

Затверджено
завідувач кафедри
СТКБ _____ Г. Гайдур
«31» _____ 2026 р.

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«ТЕХНОЛОГІЇ ВИЯВЛЕННЯ УРАЗЛИВОСТЕЙ МЕРЕЖЕВИХ РЕСУРСІВ»

Лектор курсу			Гахов Сергій Олександрович, кандидат військових наук, доцент.		Контактна інформація лектора (e-mail), сторінка курсу		e-mail: s.gakhov@duikt.edu.ua сторінка курсу– https://classroom.google.com/c/NzA3NDg5MDkwMTUx?cjc=jpvv47o	
Галузь знань			F Інформаційні технології		Рівень вищої освіти		Магістр	
Спеціальність			F5 Кібербезпека та захист інформації		Семестр		9	
Освітня програма			Інформаційна та кібернетична безпека		Тип дисципліни		Основна компонента освітньо-професійної програми	
Обсяг:	Кредитів ECTS	Годин	За видами занять:					
			Лекцій	Семінарських занять	Практичних занять	Лабораторних занять	Самостійна підготовка	
	4	120	18	-	36		66	
АНОТАЦІЯ КУРСУ								
Взаємозв'язок у структурно-логічній схемі								
Освітні компоненти, які передують вивченню			Прикладна загальна теорія систем інформаційної та кібербезпеки, Науково-технічний переклад					
Освітні компоненти для яких є базовою			Організація проведення наукових досліджень					
Мета курсу:		Формування знань та вмінь щодо застосування методів та засобів виявлення вразливостей мережеских ресурсів як складової частини забезпечення кібербезпеки інформаційних систем організацій, а також їх критичного аналізу, виявлення недоліків та протиріч для постановки наукових завдань.						
Компетентності відповідно до освітньої програми								
Soft- skills / Загальні компетентності (ЗК)					Hard-skills / Спеціальні компетентності (СК)			
К31. Здатність застосовувати знання у практичних ситуаціях. К32. Здатність проводити дослідження на відповідному рівні. К33. Здатність до абстрактного мислення, аналізу та синтезу. К34. Здатність оцінювати та забезпечувати якість виконуваних робіт. К35. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності)					КФ1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки. КФ2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі			

КЗ1, КЗ2, КЗ3, КЗ4, КЗ5, КФ1, КФ2, КФ3, КФ5, КФ6, КФ7, КФ8, КФ9, КФ10	світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки. КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури. КФ5. Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. КФ6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. КФ7. Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому. КФ8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. КФ9. Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому. КФ10. Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки.
Програмні результати навчання (ПРН)	
ПН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки. ПН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.	

RH6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.

RH8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.

RH11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

RH13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.

RH17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання.

RH21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.

ОРГАНІЗАЦІЯ НАВЧАННЯ

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: КЗ1, КЗ2, КЗ3, КЗ4, КЗ5, КФ1, КФ2, КФ3, КФ5, КФ6, КФ7, КФ8, КФ9, КФ10 Програмні результати навчання: RH4, RH5, RH6, RH8, RH11, RH13, RH17, RH21 Рекомендовані джерела: 1-6	Лекція 1 2 год		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 (ресканування). Формування компетенцій: КЗ1, КЗ2, КЗ3, КЗ4, КЗ5, КФ1, КФ2, КФ3, КФ5, КФ6, КФ7, КФ8, КФ9, КФ10	Практичне заняття 1 4 год	4	Практичне застосування методики управління вразливостями з використанням сканера вразливостей Nessus Professional.

