ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ЗАТВЕРДЖУЮ
Декан факультету інформаційних технологій
_____ Тетяна ГОВОРУЩЕНКО
Підпис Ім'я, ПРІЗВИЩЕ
«_29_»_____08_____2025 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
Теорія проєктування та тестування безпеки захищених систем

Галузь знань	F Інформаційні технології
Спеціальність	F5 Кібербезпека та захист інформації
Рівень вищої освіти	Другий (магістерський)
Освітньо-професійна програма	Кібербезпека та захист інформації
Обсяг дисципліни	9 кредитів ЄКТС
Шифр дисципліни	ОФП.01
Мова навчання	Українська
Статус дисципліни	Обов'язкова (фахової підготовки)
Факультет	Інформаційних технологій
Кафедра	Кібербезпеки

Форма здобуття освіти	Курс	Семестр	Обсяг дисципліни		Кількість годин						Курсовий проєкт	Курсова робота	Форма семестрового контролю	
					Аудиторні заняття					Самостійна робота, у т.ч. ІРЗ				
			Кредити ЄКТС	Години	Разом	Лекції	Лабораторні роботи	Практичні заняття	Семінарські заняття				Залік	Іспит
Д	1	1	5	150	50	16	34			100				+
Д	1	2	4	120	34	16	18			86				+
Разом:			**9**	**270**	**84**	**32**	**52**			**186**				**2**

Робоча програма складена на основі освітньо-професійної програми «Кібербезпека та захист інформації» за спеціальністю F5 «Кібербезпека та захист інформації»

Робоча програма складена _____ канд. техн. наук, доц. Віктор ЧЕШУН
Підпис Науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ

_____ канд. техн. наук, доц. Юрій КЛЬОЦ
Підпис Науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ

Схвалена на засіданні кафедри кібербезпеки
Протокол від «29»08.2025 р.№1

Зав. кафедри кібербезпеки _____ Юрій КЛЬОЦ
Підпис Ім'я, ПРІЗВИЩЕ

Робоча програма розглянута та схвалена вченою радою факультету інформаційних технологій

Голова вченої ради факультету _____ Тетяна ГОВОРУЩЕНКО
Підпис Ім'я, ПРІЗВИЩЕ

Хмельницький 2025

2. ЛИСТ ПОГОДЖЕННЯ

Посада	Назва кафедри	Підпис	Ім'я, ПРІЗВИЩЕ
Зав. кафедри	кібербезпеки		Юрій КЛЬОЦ
Гарант ОП	кібербезпеки		Віра ТІТОВА

3. ПОЯСНЮВАЛЬНА ЗАПИСКА

Дисципліна «Теорія проєктування та тестування безпеки захищених систем» є однією із дисциплін фахової підготовки здобувачів другого (магістерського) рівня вищої освіти, очної (денної) форми здобуття вищої освіти, які навчаються за освітньо-професійною програмою «Кібербезпека та захист інформації» в межах спеціальності F5 «Кібербезпека та захист інформації».

Пререквізити – вихідна, методологія та організація наукових досліджень, моніторинг та менеджмент інформаційної безпеки.

Постреквізити – моніторинг та менеджмент інформаційної безпеки, переддипломна практика, кваліфікаційна робота.

Відповідно до освітньої програми дисципліна сприяє забезпеченню:

компетентностей

ІК. Здатність особи розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки. ЗК01. Здатність застосовувати знання у практичних ситуаціях. ЗК04. Здатність оцінювати та забезпечувати якість виконуваних робіт. ЗК05. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності). ФК01. 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. ФК02. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки. ФК03. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури. ФК05. 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. ФК06. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. ФК08. 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. ФК10. 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. УК02. Здатність проводити тестування на проникнення у відповідності до операційних процесів інформаційних систем та інформаційних активів, розробляти сценарії тестування на проникнення на основі методів та засобів забезпечення мережевої безпеки і джерел вразливостей інформаційних ресурсів, визначати вектори можливих атак та демонструвати використання технічних вразливостей в рамках чинного законодавства,

загальних та організаційно-технічних вимог. УК03. Здатність застосовувати принципи мережевої безпеки до вимог, що стосуються конфіденційності, цілісності, доступності та аутентифікації, адмініструвати та забезпечувати безпеку мережевих комунікацій, в тому числі інтегруючі засоби віртуальних приватних мереж, проєктувати мережі, розуміючи цілі безпеки, операційні цілі та компроміси між ними.

