**СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ**

|  |  |
| --- | --- |
| **Тип дисципліни** | Вибіркова |
| **Рівень вищої освіти** | Перший (бакалаврський) |
| **Мова викладання** | Українська |
| **Кількість кредитів ЄКТС** | 8,0 |
| **Форми здобуття освіти** | Очна денна |

**Результати навчання.** Студент, який успішно завершив вивчення дисципліни, повинен: знати вразливості комп’ютерних систем та мереж, загрози та принципи здійснення атак, спрямованих на комп’ютерні системи та мережі; методи та засоби виявлення вторгнень, загроз та атак, а також методи керування та емуляції мережевих пристроїв; вміло застосовувати засоби виявлення вторгнень для забезпечення інформаційної безпеки комп’ютерних систем; бути здатним організовувати захист комп’ютерних мереж та впроваджувати сучасні засоби захисту виявлення вторгнень з метою забезпечення інформаційної безпеки комп’ютерних мереж; обґрунтовувати вибір способів збору, зберігання, передачі та захисту інформації в програмних і технічних засобах комп’ютерних систем та мереж; адмініструвати, використовувати, адаптувати та експлуатувати наявні технології комп’ютерної інженерії із забезпеченням захисту інформації в комп’ютерних системах та мережах з метою реалізації встановленої політики інформаційної безпеки.

**Зміст навчальної дисципліни.** Системи виявлення вторгнень (IDS, Intrusion Detection Systems). Класифікація IDS. Архітектура IDS. Базові технології виявлення вторгнень. Класифікація вразливостей. Реєстри вразливостей. Класифікація атак. Виявлення зловживань. Виявлення аномалій. Атаки на комп’ютерну систему. Хостові IDS (HIDS, Host-Based Intrusion Detection Systems). Методи виявлення атак на рівні вузла. Мережні атаки. Мережні IDS (NIDS, Network-Based Intrusion Detection Systems). Методи виявлення атак на рівні мережі. Системи запобігання вторгнень (IPS, Intrusion Prevention System). Сучасні засоби HIDS та NIDS та їх практичне застосування. Системи Security Information and Event Management (SIEM). Аудит інформаційної безпеки. Система Security Operation Center. Поняття демілітаризованої зони (DMZ, demilitarized zone). DLP-системи (Data Loss Prevention). Застосування приманок (Honeypots) та їх мереж (Honeynets). Переваги та недоліки використання приманок. Роль приманок в забезпеченні безпеки. Модель приманки. Класифікація та типи приманок. Мережі приманок. Архітектура мережі приманок. Статистичний та інтелектуальний аналіз даних приманок та їх мереж.

**Запланована навчальна діяльність:** кількість аудиторних годин – не менше 1/3 від загальної кількості годин, які заплановані на вивчення дисципліни.

**Методи навчання:** словесні, наочні, проблемно-пошукові (лекції); пояснювально-ілюстративні, практичні, частково-пошукові (практичні та лабораторні заняття), практичні, дослідницькі, частково-пошукові (самостійна робота: індивідуальні завдання).

**Форми оцінювання результатів навчання**: усне опитування, захист лабораторних та практичних робіт, тестовий контроль.

**Форма семестрового контролю:** залік.

**Навчальні ресурси:**

1. Almalawi, A., Tari, Z., Fahad, A., Yi, X. SCADA Security: Machine Learning Concepts for Intrusion Detection and Prevention. – John Wiley & Sons, 2021. – 224 p.
2. Sengupta, N., Sil, J. Intrusion Detection: A Data Mining Approach. – Springer Nature, 2020. – 151 p.
3. Kim, K., Aminanto, M. E., Tanuwidjaja, H. C. Network Intrusion Detection Using Deep Learning: A Feature Learning Approach, 2018. – Springer. – 92 p.
4. Модульне середовище для навчання MOODLE. Доступ до ресурсу: <https://msn.khmnu.edu.ua>
5. Електронна бібліотека університету. Доступ до ресурсу: <http://lib.khmnu.edu.ua/asp/php_f/p1age_lib.php>

**Викладачі**: старший викладач Регіда П.Г.