СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«ТЕХНОЛОГІЇ ВИЯВЛЕННЯ УРАЗЛИВОСТЕЙ МЕРЕЖЕВИХ РЕСУРСІВ»

<table>
<tr><td colspan="3">Лектор курсу</td><td colspan="2">Гахов Сергій Олександрович, кандидат військових наук, доцент.</td><td colspan="2">Контактна інформація лектора (e-mail), сторінка курсу в Moodle</td><td colspan="2">e-mail: ikbdut@gmail.com;
сторінка курсу в Moodle –
http://dn.dut.edu.ua/course/view.php?id=449</td></tr>
<tr><td colspan="3">Галузь знань</td><td colspan="2">12 Інформаційні технології</td><td colspan="2">Рівень вищої освіти</td><td colspan="2">Доктор філософії</td></tr>
<tr><td colspan="3">Спеціальність</td><td colspan="2">Кібербезпека</td><td colspan="2">Семестр</td><td colspan="2">2</td></tr>
<tr><td colspan="3">Освітня програма</td><td colspan="2">Доктор філософії кібербезпеки</td><td colspan="2">Тип дисципліни</td><td colspan="2">Вибіркова компонента освітньо-наукової програми</td></tr>
<tr><td rowspan="2">Обсяг:</td><td>Кредитів ECTS</td><td>Годин</td><td colspan="6">За видами занять:</td></tr>
<tr><td>3</td><td>90</td><td>Лекцій
18</td><td>Семінарських занять
-</td><td>Практичних занять
18</td><td>Лабораторних занять
-</td><td colspan="2">Самостійна підготовка
54</td></tr>
<tr><td colspan="9">АНОТАЦІЯ КУРСУ</td></tr>
<tr><td colspan="9">Взаємозв’язок у структурно-логічній схемі</td></tr>
<tr><td colspan="3">Освітні компоненти, які передують вивченню</td><td colspan="6">Методологія наукових досліджень у кібербезпеці</td></tr>
<tr><td colspan="3">Освітні компоненти для яких є базовою</td><td colspan="6"></td></tr>
<tr><td>Мета курсу:</td><td colspan="8">Формування знань та вмінь щодо застосування методів та засобів виявлення вразливостей мережевих ресурсів як складової частини забезпечення кібербезпеки інформаційних систем організацій, а також їх критичного аналізу, виявлення недоліків та протиріч для постановки наукових завдань.</td></tr>
<tr><td colspan="9">Компетентності відповідно до освітньої програми</td></tr>
<tr><td colspan="5">Soft- skills / Загальні компетентності (ЗК)</td><td colspan="4">Hard-skills / Спеціальні компетентності (СК)</td></tr>
<tr><td colspan="5">ЗК-3. Знання інформаційних технологій</td><td colspan="4">ФК-4. Професійна компетентність
ФК-5. Загальнонаукова компетентність
ФК-6. Політехнічна компетентність
ФК-7. Інженерна компетентність</td></tr>
<tr><td colspan="9">Програмні результати навчання (ПРН)</td></tr>
<tr><td colspan="9">ПРН-18. Уміти аналізувати існуючі технології, методи і засоби застосування шкідливого програмного забезпечення, нівелювання уразливостей мережевих та Web-ресурсів.
ПРН-19. Уміти проектувати перспективні технології виявлення шкідливого програмного забезпечення, а також уразливостей мережевих та Web-ресурсів й застосовувати їх на практиці.
ПРН-20. Уміти визначати і вирішувати етичні питання при проведенні досліджень та пошуку відмінностей у шкідливому програмного забезпечення, уразливостях мережевих та Web-ресурсів.
ПРН-26. Уміти використовувати сучасні техніки для проведення досліджень за напрямом захисту інформації, організації й забезпечення безпеки мережевої інфраструктури об’єктів інформаційної діяльності, а також наукових досліджень вищих рівнів.
ПРН-27. Бути здатним оволодіти спеціалізованими програмними пакетами, протоколами передачі даних, спеціальною мікропроцесорною технікою, сучасними інформаційними та безпековими технологіями.</td></tr>
<tr><td colspan="9">ОРГАНІЗАЦІЯ НАВЧАННЯ</td></tr>
</table>