<u>Програмні результати навчання:</u> РН4, РН5, РН6, РН8, РН11, РН13, РН17, РН21 <u>Рекомендовані джерела:</u> 1-6			
<i>Тема 1. Основи забезпечення кібербезпеки сучасного підприємства. Роль і місце технологій виявлення вразливостей мережевих ресурсів у системі забезпечення кібербезпеки. Впровадження процесу управління вразливостями.</i> <u>Знати:</u> 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. <u>Вміти:</u> застосовувати методику управління вразливостями: здійснювати заходи підготовчого етапу; здійснювати початкове сканування вразливостей; визначати коригуючі дії або приймати ризик; здійснювати коригувальні дії; здійснювати перевірку (ресканування). <u>Формування компетенцій:</u> КЗ1, КЗ2, КЗ3, КЗ4, КЗ5, КФ1, КФ2, КФ3, КФ5, КФ6, КФ7, КФ8, КФ9, КФ10 <u>Програмні результати навчання:</u> РН4, РН5, РН6, РН8, РН11, РН13, РН17, РН21 <u>Рекомендовані джерела:</u> 1-6	Самостійна робота 1 10 год	2	Самостійна підготовка. Удосконалення отриманих знань та умінь, отриманих (надбаних) за попередніми лекцією та практичним заняттям.
<i>Тема 2. Основи інформаційно-аналітичної діяльності фахівців з кібербезпеки.</i> <u>Знати:</u> 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. <u>Формування компетенцій:</u> КЗ1, КЗ2, КЗ3, КЗ4, КЗ5, КФ1, КФ2, КФ3, КФ5, КФ6, КФ7, КФ8, КФ9, КФ10 <u>Програмні результати навчання:</u> РН4, РН5, РН6, РН8, РН11, РН13, РН17, РН21 <u>Рекомендовані джерела:</u> 1-6	Лекція 2 2 год		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; налаштувати політики сканування. Формування компетенцій: КЗ1, КЗ2, КЗ3, КЗ4, КЗ5, КФ1, КФ2, КФ3, КФ5, КФ6, КФ7, КФ8, КФ9, КФ10 Програмні результати навчання: РН4, РН5, РН6, РН8, РН11, РН13, РН17, РН21 Рекомендовані джерела: 5, 6	Практичне заняття 2 4 год	4	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 з кібербезпеки; методологію сканування, параметри активного розкладу сканування, конфігурацію політики сканування, налаштування політики сканування. Вміти: застосовувати конфігурації політики сканування; налаштувати політики сканування. Формування компетенцій: КЗ1, КЗ2, КЗ3, КЗ4, КЗ5, КФ1, КФ2, КФ3, КФ5, КФ6, КФ7, КФ8, КФ9, КФ10 Програмні результати навчання: РН4, РН5, РН6, РН8, РН11, РН13, РН17, РН21 Рекомендовані джерела: 1-6	Самостійна робота 2 7 год	2	Самостійна підготовка. Удосконалення отриманих знань та умінь, отриманих (надбаних) за попередніми лекцією та практичним заняттям.
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	Лекція 3 2 год		Лекція-візуалізація

застосування технології тестування на проникнення для різних варіантів. Формування компетенцій: КЗ1, КЗ2, КЗ3, КЗ4, КЗ5, КФ1, КФ2, КФ3, КФ5, КФ6, КФ7, КФ8, КФ9, КФ10 Програмні результати навчання: РН4, РН5, РН6, РН8, РН11, РН13, РН17, РН21 Рекомендовані джерела: 1-6			
Тема 3. Основи застосування сканера вразливостей Nessus Professional. Основи сканування. Знати: шаблони сканування та політик. Вміти: застосовувати шаблони сканування та політик. Формування компетенцій: КЗ1, КЗ2, КЗ3, КЗ4, КЗ5, КФ1, КФ2, КФ3, КФ5, КФ6, КФ7, КФ8, КФ9, КФ10 Програмні результати навчання: РН4, РН5, РН6, РН8, РН11, РН13, РН17, РН21 Рекомендовані джерела: 5, 6	Практичне заняття 3 4 год	4	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; принципи 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; шаблони сканування та політик. Вміти: застосовувати шаблони сканування та політик. Формування компетенцій: КЗ1, КЗ2, КЗ3, КЗ4, КЗ5, КФ1, КФ2, КФ3, КФ5, КФ6, КФ7, КФ8, КФ9, КФ10 Програмні результати навчання: РН4, РН5, РН6, РН8, РН11, РН13, РН17, РН21 Рекомендовані джерела: 1-6	Самостійна робота 3 7 год	2	Самостійна підготовка. Удосконалення отриманих знань та умінь, отриманих (надбаних) за попередніми лекцією та практичним заняттям.
Тема 4. Технології виявлення вразливостей мережевих ресурсів. Загальні положення. Знати: технологію сканування мережі; порядок визначення топології мережі; місця розміщення сканерів уразливостей; порядок визначення	Лекція 4 2 год		Лекція-візуалізація

