečnosti, jejich typům a charakteristikám, architekturám implementace a běžným řešením;

3. Porozumět roli systémů prevence narušení v technologiích kybernetické bezpečnosti, jejich typům a charakteristikám, architekturám implementace a běžným řešením;

4. Pochopit roli antimalwaru v technologiích kybernetické bezpečnosti, jak se malware šíří, různé typy malwaru, jak detekovat, odstranit a zabránit infekci malwarem, jak funguje konkrétní případ antimalwarového softwaru - antiviru - a jeho běžná řešení.

**Obsah**

1. Firewally

1.1 Úvod do firewallů

1.2 Potřeba brány firewall

1.3 Typy a vlastnosti brány firewall

1.4 Topologie a architektury brány firewall

1.5 Příklady firewallů

2. Systémy detekce narušení

2.1 Úvod do systémů detekce narušení

2.2 Typy a charakteristika systémů detekce narušení

2.3 Implementační architektury systémů detekce narušení

2.4 Systémy detekce narušení Společná řešení a příklady

3. Systémy prevence narušení

3.1 Úvod do systémů prevence narušení

3.2 Typy a charakteristiky systémů prevence narušení

3.3 Architektury implementace systémů prevence narušení

4. Malware a antivirus

4.1 Úvod do malwaru

4.2 Jak se dostáváme k malwarovým infekcím

4.3 Nejčastější typy malwaru

4.4 Jak zjistit, odstranit a zabránit nákaze malwarem

4.5 Specifický případ antiviru

4.6 Jak funguje antivirus

4.7 Výběr dobrého antivirového softwaru

**Metodiky výuky**

učebnice a video lekce s výkladem obsahu kurzu, soubor cvičení k procvičení a aplikaci poznatků z učebnice a video lekce a soubor her pro doplňkový pedagogický přístup k výuce. K dispozici je také závěrečný test pro osobní hodnocení.

**Hlavní bibliografie**

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

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

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