Тема, опис теми	Вид заняття	Оцінювання за тему	Форми і методи навчання/питання до самостійної роботи
Тема 1. Основи забезпечення кібербезпеки сучасного підприємства. Роль і місце технологій виявлення вразливостей мережевих ресурсів у системі забезпечення кібербезпеки. ***Знати***: поняття «корпоративна інформаційна система» як об'єкт захисту; превентивні, детективні та корективні заходи забезпечення кібербезпеки сучасного підприємства; поняття «подія безпеки», поняття «вразливість»; класифікація вразливостей; джерела даних щодо вразливостей; прийняті позначення вразливостей. ***Формування компетенцій:*** ЗК-3, ФК-4, ФК-5, ФК-6, ФК-7 ***Програмні результати навчання:*** ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27 ***Рекомендовані джерела:*** 1-6	Лекція 1 2 год	6	Лекція-візуалізація
Тема 1. Впровадження процесу управління вразливостями. ***Знати:*** зміст процесу управління вразливостями; мета управління вразливістю; ролі та обов'язки посадових осіб. ***Вміти:*** застосовувати методику управління вразливостями: здійснювати заходи підготовчого етапу; здійснювати початкове сканування вразливостей; визначати коригуючі дії або приймати ризик; здійснювати коригувальні дії; здійснювати перевірку (рескановання). ***Формування компетенцій:*** ЗК-3, ФК-4, ФК-5, ФК-6, ФК-7 ***Програмні результати навчання:*** ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27 ***Рекомендовані джерела:*** 1-6	Практичне заняття 1 2 год		Практичне застосування методики управління вразливостями з використанням сканера вразливостей Nessus Professional.
Тема 1. Основи забезпечення кібербезпеки сучасного підприємства. Роль і місце технологій виявлення вразливостей мережевих ресурсів у системі забезпечення кібербезпеки. Впровадження процесу управління вразливостями. ***Знати:*** поняття «корпоративна інформаційна система» як об'єкт захисту; превентивні, детективні та корективні заходи забезпечення кібербезпеки сучасного підприємства; поняття «подія безпеки», поняття «вразливість»; класифікація вразливостей; джерела даних щодо вразливостей; прийняті позначення вразливостей; зміст процесу управління вразливостями; мета управління вразливістю; ролі та обов'язки посадових осіб.	Самостійна робота 1 6 год		Самостійна підготовка. Удосконалення отриманих знань та умінь, отриманих (надбаних) за попередніми лекцією та практичним заняттям.

Вміти: застосовувати методику управління вразливостями: здійснювати заходи підготовчого етапу; здійснювати початкове сканування вразливостей; визначати коригуючі дії або приймати ризик; здійснювати коригувальні дії; здійснювати перевірку (рескановання). ***Формування компетенцій:*** ЗК-3, ФК-4, ФК-5, ФК-6, ФК-7 ***Програмні результати навчання:*** ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27 ***Рекомендовані джерела:*** 1-6			
Тема 2. Основи інформаційно-аналітичної діяльності фахівців з кібербезпеки. ***Знати***: основи інформаційно-аналітичної діяльності фахівців з кібербезпеки; зміст інформаційно-аналітичної діяльності фахівців з кібербезпеки; методологію аналітичних досліджень кіберінцидентів; основні методи аналітичної діяльності фахівців з кібербезпеки; інформаційні джерела для здійснення аналітичної діяльності фахівців з кібербезпеки. ***Формування компетенцій:*** ЗК-3, ФК-4, ФК-5, ФК-6, ФК-7 ***Програмні результати навчання:*** ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27 ***Рекомендовані джерела:*** 1-6	Лекція 2 2 год	6	Лекція-візуалізація
Тема 2. Стратегії сканування, які рекомендують Tenable. ***Знати:*** методологію сканування, параметри активного розкладу сканування, конфігурацію політики сканування, налаштування політики сканування. ***Вміти:*** застосовувати конфігурації політики сканування; налаштувувати політики сканування. ***Формування компетенцій:*** ЗК-3, ФК-4, ФК-5, ФК-6, ФК-7 ***Програмні результати навчання:*** ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27 ***Рекомендовані джерела:*** 5, 6	Практичне заняття 2 2 год		Практичне застосування методики управління вразливостями з використанням сканера вразливостей Nessus Professional.
Тема 2. Основи інформаційно-аналітичної діяльності фахівців з кібербезпеки. ***Знати***: основи інформаційно-аналітичної діяльності фахівців з кібербезпеки; зміст інформаційно-аналітичної діяльності фахівців з кібербезпеки; методологію аналітичних досліджень кіберінцидентів; основні методи аналітичної діяльності фахівців з кібербезпеки; інформаційні джерела для здійснення аналітичної діяльності фахівців	Самостійна робота 2 6 год		Самостійна підготовка. Удосконалення отриманих знань та умінь, отриманих (надбаних) за попередніми лекцією та практичним заняттям.