програмних результатів навчання

ПРН1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. ПРН3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі. ПРН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки. ПРН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. ПРН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури. ПРН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації. ПРН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації. ПРН13. 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. ПРН15. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб. ПРН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень. ПРН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки. ПРН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проєкти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності. ПРН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик. ПРН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації. ПРН25. Проводити тестування на проникнення у відповідності до операційних процесів інформаційних систем та інформаційних активів, розробляти сценарії тестування на проникнення на основі методів та засобів забезпечення мережевої безпеки і джерел вразливостей інформаційних ресурсів, визначати вектори можливих атак та демонструвати використання технічних вразливостей в рамках чинного законодавства, загальних та організаційно-технічних вимог. ПРН26. Застосовувати принципи мережевої безпеки до вимог, що стосуються конфіденційності, цілісності, доступності та аутентифікації, адмініструвати та забезпечувати безпеку мережевих комунікацій, в тому числі інтегруючі засоби віртуальних приватних мереж, проєктувати мережі, розуміючи цілі безпеки, операційні цілі та компроміси між ними.

Мета дисципліни. Формування у студентів системних знань і практичних навичок з тестування на проникнення на базі освоєння принципів та методів збору цифрової інформації

для дослідження вразливостей операційних систем, комп'ютерних та бездротових мереж, хмарних технологій, технологій Інтернету речей та SCADA; проведення статичного аналізу вразливостей інформаційних систем, використовуючи інструменти та методи тестування на проникнення; розробки та проєктування захищених інформаційних систем; розробки, впровадження та використання методів та засобів технічного захисту інформації; розробки систем управління доступом до інформаційних ресурсів; планування навчання, контролю та супроводу роботи з персоналом тощо.

Предмет дисципліни. Сучасні процеси дослідження, аналізу, створення та забезпечення функціонування інформаційних систем і технологій, інших бізнес-операційних процесів на об'єктах інформаційної діяльності та критичних інфраструктур сфери інформаційної безпеки та/або кібербезпеки; інфраструктура об'єктів інформаційної діяльності та критичних інфраструктур; системи та комплекси створення, обробки, передачі, зберігання, знищення, захисту та відображення даних (інформаційних потоків); програмне та програмно-апаратне забезпечення (засоби) кіберзахисту; інформаційні системи (інформаційно-комунікаційні, інформаційно-телекомунікаційні, автоматизовані) та технології; інструменти та методи тестування на проникнення.

Завданням дисципліни Формування у майбутніх спеціалістів умінь, навичок та компетентностей для аналізу вразливостей інформаційних систем та технології тестування на проникнення, проєктування захищених операційних систем, мереж та веб-ресурсів, технічного та організаційного захисту інформаційних систем у т. ч. з використанням спеціального апаратного та програмного забезпечення.

Результати навчання. Здобувач, який успішно завершив вивчення дисципліни, повинен: вільно *володіти* державною мовою для представлення практичної діяльності та обговорення питань аналізу вразливостей, тестування на проникнення, технічного й організаційного захисту інформації, мережевої безпеки; *обґрунтовувати* та *доносити* висновки, знання та пояснення; *планувати* навчання, *супроводжувати* та *контролювати* персонал; *розробляти*, *впроваджувати*, *удосконалювати* ІТ у сфері безпеки; *проводити* дослідження, *реалізовувати* проєкти, *впроваджувати* стандарти та практики; *аналізувати* та *забезпечувати* управління доступом; *розробляти* та *оцінювати* методи захисту; *забезпечувати* безперервність процесів; *приймати* рішення, обґрунтовувати вибір ПЗ та інструментів; *адаптувати* методи тестування, *розробляти* сценарії, *класифікувати* вразливості, *демонструвати* їх використання; *забезпечувати* конфіденційність, цілісність, доступність, *адмініструвати* мережі та *проєктувати* їх з урахуванням цілей безпеки.