цілей сканування; стратегії сканування; користувальницькі вимоги; методологію сканування: параметри розкладу активного сканування; конфігурація політики сканування; налаштування політики сканування. <u>Формування компетенцій:</u> КЗ1, КЗ2, КЗ3, КЗ4, КЗ5, КФ1, КФ2, КФ3, КФ5, КФ6, КФ7, КФ8, КФ9, КФ10 <u>Програмні результати навчання:</u> РН4, РН5, РН6, РН8, РН11, РН13, РН17, РН21 <u>Рекомендовані джерела:</u> 1-6			
Тема 4. Основи застосування сканера вразливостей Nessus Professional. Налаштування сканування та політики. <u>Знати:</u> порядок налаштування сканування та політики. <u>Вміти:</u> налаштовувати сканування виявлення. <u>Формування компетенцій:</u> КЗ1, КЗ2, КЗ3, КЗ4, КЗ5, КФ1, КФ2, КФ3, КФ5, КФ6, КФ7, КФ8, КФ9, КФ10 <u>Програмні результати навчання:</u> РН4, РН5, РН6, РН8, РН11, РН13, РН17, РН21 <u>Рекомендовані джерела:</u> 5, 6	Практичне заняття 4 4 год	4	Практичне застосування методики управління вразливостями з використанням сканера вразливостей Nessus Professional.
Тема 4. Технології сканування мережевих ресурсів. Загальні положення. <u>Знати:</u> 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; порядок налаштування сканування та політики. <u>Вміти:</u> налаштовувати сканування виявлення. <u>Формування компетенцій:</u> КЗ1, КЗ2, КЗ3, КЗ4, КЗ5, КФ1, КФ2, КФ3, КФ5, КФ6, КФ7, КФ8, КФ9, КФ10 <u>Програмні результати навчання:</u> РН4, РН5, РН6, РН8, РН11, РН13, РН17, РН21 <u>Рекомендовані джерела:</u> 1-6	Самостійна робота 4 7 год	3	Самостійна підготовка. Удосконалення отриманих знань та умінь, отриманих (надбаних) за попередніми лекцією та практичним заняттям.
Тема 5. Основи застосування сканера вразливостей Nessus Professional. Установки сканування та політик. <u>Знати:</u> 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.	Лекція 5 2 год		Лекція-візуалізація

<u>Формування компетенцій:</u> К31, К32, К33, К34, К35, КФ1, КФ2, КФ3, КФ5, КФ6, КФ7, КФ8, КФ9, КФ10 <u>Програмні результати навчання:</u> РН4, РН5, РН6, РН8, РН11, РН13, РН17, РН21 <u>Рекомендовані джерела:</u> 5, 6			
Тема 5. Основи застосування сканера вразливостей Nessus Professional. Налаштування сканування оцінки. <u>Знати:</u> типи сканувань. <u>Вміти:</u> налаштовувати та створювати звіт сканування; налаштовувати просунуте сканування. <u>Формування компетенцій:</u> К31, К32, К33, К34, К35, КФ1, КФ2, КФ3, КФ5, КФ6, КФ7, КФ8, КФ9, КФ10 <u>Програмні результати навчання:</u> РН4, РН5, РН6, РН8, РН11, РН13, РН17, РН21 <u>Рекомендовані джерела:</u> 5, 6	Практичне заняття 5 4 год	4	Практичне застосування методики управління вразливостями з використанням сканера вразливостей Nessus Professional.
Тема 5. Основи застосування сканера вразливостей Nessus Professional. Установки сканування та політик. <u>Знати:</u> 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. <u>Вміти:</u> налаштовувати та створювати звіт сканування; налаштовувати просунуте сканування. <u>Формування компетенцій:</u> К31, К32, К33, К34, К35, КФ1, КФ2, КФ3, КФ5, КФ6, КФ7, КФ8, КФ9, КФ10 <u>Програмні результати навчання:</u> РН4, РН5, РН6, РН8, РН11, РН13, РН17, РН21 <u>Рекомендовані джерела:</u> 5, 6	Самостійна робота 5 7 год	3	Самостійна підготовка. Удосконалення отриманих знань та умінь, отриманих (надбаних) за попередніми лекцією та практичним заняттям.
Тема 6. Основи застосування IBM QRadar Vulnerability Manager. Призначення та можливості програмного комплексу. <u>Знати:</u> 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. <u>Формування компетенцій:</u> К31, К32, К33, К34, К35, КФ1, КФ2, КФ3, КФ5, КФ6, КФ7, КФ8, КФ9, КФ10	Лекція 6 2 год		Лекція-візуалізація