з кібербезпеки; методологію сканування, параметри активного розкладу сканування, конфігурацію політики сканування, налаштування політики сканування. ***Вміти:*** застосовувати конфігурації політики сканування; налаштувати політики сканування. ***Формування компетенцій:*** ЗК-3, ФК-4, ФК-5, ФК-6, ФК-7 ***Програмні результати навчання:*** ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27 ***Рекомендовані джерела:*** 1-6			
Тема 3. Основи технології тестування на проникнення (Penetration Testing). ***Знати***: цілі тестування на проникнення; види тестування на проникнення та їх зміст; принципові відмінності тестування на проникнення та сканування вразливостей; зміст тестування рівня додатків та мережевого рівня; зміст тестування на проникнення сегментів мережі та на предмет соціальної інженерії; порядок подання та зміст звітності за результатами тестування на проникнення; технологію проведення тестування на проникнення; приклади застосування технології тестування на проникнення для різних варіантів. ***Формування компетенцій:*** ЗК-3, ФК-4, ФК-5, ФК-6, ФК-7 ***Програмні результати навчання:*** ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27 ***Рекомендовані джерела:*** 1-6	Лекція 3 2 год	6	Лекція-візуалізація
Тема 3. Основи застосування сканера вразливостей Nessus Professional. Основи сканування. ***Знати:*** шаблони сканування та політик. ***Вміти:*** застосовувати шаблони сканування та політик. ***Формування компетенцій:*** ЗК-3, ФК-4, ФК-5, ФК-6, ФК-7 ***Програмні результати навчання:*** ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27 ***Рекомендовані джерела:*** 5, 6	Практичне заняття 3 2 год		Практичне застосування методики управління вразливостями з використанням сканера вразливостей Nessus Professional.
Тема 3. Основи технології тестування на проникнення (Penetration Testing). ***Знати***: цілі тестування на проникнення; види тестування на проникнення та їх зміст; принципові відмінності тестування на проникнення та сканування вразливостей; зміст тестування рівня	Самостійна робота 3 6 год		Самостійна підготовка. Удосконалення отриманих знань та умінь, отриманих (надбаних) за попередніми лекцією та практичним заняттям.

додатків та мережевого рівня; зміст тестування на проникнення сегментів мережі та на предмет соціальної інженерії; порядок подання та зміст звітності за результатами тестування на проникнення; технологію проведення тестування на проникнення; приклади застосування технології тестування на проникнення для різних варіантів; шаблони сканування та політик. ***Вміти:*** застосовувати шаблони сканування та політик. ***Формування компетенцій:*** ЗК-3, ФК-4, ФК-5, ФК-6, ФК-7 ***Програмні результати навчання:*** ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27 ***Рекомендовані джерела:*** 1-6			
Тема 4. Технології виявлення вразливостей мережевих ресурсів. Загальні положення. ***Знати:*** технологію сканування мережі; порядок визначення топології мережі; місця розміщення сканерів уразливостей; порядок визначення цілей сканування; стратегії сканування; користувальницькі вимоги; методологію сканування: параметри розкладу активного сканування; конфігурація політики сканування; налаштування політики сканування. ***Формування компетенцій:*** ЗК-3, ФК-4, ФК-5, ФК-6, ФК-7 ***Програмні результати навчання:*** ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27 ***Рекомендовані джерела:*** 1-6	Лекція 4 2 год	6	Лекція-візуалізація
Тема 4. Основи застосування сканера вразливостей Nessus Professional. Налаштування сканування та політики. ***Знати:*** порядок налаштування сканування та політики. ***Вміти:*** налаштовувати сканування виявлення. ***Формування компетенцій:*** ЗК-3, ФК-4, ФК-5, ФК-6, ФК-7 ***Програмні результати навчання:*** ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27 ***Рекомендовані джерела:*** 5, 6	Практичне заняття 4 2 год		Практичне застосування методики управління вразливостями з використанням сканера вразливостей Nessus Professional.
Тема 4. Технології сканування мережевих ресурсів. Загальні положення. ***Знати:*** технологію сканування мережі; порядок визначення топології мережі; місця розміщення сканерів уразливостей; порядок визначення цілей сканування; стратегії сканування; користувальницькі вимоги; методологію сканування: параметри розкладу активного сканування;	Самостійна робота 4 6 год		Самостійна підготовка. Удосконалення отриманих знань та умінь, отриманих (надбаних) за попередніми лекцією та практичним заняттям.