4. СТРУКТУРА ЗАЛІКОВИХ КРЕДИТІВ ДИСЦИПЛІНИ

І семестр

Назва теми	**Кількість годин відведених на:**		
	лекції	**лабораторні роботи**	**СРС**
Тема 1. Проєктування захищених операційних систем, мереж та веб-ресурсів	8	20	48
Тема 2. Технічний та організаційний захист інформаційних систем	8	14	52
Разом:	**16**	**34**	**100**

II семестр

Назва теми	Кількість годин відведених на:		
	лекції	**лабораторні роботи**	**СРС**
Тема 1. Аналіз вразливостей та технології тестування кібербезпеки	12	18	70
Тема 2. Теоретичні засади тестування на проникнення	4	-	16
Разом:	**16**	**18**	**86**

5. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

5.1 Зміст лекційного курсу

Перелік лекцій (I семестр)

Номер лекції	Перелік тем лекцій, їх анотація	Години
Тема 1. Проєктування захищених операційних систем, мереж та веб-ресурсів		**8**
1	**Проєктування та розробка захищених операційних систем (ОС)** Принципи створення захищених ОС. Розробка захищених ОС "з нуля". Побудова "довірених" версій шляхом модернізації існуючих ОС. Визначення вимог до архітектури комплексу засобів захисту в залежності від задач, які виконує ОС. Адміністративні заходи захисту. Літ.: [4] с. 28-36, 140-166;	2
2	**Концепції та методологія безпеки мережевої інфраструктури** Принципи організації безпеки мережевої інфраструктури. Моделі управління мережевими ресурсами. Безпека міжмережевої взаємодії. Технології побудови захищених корпоративних мереж. Проєктування мереж, включаючи розуміння цілей безпеки, операційних цілей та компромісів між ними. Літ.: [4] с. 59-116, 166-197, 227-306; [26]; [27]; [32]; [33]; [34]	2
3	**Технології Honeynets та Deception, DLP-системи** Переваги та недоліки застосування технологій Sandboxing, Honeypots, Honeynets, та Deception у мережевій інфраструктурі. Підвищення мережної безпеки за рахунок впровадження Honeynet- та Deception-технологій. Аналіз недоліків систем DLP. DLP-системи та закон. Методи для підвищення ефективності та законності DLP-систем. Особливості проєктування систем DLP. Літ.: [20]; [21];	2
4	**Проєктування та розробка захищених веб-ресурсів** Архітектура, функціонування та механізми безпеки веб-додатків і веб-серверів. Взаємодія між веб-сервісами. REST-інтерфейс та його безпека. Особливості застосування баз даних для побудови захищених веб-рішень. Відкритий проект по забезпеченню безпеки веб-додатків (OWASP). Перспективи організації та виконання тестування рівня безпеки для певного веб-ресурсу. Літ.: [5] с. 298-357; [9]; [10]	2
Тема 2. Технічний та організаційний захист інформаційних систем		**8**
5	**Аутентифікація і системи контролю та управління доступом (СКУД)** Аналіз існуючих підходів до вирішення задач аутентифікації. Біометрична аутентифікація на основі розпізнавання зображень (штучні нейронні та	2

	капсульні мережі, алгоритм розпізнавання облич Eigenface та його реалізація). Визначення вимог до СКУД відповідно до політики інформаційної безпеки. Обґрунтування моделі управління доступом. Концепція та етапи створення СКУД. Розробка технічного завдання, проєктування, дослідна експлуатація, супровід. Літ.: [4] с. 115-166; [25]	
6	**Методи та засоби захисту від витоку інформації.** Ідентифікація та дослідження каналів витоку інформації. Організаційно-технічні заходи щодо блокування каналів витоку інформації на об'єкті. Проєктування систем захисту від витоку інформації. Літ.: [6] с. 92-109, 206-229, 250-408	2
7	**Захист інформації на об'єктах критичної інфраструктури** Визначення інформації, що потребує захисту на об'єктах критичної інфраструктури (ОКІ). Канали витоку інформації та підстави їх утворення. Засоби та комплекси виявлення прихованого підключення до інформаційних мереж (радіозакладні пристрої, приховане під'єднання до ліній зв'язку, приховані відеокамери, прихований майнінг тощо). Порядок проведення обстеження і аналізу ОКІ з метою забезпечення захисту інформації. Літ.: [6] с. 111-206, 229-274	2
8	**Організація режиму та охорони, робота з персоналом** Робота з документами та документованою інформацією, організація розробки і використання документів та носіїв конфіденційної інформації, їх облік, виконання, повернення, зберігання і знищення. Використання технічних засобів збору, обробки, накопичення і зберігання конфіденційної інформації. Підбір та розстановка персоналу. Навчання персоналу. Контроль за роботою персоналу. Відповідальність за порушення правил захисту інформації. Літ.: [4] с. 210-310; [35]	2
	Разом за семестр:	**16**