<u>Програмні результати навчання:</u> PH4, PH5, PH6, PH8, PH11, PH13, PH17, PH21 <u>Рекомендовані джерела:</u> 7-10			
Тема 6. Основи застосування сканера вразливостей Nessus Professional. Аналіз результатів сканування. <u>Знати:</u> зміст панелі інструментів та можливості Nessus Professional. <u>Вміти:</u> застосовувати сканер та проводити аналіз вразливостей. <u>Формування компетенцій:</u> К31, К32, К33, К34, К35, КФ1, КФ2, КФ3, КФ5, КФ6, КФ7, КФ8, КФ9, КФ10 <u>Програмні результати навчання:</u> PH4, PH5, PH6, PH8, PH11, PH13, PH17, PH21 <u>Рекомендовані джерела:</u> 5, 6	Практичне заняття 6 4 год	4	Практичне застосування методики управління вразливостями з використанням сканера вразливостей Nessus Professional.
Тема 6. Основи застосування IBM QRadar Vulnerability Manager. Призначення та можливості програмного комплексу. <u>Знати:</u> 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. <u>Формування компетенцій:</u> К31, К32, К33, К34, К35, КФ1, КФ2, КФ3, КФ5, КФ6, КФ7, КФ8, КФ9, КФ10 <u>Програмні результати навчання:</u> PH4, PH5, PH6, PH8, PH11, PH13, PH17, PH21 <u>Рекомендовані джерела:</u> 7-10	Самостійна робота 6 7 год	3	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 краці практики. <u>Знати:</u> 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 пропускну здатності мережі для одночасного сканування активів; карти мережевого інтерфейсу на сканерах; порядок управління вразливістю; зміст повідомлення про сканування вразливості; порядок запуску сканування нових активів. <u>Формування компетенцій:</u> К31, К32, К33, К34, К35, КФ1, КФ2, КФ3, КФ5, КФ6, КФ7, КФ8, КФ9, КФ10	Лекція 7 2 год		Лекція-візуалізація

<u>Програмні результати навчання:</u> PH4, PH5, PH6, PH8, PH11, PH13, PH17, PH21 <u>Рекомендовані джерела:</u> 7-10			
Тема 7. Основи застосування IBM QRadar Vulnerability Manager. Налаштування сканування вразливостей та кращі практики. <u>Знати:</u> типи політики сканування в IBM QRadar Vulnerability Manager; типові місця розміщення сканера в мережі. <u>Вміти:</u> налаштувати конфігурації пошуку активів; налаштувати продуктивність виявлення активів; здійснювати сканування веб-додатків та проводити динамічне сканування. <u>Формування компетенцій:</u> K31, K32, K33, K34, K35, КФ1, КФ2, КФ3, КФ5, КФ6, КФ7, КФ8, КФ9, КФ10 <u>Програмні результати навчання:</u> PH4, PH5, PH6, PH8, PH11, PH13, PH17, PH21 <u>Рекомендовані джерела:</u> 7-10	Практичне заняття 7 4 год	4	Практичне застосування методики управління вразливостями з використанням програмного комплексу IBM QRadar Vulnerability Manager.
Тема 7. Основи застосування IBM QRadar Vulnerability Manager. Налаштування сканування вразливостей та кращі практики. <u>Знати:</u> 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 пропускну здатності мережі для одночасного сканування активів; карти мережевого інтерфейсу на сканерах; порядок управління вразливістю; зміст повідомлення про сканування вразливості; порядок запуску сканування нових активів. <u>Вміти:</u> налаштувати конфігурації пошуку активів; налаштувати продуктивність виявлення активів; здійснювати сканування веб-додатків та проводити динамічне сканування. <u>Формування компетенцій:</u> K31, K32, K33, K34, K35, КФ1, КФ2, КФ3, КФ5, КФ6, КФ7, КФ8, КФ9, КФ10 <u>Програмні результати навчання:</u> PH4, PH5, PH6, PH8, PH11, PH13, PH17, PH21 <u>Рекомендовані джерела:</u> 7-10	Самостійна робота 7 7 год	3	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. <u>Знати:</u> зміст та порядок керування виявленими вразливостями. Common Vulnerability Scoring System (CVSS); порядок дослідження	Лекція 8 2 год		Лекція-візуалізація