конфігурація політики сканування; налаштування політики сканування; порядок налаштування сканування та політики. ***Вміти:*** налаштовувати сканування виявлення. ***Формування компетенцій:*** ЗК-3, ФК-4, ФК-5, ФК-6, ФК-7 ***Програмні результати навчання:*** ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27 ***Рекомендовані джерела:*** 1-6			
Тема 5. Основи застосування сканера вразливостей Nessus Professional. Установки сканування та політик. ***Знати:*** види та порядок налаштування сканування та політик сканера вразливостей Nessus Professional: Basic Scan Settings, Scan Targets, Discovery Scan Settings, Assessment Scan Settings, Report Scan Settings, Advanced Scan Settings, Credentials. ***Формування компетенцій:*** ЗК-3, ФК-4, ФК-5, ФК-6, ФК-7 ***Програмні результати навчання:*** ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27 ***Рекомендовані джерела:*** 5, 6	Лекція 5 2 год	6	Лекція-візуалізація
Тема 5. Основи застосування сканера вразливостей Nessus Professional. Налаштування сканування оцінки. ***Знати:*** типи сканувань. ***Вміти:*** налаштовувати та створювати звіт сканування; налаштовувати просунуте сканування. ***Формування компетенцій:*** ЗК-3, ФК-4, ФК-5, ФК-6, ФК-7 ***Програмні результати навчання:*** ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27 ***Рекомендовані джерела:*** 5, 6	Практичне заняття 5 2 год		Практичне застосування методики управління вразливостями з використанням сканера вразливостей Nessus Professional.
Тема 5. Основи застосування сканера вразливостей Nessus Professional. Установки сканування та політик. ***Знати:*** види та порядок налаштування сканування та політик сканера вразливостей Nessus Professional: Basic Scan Settings, Scan Targets, Discovery Scan Settings, Assessment Scan Settings, Report Scan Settings, Advanced Scan Settings, Credentials. ***Вміти:*** налаштовувати та створювати звіт сканування; налаштовувати просунуте сканування. ***Формування компетенцій:*** ЗК-3, ФК-4, ФК-5, ФК-6, ФК-7 ***Програмні результати навчання:*** ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27	Самостійна робота 5 6 год		Самостійна підготовка. Удосконалення отриманих знань та умінь, отриманих (надбаних) за попередніми лекцією та практичним заняттям.

Рекомендовані джерела: 5, 6			
Тема 6. Основи застосування IBM QRadar Vulnerability Manager. Призначення та можливості програмного комплексу. ***Знати:*** призначення та можливості програмного комплексу IBM QRadar Vulnerability Manager; функціональні компоненти IBM QRadar Vulnerability Manager; види перевірок на вразливість, які здійснюються за допомогою IBM QRadar Vulnerability Manager; порядок інсталяції та розгортання IBM QRadar Vulnerability Manager. ***Формування компетенцій:*** ЗК-3, ФК-4, ФК-5, ФК-6, ФК-7 ***Програмні результати навчання:*** ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27 ***Рекомендовані джерела:*** 7-10	Лекція 6 2 год	6	Лекція-візуалізація
Тема 6. Основи застосування сканера вразливостей Nessus Professional. Аналіз результатів сканування. ***Знати:*** зміст панелі інструментів та можливості Nessus Professional. ***Вміти:*** застосовувати сканер та проводити аналіз вразливостей. ***Формування компетенцій:*** ЗК-3, ФК-4, ФК-5, ФК-6, ФК-7 ***Програмні результати навчання:*** ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27 ***Рекомендовані джерела:*** 5, 6	Практичне заняття 6 2 год		Практичне застосування методики управління вразливостями з використанням сканера вразливостей Nessus Professional.
Тема 6. Основи застосування IBM QRadar Vulnerability Manager. Призначення та можливості програмного комплексу. ***Знати:*** призначення та можливості програмного комплексу IBM QRadar Vulnerability Manager; функціональні компоненти IBM QRadar Vulnerability Manager; види перевірок на вразливість, які здійснюються за допомогою IBM QRadar Vulnerability Manager; порядок інсталяції та розгортання IBM QRadar Vulnerability Manager. ***Формування компетенцій:*** ЗК-3, ФК-4, ФК-5, ФК-6, ФК-7 ***Програмні результати навчання:*** ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27 ***Рекомендовані джерела:*** 7-10	Самостійна робота 6 6 год		Самостійна підготовка. Удосконалення отриманих знань та умінь, отриманих (надбаних) за попередніми лекцією та практичним заняттям.
Тема 7. Основи застосування IBM QRadar Vulnerability Manager. Налаштування сканування вразливостей та кращі практики. ***Знати:*** типи політик сканування; тривалість сканування та порядок сканування портів; налаштування конфігурації пошуку активів; порядок сканування веб-додатків; місця розміщення сканера в мережі;	Лекція 7 2 год	6	Лекція-візуалізація