Перелік лекцій (II семестр)

Номер лекції	Перелік тем лекцій, їх анотація	Години
Тема 1. Аналіз вразливостей та технології тестування кібербезпеки		**12**
1	**Методи тестування безпеки систем** Методологія організації атак на кібербезпеку. Різні класи атак. Етапи кібератак. Категорії кіберзловмисників. Методики тестування стійкості (безпеки) мережних пристроїв (брандмауера, маршрутизатора, комутатора). Методики тестування стійкості (безпеки) систем виявлення вторгнень. Літ.: [7] с. 18-163; [13]; [28]; [30]	2
2	**Розвідка на основі відкритих джерел (OSINT)** OSINT через Всесвітню павутину (WWW), аналіз веб-сайтів, DNS-опитування. Автоматизація роботи з OSINT за допомогою інструментів/фреймворків/скриптів. Літ.: [3] с. 13-193; [16]; [29]	2
3	**Аналіз вразливостей та тестування безпеки комп'ютерних мереж** Інформація зовнішньої мережі, розвідка, сканування та аналіз вразливостей. Внутрішня мережна інформаційна розвідка, перебір внутрішньої мережі, сканування та аналіз вразливостей. Аналіз вразливостей локальної та віддаленої систем за допомогою визначених сценаріїв. Загальні вектори атак на мережевому рівні. Мережеві атаки, зв'язок мережевої атаки із загрозами та вразливими місцями.	2

	Літ.: [1] с. 8-134; [31]	
4	**Аналіз вразливостей та тестування безпеки бездротових мереж, Інтернету речей, OT/SCADA та хмарних технологій.** Аналіз вразливостей WLAN. Процес аналізу трафіка. Методологія проведення атаки. Атаки на Bluetooth. Аналіз вразливостей IoT та OT/SCADA. Проблеми безпеки в IoT та OT/SCADA. Зовнішні системи збору даних. Поверхня атаки і пов'язані загрози. Спеціальні методики виявлення вразливостей. Аналіз вразливостей хмари. Обмеження хмарних архітектур з точки зору інформаційної безпеки. Спеціальні методики виявлення вразливостей. Літ.: [2] с. 135-151, 215-239;	2
5	**Аналіз вразливостей веб-ресурсів** Аналіз методів збору інформації. Карта веб-додатка. Виявлення кінцевих точок та сторонніх залежностей. Ознаки нестійкої (небезпечної) архітектури веб-додатків. Методи пошуку слабких місць в архітектурі додатків. Виявлення вразливостей за допомогою визначених сценаріїв. Аналіз типових атак на веб-додатки та особливості їх проведення. Літ.: [2] с. 115-135; [9]; [10]	2
6	**Бінарний аналіз вразливостей програмного забезпечення** Принципи та підходи бінарного аналізу. Інструментарій бінарного аналізу. Аналіз вразливостей програмного забезпечення. Літ.: [8] с. 35-54, 113-303	2
Тема 2. Теоретичні засади тестування на проникнення		**4**
7	**Юридичні аспекти та організаційне забезпечення тестування на проникнення** Безпека та тестування на проникнення. Аналіз видів та цілей тестування на проникнення. Юридичні причини, правові рамки тестування на проникнення та їх обмеження. Аналіз та формування загальних вимог до тестування на проникнення. Формування організаційно-технічних вимог з врахуванням етичних обмежень. Особливості формування вимог до персоналу. Літ.: [7] с. 164-255; [11]; [12]; [13]	2
8	**Методика та документаційне забезпечення тестування на проникнення** П'ять фаз експерименту тестування на проникнення, особливості його проведення. Аналіз модулів та процедур тестування. Етапи планування та написання звітів за результатами тестування. Особливості проведення сертифікації тестерів на проникнення. Літ.: [7] с. 164-255; [14]	2
	Разом за семестр:	**16**

5.2 Зміст лабораторних робіт

Перелік лабораторних робіт (І семестр)