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: КЗ1, КЗ2, КЗ3, КЗ4, КЗ5, КФ1, КФ2, КФ3, КФ5, КФ6, КФ7, КФ8, КФ9, КФ10 Програмні результати навчання: РН4, РН5, РН6, РН8, РН11, РН13, РН17, РН21 Рекомендовані джерела: 7-10			
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: КЗ1, КЗ2, КЗ3, КЗ4, КЗ5, КФ1, КФ2, КФ3, КФ5, КФ6, КФ7, КФ8, КФ9, КФ10 Програмні результати навчання: РН4, РН5, РН6, РН8, РН11, РН13, РН17, РН21 Рекомендовані джерела: 7-10	Практичне заняття 8 4 год	4	Практичне застосування методики управління вразливостями з використанням програмного комплексу 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. Вміти: керувати виявленими вразливостями в середовищі IBM QRadar Vulnerability Manager.	Самостійна робота 8 7 год	3	Самостійна підготовка. Удосконалення отриманих знань та умінь, отриманих (надбаних) за попередніми лекцією та практичним заняттям.

<u>Формування компетенцій:</u> К31, К32, К33, К34, К35, КФ1, КФ2, КФ3, КФ5, КФ6, КФ7, КФ8, КФ9, КФ10 <u>Програмні результати навчання:</u> РН4, РН5, РН6, РН8, РН11, РН13, РН17, РН21 <u>Рекомендовані джерела:</u> 7-10			
Тема 9. Технологія управління вразливостями в корпоративній інформаційній системі з використанням IBM QRadar SIEM та Tenable.sc. <u>Знати:</u> 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. <u>Формування компетенцій:</u> К31, К32, К33, К34, К35, КФ1, КФ2, КФ3, КФ5, КФ6, КФ7, КФ8, КФ9, КФ10 <u>Програмні результати навчання:</u> РН4, РН5, РН6, РН8, РН11, РН13, РН17, РН21 <u>Рекомендовані джерела:</u> 7-10	Лекція 9 2 год		Лекція-візуалізація
Тема 9. Основи застосування IBM QRadar Vulnerability Manager. Порядок інтеграції зі сканерами Tenable.io та Tenable.sc. <u>Знати:</u> порядок додавання сканування Tenable.sc до IBM QRadar SIEM. <u>Вміти:</u> планувати та застосовувати сканування вразливостей в IBM QRadar SIEM. <u>Формування компетенцій:</u> К31, К32, К33, К34, К35, КФ1, КФ2, КФ3, КФ5, КФ6, КФ7, КФ8, КФ9, КФ10 <u>Програмні результати навчання:</u> РН4, РН5, РН6, РН8, РН11, РН13, РН17, РН21 <u>Рекомендовані джерела:</u> 7-10	Практичне заняття 9 4 год	4	Практичне застосування методики управління вразливостями з використанням програмного комплексу IBM QRadar Vulnerability Manager.
Тема 9. Технологія управління вразливостями в корпоративній інформаційній системі з використанням IBM QRadar SIEM та Tenable.sc. <u>Знати:</u> 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 7 год	3	Самостійна підготовка. Удосконалення отриманих знань та умінь, отриманих (надбаних) за попередніми лекцією та практичним заняттям.