зміст та порядок динамічного сканування; вимоги щодо пропускної здатності мережі для одночасного сканування активів; карти мережевого інтерфейсу на сканерах; порядок управління вразливістю; зміст повідомлення про сканування вразливості; порядок запуску сканування нових активів. ***Формування компетенцій:*** ЗК-3, ФК-4, ФК-5, ФК-6, ФК-7 ***Програмні результати навчання:*** ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27 ***Рекомендовані джерела:*** 7-10			
Тема 7. Основи застосування IBM QRadar Vulnerability Manager. Налаштування сканування вразливостей та кращі практики. ***Знати:*** типи політики сканування в IBM QRadar Vulnerability Manager; типові місця розміщення сканера в мережі. ***Вміти:*** налаштувати конфігурації пошуку активів; налаштувати продуктивність виявлення активів; здійснювати сканування веб-додатків та проводити динамічне сканування. ***Формування компетенцій:*** ЗК-3, ФК-4, ФК-5, ФК-6, ФК-7 ***Програмні результати навчання:*** ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27 ***Рекомендовані джерела:*** 7-10	Практичне заняття 7 2 год		Практичне застосування методики управління вразливостями з використанням програмного комплекса IBM QRadar Vulnerability Manager.
Тема 7. Основи застосування IBM QRadar Vulnerability Manager. Налаштування сканування вразливостей та кращі практики. ***Знати:*** типи політик сканування; тривалість сканування та порядок сканування портів; налаштування конфігурації пошуку активів; порядок сканування веб-додатків; місця розміщення сканера в мережі; зміст та порядок динамічного сканування; вимоги щодо пропускної здатності мережі для одночасного сканування активів; карти мережевого інтерфейсу на сканерах; порядок управління вразливістю; зміст повідомлення про сканування вразливості; порядок запуску сканування нових активів. ***Вміти:*** налаштувати конфігурації пошуку активів; налаштувати продуктивність виявлення активів; здійснювати сканування веб-додатків та проводити динамічне сканування. ***Формування компетенцій:*** ЗК-3, ФК-4, ФК-5, ФК-6, ФК-7 ***Програмні результати навчання:*** ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27 ***Рекомендовані джерела:*** 7-10	Самостійна робота 7 6 год		Самостійна підготовка. Удосконалення отриманих знань та умінь, отриманих (надбаних) за попередніми лекцією та практичним заняттям.

Тема 8. Основи застосування IBM QRadar Vulnerability Manager. Керування виявленими вразливостями. ***Знати:*** зміст та порядок керування виявленими вразливостями. Common Vulnerability Scoring System (CVSS); порядок дослідження показників ризику вразливості; порядок конфігурування індивідуальних оцінок ризику для вразливості; порядок дослідження даних про вразливість; вразливості мережі; вразливості активів; вразливості відкритих служб; порядок дослідження історії вразливості; порядок зменшення кількості помилково-позитивних вразливостей; порядок дослідження активів та вразливих груп з високим ризиком; зміст визначення пріоритетності вразливості шляхом застосування політики щодо ризику. ***Формування компетенцій:*** ЗК-3, ФК-4, ФК-5, ФК-6, ФК-7 ***Програмні результати навчання:*** ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27 ***Рекомендовані джерела:*** 7-10	Лекція 8 2 год	6	Лекція-візуалізація
Тема 8. Основи застосування IBM QRadar Vulnerability Manager. Керування вразливостями. ***Знати:*** зміст та порядок керування виявленими вразливостями. ***Вміти:*** керувати виявленими вразливостями в середовищі IBM QRadar Vulnerability Manager. ***Формування компетенцій:*** ЗК-3, ФК-4, ФК-5, ФК-6, ФК-7 ***Програмні результати навчання:*** ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27 ***Рекомендовані джерела:*** 7-10	Практичне заняття 8 2 год		Практичне застосування методики управління вразливостями з використанням програмного комплекса IBM QRadar Vulnerability Manager.
Тема 8. Основи застосування IBM QRadar Vulnerability Manager. Керування виявленими вразливостями. ***Знати:*** зміст та порядок керування виявленими вразливостями. Common Vulnerability Scoring System (CVSS); порядок дослідження показників ризику вразливості; порядок конфігурування індивідуальних оцінок ризику для вразливості; порядок дослідження даних про вразливість; вразливості мережі; вразливості активів; вразливості відкритих служб; порядок дослідження історії вразливості; порядок зменшення кількості помилково-позитивних вразливостей; порядок дослідження активів та вразливих груп з високим ризиком; зміст визначення пріоритетності вразливості шляхом застосування політики щодо ризику.	Самостійна робота 8 6 год		Самостійна підготовка. Удосконалення отриманих знань та умінь, отриманих (надбаних) за попередніми лекцією та практичним заняттям.