№ п/п	Теми лабораторних робіт	Кількість годин
Тема 1. Проєктування захищених операційних систем, мереж та веб-ресурсів		**20**
1	Проєктування "довіреної" версії ОС за допомогою антивірусного захисту. Літ.: [4] с. 28-36, 140-166; [23]; [24]	4
2	Проєктування захищеної мережі на основі технології Honeypot. Літ.: [4] с. 59-116, 166-197, 227-306; [20]; [21]; [23]	4

3	Проєктування захищеної мережі на основі технології Deception. Літ.: [4] с. 59-116, 166-197, 227-306; [20]; [21]; [23]	4
4	Проєктування та дослідження DLP-системи. Літ.: [4] с. 59-116, 166-197, 227-306; [20]; [21]; [23]	4
5	Забезпечення безпеки багатокомпонентних веб-додатків. Літ.: [5] с. 298-357; [9]; [10]; [23]	4
Тема 2. Технічний та організаційний захист інформаційних систем		**14**
6	Проєктування системи аутентифікації на основі розпізнавання зображень. Літ.: [4] с. 115-166; [22]	4
7	Проєктування системи відеомоніторингу, контролю та управління доступом. Літ.: [4] с. 115-166; [22]	4
8	Проєктування систем захисту від витоку інформації акустичними каналами та через побічне електромагнітне випромінювання. Літ.: [6] с. 92-109, 206-229, 250-408; [22]	4
9	Узагальнення матеріалу. Тестування	2
	Разом за семестр:	**34**

Перелік лабораторних робіт (II семестр)

№ п/п	**Теми лабораторних робіт**	**Кількість годин**
Тема 1. Аналіз вразливостей та технології тестування кібербезпеки		**18**
1	Розвідка та збирання інформації з відкритих джерел за допомогою Maltego Літ.: [3] с. 13-193; [15]; [16]	2
2	Розгортання pen-test станції. Підготовка до роботи Metasploit та postgresql Літ.: [1] с. 12-88; [7] с. 18-163; [13]; [19]	2
3	Збір інформації та аналіз вразливостей за допомогою Metasploit Літ.: [1] с. 88-134; [7] с. 18-163; [13]; [19]	2
4	Дослідження використання енкодерів для обходу захисту антивірусних програм Літ.: [2] с. 70-85; [7] с. 18-163; [13]; [19]	2
5	Дослідження експлуатації та пост-експлуатації виявлених вразливостей Літ.: [2] с. 85-115; [7] с. 18-163; [13]; [19]	2
6	Дослідження стійкості паролів WPA2/WPA за допомогою Hashcat в Kali Linux Літ.: [2] с. 23-39, 135-151, 215-239; [7] с. 18-163; [13]; [17]; [18]	2
7	Дослідження стійкості мережі через стрес-тести (DoS веб-сайту) з SlowHTTPTest в Kali Linux Літ.: [1] с. 8-134; [17]; [18]	2
8	Аналіз уразливостей WordPress: WPScanner і Plecost. Робота з W3af в Kali Linux Літ.: [2] с. 115-135; [9]; [10]; [17]; [18]	2
9	Узагальнення матеріалу. Тестування	2
	Разом за семестр:	**18**

5.3 Зміст самостійної (у т.ч. індивідуальної) роботи

Самостійна робота студентів полягає у опрацюванні теоретичного матеріалу з відповідних джерел інформації, підготовці до виконання та захисту лабораторних робіт, до тестування тощо. Керівництво самостійною роботою здійснює викладач згідно з розкладом консультацій в позаурочний час.