<u>Вміти:</u> планувати та застосовувати сканування вразливостей в IBM QRadar SIEM. <u>Формування компетенцій:</u> КЗ1, КЗ2, КЗ3, КЗ4, КЗ5, КФ1, КФ2, КФ3, КФ5, КФ6, КФ7, КФ8, КФ9, КФ10 <u>Програмні результати навчання:</u> РН4, РН5, РН6, РН8, РН11, РН13, РН17, РН21 <u>результати навчання:</u> ПРН-18, ПРН-19, ПРН-20, ПРН-26, ПРН-27 <u>Рекомендовані джерела:</u> 7-10			
МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ			
Навчальна лабораторія реагування на кіберінциденти: 1. Комп'ютери Dell OptiPlex 3050/Core i5 7500T – 14 шт. 2. Мультимедійна система Acer 113 – 1 шт. 3. Набір серверів Server Dell PE R530 – 3шт. 4. Робочі станції Dell Precision Tower 3620 i7 – 14 шт. Dell OptiPlex 3050 i5; 5. Маршрутизатор Mikrotik CSS326-24G-2S+RM. – 1 шт. 6. Комутатор Mikrotik CSS326-24G-2S+ RM – 1шт. Програмно-апаратні комплекси: 1. ESET PROTECT Enterprise On-Prem. № ліцензії – A33-AMJ-UTU, до 30.11.2026. Кількість пристроїв – 60. 2. IBM QRadar SIEM. № ліцензії – 31XX-SIEM-QRM-QVM. . Навчальна ліцензія 3. IBM i2 Analyst's Notebook Premium. Навчальна ліцензія 4. Tenable Nessus Professional. Навчальна ліцензія			
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.			
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 студент 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 студент повинен вказати джерело, використане в ході виконання завдання. У разі виявлення факту плагіату студент отримує за завдання 0 балів. • Студент, 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 студент видаляється з заняття, за заняття отримує 0 балів.

* КРИТЕРІЇ ТА МЕТОДИ ОЦІНЮВАННЯ

Умовою допуску до підсумкового контролю є набрання студентом 60 балів у сукупності за всіма темами дисципліни

Форми контролю	Види навчальної роботи	Оцінювання
ПОТОЧНИЙ КОНТРОЛЬ	Робота на заняттях, у т.ч.:	
	• Виконання практичних робіт • Самостійна робота	36 балів 23 бала
Додаткова оцінка	Участь у наукових конференціях, підготовка наукових публікацій, отримання міжнародного сертифікату за напрямом.	10 балів за рішенням викладача
ПІДСУМКОВЕ ОЦІНЮВАННЯ <i>ісnum</i>	Метою заліку є контроль сформованості практичних навичок та професійних компетентностей, необхідних для виконання наукової роботи. Іспит проходить у письмовій формі.	40 балів

ПІДСУМКОВА ОЦІНКА ЗА ДИСЦИПЛІНУ

бали	Критерії оцінювання	Рівень компетентності	Оцінка /затис в екзаменаційній відомості
90-100	Студент 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-	Високий Повністю забезпечує вимоги до знань, умінь і навичок, що викладені в робочій програмі дисципліни. Власні пропозиції студента в оцінках і вирішенні практичних задач підвищує його вміння використовувати знання, які він отримав при вивченні інших дисциплін, а також знання, набуті при самостійному поглибленому вивченні питань, що	Відмінно / Зараховано (А)

	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 Студент проявляє невпевненість в тлумаченні теоретичних положень чи складних практичних завдань.	відносяться до дисципліни, яка вивчається.	
82-89	Студент 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 студенту самостійне вирішення основних практичних задач в умовах, коли вихідні дані в них змінюються порівняно з прикладами, що розглянуті при вивченні дисципліни	Добре / Зараховано (B)
75-81	Студент 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)
67-74	Студент 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 розглядалися 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)
60-66	Студент 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, студент 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	Студент може відтворити окремі фрагменти з курсу. Незважаючи на те, що програму навчальної дисципліни студент виконав, працював він пасивно, його відповіді під час практичних робіт в більшості є невірними, необґрунтованими. Цілісність розуміння матеріалу з дисципліни у студента відсутня.	Низький Не забезпечує практичної реалізації задач, що формуються при вивченні дисципліни	Незадовільно з можливістю повторного складання) / Не зараховано (FX) В залікову книжку не представляється
0-34	Студент повністю не виконав вимог робочої програми навчальної дисципліни. Його знання на підсумкових етапах навчання є фрагментарними. Студент не допущений до здачі заліку.	Незадовільний Студент 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 представляється

ПОЛІТИКА ДОБРОЧЕСНОСТІ

Здобувач вищої освіти виконуючи самостійну або індивідуальну роботу повинен дотримуватись політики доброчесності. У разі наявності плагіату в будь-яких видах робіт здобувача, він отримує незадовільну оцінку і повинен повторно виконати завдання, які передбачені у Силабусі.