Вміти: керувати виявленими вразливостями в середовищі IBM QRadar Vulnerability Manager. ***Формування компетенцій:*** ЗК-3, ФК-4, ФК-5, ФК-6, ФК-7 ***Програмні результати навчання:*** ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27 ***Рекомендовані джерела:*** 7-10			
Тема 9. Технологія управління вразливостями в корпоративній інформаційній системі з використанням IBM QRadar SIEM та Tenable.sc. ***Знати:*** призначення, функції та склад рішення Tenable.sc; порядок додавання сканування Tenable.sc до IBM QRadar SIEM; зміст планування сканування вразливості в IBM QRadar SIEM; порядок перегляду стану сканування на вразливість в IBM QRadar SIEM; підтримувані сканери вразливості в IBM QRadar SIEM. ***Формування компетенцій:*** ЗК-3, ФК-4, ФК-5, ФК-6, ФК-7 ***Програмні результати навчання:*** ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27 ***Рекомендовані джерела:*** 7-10	Лекція 9 2 год	6	Лекція-візуалізація
Тема 9. Основи застосування IBM QRadar Vulnerability Manager. Порядок інтеграції зі сканерами Tenable.io та Tenable.sc. ***Знати:*** порядок додавання сканування Tenable.sc до IBM QRadar SIEM. ***Вміти:*** планувати та застосовувати сканування вразливостей в IBM QRadar SIEM. ***Формування компетенцій:*** ЗК-3, ФК-4, ФК-5, ФК-6, ФК-7 ***Програмні результати навчання:*** ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27 ***Рекомендовані джерела:*** 7-10	Практичне заняття 9 2 год		Практичне застосування методики управління вразливостями з використанням програмного комплекса IBM QRadar Vulnerability Manager.
Тема 9. Технологія управління вразливостями в корпоративній інформаційній системі з використанням IBM QRadar SIEM та Tenable.sc. ***Знати:*** призначення, функції та склад рішення Tenable.sc; порядок додавання сканування Tenable.sc до IBM QRadar SIEM; зміст планування сканування вразливості в IBM QRadar SIEM; порядок перегляду стану сканування на вразливість в IBM QRadar SIEM; підтримувані сканери вразливості в IBM QRadar SIEM.	Самостійна робота 9 6 год		Самостійна підготовка. Удосконалення отриманих знань та умінь, отриманих (надбаних) за попередніми лекцією та практичним заняттям.

Вміти: планувати та застосовувати сканування вразливостей в IBM QRadar SIEM. ***Формування компетенцій:*** ЗК-3, ФК-4, ФК-5, ФК-6, ФК-7 ***Програмні результати навчання:*** ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27 ***Рекомендовані джерела:*** 7-10			

МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

Комп‘ютерне обладнання, мережа Інтернет ауд. 420, програмні комплекси Nessus Professional, Tenable.sc, IBM QRadar SIEM та IBM QRadar Vulnerability Manager.

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

1. Park Foreman. Vulnerability Management. Second Edition. CRC Press Taylor & Francis Group, 2019. 330 p.
2. Technical Guide to Information Security Testing and Assessment. Recommendations of the National Institute of Standards and Technology. Karen Scarfone. Murugiah Souppaya. Amanda Cody. Angela Orebaugh. NIST Special Publication 800-115. (Sep. 2008). 80 p. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf.
3. Computer Security Incident Handling Guide. Recommendations of the National Institute of Standards and Technology. Paul Cichonski. Tom Millar. Tim Grance. Karen Scarfone. Special Publication 800-61 Revision 2 https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf.
4. Tom Palmaers. Implementing a vulnerability management process. SANS Institute. Accepted: 03/23/2013. 24 p. https://www.sans.org/reading-room/whitepapers/threats/implementing-vulnerability-management-process-34180.
5. Nessus 8.15.x User Guide Last Updated: October 19, 2021. 621 p. https://docs.tenable.com/nessus/8_15/Content/PDF/Nessus_8_15.pdf.
6. Tenable Scan Strategy Tenable Professional Services. Last Revised: May 07, 2021. 22 p. https://docs.tenable.com/other/nessus/Tenable_ProServ_Scan_Strategy_Guide.pdf.
7. IBM QRadar Vulnerability Manager 7.4.0. User Guide. 152 p. https://www.ibm.com/docs/en/SS42VS_7.4/pdf/b_qvm_ug.pdf.
8. IBM QRadar 7.3.3. Architecture and Deployment Guide. 60 p. https://www.ibm.com/docs/en/SS42VS_7.4/pdf/b_siem_deployment.pdf.
9. IBM Security QRadar 7.4.3. Administration Guide. 446 p. https://www.ibm.com/docs/en/SS42VS_7.4/pdf/b_qradar_admin_guide.
10. IBM QRadar 7.4.3. User Guide. 256 p. https://www.ibm.com/docs/en/SS42VS_7.4/pdf/b_qradar_users_guide.pdf.
11.

ПОЛІТИКА КУРСУ («ПРАВИЛА ГРИ»)

- Курс передбачає роботу в колективі.
- Середовище в аудиторії є дружнім, творчим, відкритим до конструктивної критики.
- Освоєння дисципліни передбачає обов’язкове відвідування лекцій і практичних занять, а також самостійну роботу.
- Самостійна робота включає в себе теоретичне вивчення питань, що стосуються тем лекційних занять, які не ввійшли в теоретичний курс, або ж були розглянуті коротко, їх поглиблена проробка за рекомендованою літературою.
- Усі завдання, передбачені програмою, мають бути виконані у встановлений термін.
- Якщо аспірант відсутній з поважної причини, він презентує виконані завдання під час самостійної підготовки та консультації викладача.
- Під час роботи над завданнями не допустимо порушення академічної доброчесності: при використанні Інтернет ресурсів та інших джерел інформації аспірант повинен вказати джерело, використане в ході виконання завдання. У разі виявлення факту плагіату аспірант отримує за завдання 0 балів.
- Аспірант, який спізнився, вважається таким, що пропустив заняття з неповажної причини з виставленням 0 балів за заняття, і при цьому має право бути присутнім на занятті.
- За використання телефонів і комп’ютерних засобів без дозволу викладача, порушення дисципліни аспірант видаляється з заняття, за заняття отримує 0 балів.

* КРИТЕРІЇ ТА МЕТОДИ ОЦІНЮВАННЯ

Умовою допуску до підсумкового контролю є набрання аспірантом 30 балів у сукупності за всіма темами дисципліни

Форми контролю	Види навчальної роботи	Оцінювання
ПОТОЧНИЙ КОНТРОЛЬ	***Робота на заняттях,*** *у т.ч.:*	
	• присутність на заняттях (при пропусках занять з поважних причин допускається відпрацювання пройденого матеріалу)	за кожне відвідування 0,5 бала
	• звіт про виконання практичного завдання	за кожен звіт максимум 1 балів
Додаткова оцінка	Участь у наукових конференціях, підготовка наукових публікацій, отримання міжнародного сертифікату за напрямом.	Звільняється від заліку
ПІДСУМКОВЕ ОЦІНЮВАННЯ ***залік***	Метою заліку є контроль сформованості практичних навичок та професійних компетентностей, необхідних для виконання наукової роботи. Залік проходить у письмовій формі.	46 балів

ПІДСУМКОВА ОЦІНКА ЗА ДИСЦИПЛІНУ

бали	**Критерії оцінювання**	**Рівень компетентності**	**Оцінка** */запис в екзаменаційній відомості*
90-100	Аспірант демонструє повні й міцні знання навчального матеріалу в обсязі, що відповідає робочій програмі дисципліни, правильно й обґрунтовано приймає необхідні рішення в різних нестандартних ситуаціях. Вміє реалізувати теоретичні положення дисципліни в практичних розрахунках, аналізувати та співставляти дані об'єктів діяльності фахівця на основі набутих з даної та суміжних дисциплін знань та умінь. Знає сучасні технології та методи розрахунків з даної дисципліни. За час навчання при проведенні практичних занять, при виконанні індивідуальних / контрольних завдань проявив вміння самостійно вирішувати поставлені завдання, активно включатись в дискусії, може відстоювати власну позицію в питаннях та рішеннях, що розглядаються. Зменшення 100-бальної оцінки може бути пов'язане з недостатнім розкриттям питань, що стосується дисципліни, яка вивчається, але виходить за рамки об'єму матеріалу, передбаченого робочою програмою, або аспірант проявляє невпевненість в тлумаченні теоретичних положень чи складних практичних завдань.	**Високий** Повністю забезпечує вимоги до знань, умінь і навичок, що викладені в робочій програмі дисципліни. Власні пропозиції аспіранта в оцінках і вирішенні практичних задач підвищує його вміння використовувати знання, які він отримав при вивчені інших дисциплін, а також знання, набуті при самостійному поглибленому вивчені питань, що відносяться до дисципліни, яка вивчається.	Відмінно / Зараховано (А)
82-89	Аспірант демонструє гарні знання, добре володіє матеріалом, що відповідає робочій програмі дисципліни, робить на їх основі аналіз можливих ситуацій та вміє застосовувати теоретичні положення при вирішенні практичних задач, але допускає окремі неточності. Вміє самостійно виправляти допущені помилки, кількість яких є незначною. Знає сучасні технології та методи розрахунків з даної дисципліни. За час навчання при проведенні практичних занять, при виконанні індивідуальних / контрольних завдань та поясненні прийнятих рішень, дає вичерпні пояснення.	**Достатній** Забезпечує аспіранту самостійне вирішення основних практичних задач в умовах, коли вихідні дані в них змінюються порівняно з прикладами, що розглянуті при вивчені	Добре / Зараховано (В)

		дисципліни	
75-81	Аспірант в загальному добре володіє матеріалом, знає основні положення матеріалу, що відповідає робочій програмі дисципліни, робить на їх основі аналіз можливих ситуацій та вміє застосовувати при вирішенні типових практичних завдань, але допускає окремі неточності. Вміє пояснити основні положення виконаних завдань та дати правильні відповіді при зміні результату при заданій зміні вихідних параметрів. Помилки у відповідях/ рішеннях/ розрахунках не є системними. Знає характеристики основних положень, що мають визначальне значення при проведенні практичних занять, при виконанні індивідуальних / контрольних завдань та поясненні прийнятих рішень, в межах дисципліни, що вивчається.	**Достатній** Конкретний рівень, за вивченим матеріалом робочої програми дисципліни. Додаткові питання про можливість використання теоретичних положень для практичного використання викликають утруднення.	Добре / Зараховано (C)
64-74	Аспірант засвоїв основний теоретичний матеріал, передбачений робочою програмою дисципліни, та розуміє постанову стандартних практичних завдань, має пропозиції щодо напрямку їх вирішень. Розуміє основні положення, що є визначальними в курсі, може вирішувати подібні завдання тим, що розглядались з викладачем, але допускає значну кількість неточностей і грубих помилок, які може усувати за допомогою викладача. .	**Середній** Забезпечує достатньо надійний рівень відтворення основних положень дисципліни	Задовільно / Зараховано (D)
60-63	Аспірант має певні знання, передбачені в робочій програмі дисципліни, володіє основними положеннями, що вивчаються на рівні, який визначається як мінімально допустимий. З використанням основних теоретичних положень, аспірант з труднощами пояснює правила вирішення практичних/розрахункових завдань дисципліни. Виконання практичних / індивідуальних / контрольних завдань значно формалізовано: є відповідність алгоритму, але відсутнє глибоке розуміння роботи та взаємозв'язків з іншими дисциплінами.	**Середній** Є мінімально допустимим у всіх складових навчальної програми з дисципліни	Задовільно / Зараховано (E)
35-59	Аспірант може відтворити окремі фрагменти з курсу. Незважаючи на те, що програму навчальної дисципліни аспірант виконав, працював він пасивно, його відповіді під час практичних робіт в більшості є невірними, необґрунтованими. Цілісність розуміння матеріалу з дисципліни у аспіранта відсутні.	**Низький** Не забезпечує практичної реалізації задач, що формуються при вивчені дисципліни	Незадовільно з можливістю повторного складання) / Не зараховано (FX) *В залікову книжку не проставляється*
1-34	Аспірант повністю не виконав вимог робочої програми навчальної дисципліни. Його знання на підсумкових етапах навчання є фрагментарними. Аспірант не допущений до здачі заліку.	**Незадовільний** Аспірант не підготовлений до самостійного вирішення задач, які окреслює мета та завдання дисципліни	Незадовільно з обов'язковим повторним вивченням / Не допущений (F) *В залікову книжку не проставляється*