№ тижня	Теми самостійної роботи (І семестр)	Кількість годин
1	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №1. Підготовка до виконання лабораторної роботи №1.	6
2	Опрацювання теоретичного матеріалу лекції №1. Оформлення звіту та підготовка до захисту лабораторної роботи №1.	6
3	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №2. Підготовка до виконання лабораторної роботи №2.	6
4	Опрацювання теоретичного матеріалу лекції №2. Оформлення звіту та підготовка до захисту лабораторної роботи №2.	6
5	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №3. Підготовка до виконання лабораторної роботи №3.	6
6	Опрацювання теоретичного матеріалу лекції №3. Оформлення звіту та підготовка до захисту лабораторної роботи №3.	6
7	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №4. Підготовка до виконання лабораторної роботи №4.	6
8	Опрацювання теоретичного матеріалу лекції №4. Оформлення звіту та підготовка до захисту лабораторної роботи №4.	6
9	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №5. Підготовка до виконання лабораторної роботи №5.	6
10	Опрацювання теоретичного матеріалу лекції №5. Оформлення звіту та підготовка до захисту лабораторної роботи №5.	6
11	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №6. Підготовка до виконання лабораторної роботи №6.	6
12	Опрацювання теоретичного матеріалу лекції №6. Оформлення звіту та підготовка до захисту лабораторної роботи №6.	6
13	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №7. Підготовка до виконання лабораторної роботи №7.	6
14	Опрацювання теоретичного матеріалу лекції №7. Оформлення звіту та підготовка до захисту лабораторної роботи №7.	6
15	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №8. Підготовка до виконання лабораторної роботи №8.	6
16	Опрацювання теоретичного матеріалу лекції №8. Оформлення звіту та підготовка до захисту лабораторної роботи №8.	6
17	Підготовка до тестування за пройденим теоретичним матеріалом.	4
	Разом за семестр:	100

№ тижня	Теми самостійної роботи (ІІ семестр)	Кількість годин
1	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №1. Підготовка до виконання лабораторної роботи №1.	5
2	Опрацювання теоретичного матеріалу лекції №1. Оформлення звіту та підготовка до захисту лабораторної роботи №1.	5
3	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №2. Підготовка до виконання лабораторної роботи №2.	5
4	Опрацювання теоретичного матеріалу лекції №2. Оформлення звіту та підготовка до захисту лабораторної роботи №2.	5
5	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №3. Підготовка до виконання лабораторної роботи №3.	5
6	Опрацювання теоретичного матеріалу лекції №3. Оформлення звіту та підготовка до захисту лабораторної роботи №3.	5
7	Опрацювання конспекту лекцій та теоретичного матеріалу лекції	5

	№4. Підготовка до виконання лабораторної роботи №4.	
8	Опрацювання теоретичного матеріалу лекції №4. Оформлення звіту та підготовка до захисту лабораторної роботи №4.	5
9	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №5. Підготовка до виконання лабораторної роботи №5.	5
10	Опрацювання теоретичного матеріалу лекції №5. Оформлення звіту та підготовка до захисту лабораторної роботи №5.	5
11	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №6. Підготовка до виконання лабораторної роботи №6.	5
12	Опрацювання теоретичного матеріалу лекції №6. Оформлення звіту та підготовка до захисту лабораторної роботи №6.	5
13	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №7. Підготовка до виконання лабораторної роботи №7.	5
14	Опрацювання теоретичного матеріалу лекції №7. Оформлення звіту та підготовка до захисту лабораторної роботи №7.	5
15	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №8. Підготовка до виконання лабораторної роботи №8.	5
16	Опрацювання теоретичного матеріалу лекції №8. Оформлення звіту та підготовка до захисту лабораторної роботи №8.	5
17	Підготовка до тестування за пройденим теоретичним матеріалом.	6
	Разом за семестр:	86

6. ТЕХНОЛОГІЇ ТА МЕТОДИ НАВЧАННЯ

Процес навчання з дисципліни ґрунтується на використанні традиційних та сучасних методів. Зокрема, лекції проводяться з використанням словесних, наочних та проблемних методів з супроводом презентаційних матеріалів; лабораторні роботи – з використанням практичних, частково-пошукових та ігрових методів, із застосуванням сучасних інформаційно-комп'ютерних технологій; самостійна робота (опрацювання теоретичного матеріалу, підготовка до виконання та захисту лабораторних робіт, тестування), з використанням пояснювально-ілюстративних та дослідницьких методів, інформаційно-комп'ютерних технологій та технологій дистанційного навчання.

7. МЕТОДИ КОНТРОЛЮ

Поточний контроль здійснюється під час лабораторних занять, а також у дні проведення контрольних заходів, встановлених робочою програмою і графіком освітнього процесу, в т.ч. з використанням Модульного середовища для навчання. При цьому використовуються такі методи поточного контролю:

- оцінювання результатів захисту лабораторних робіт;
- тестовий контроль теоретичного матеріалу.

При виведенні підсумкової семестрової оцінки враховуються результати як поточного, так і підсумкового контролів, який проводиться з усього матеріалу дисципліни за білетами, попередньо розробленими і затвердженими на засіданні кафедри. Здобувач вищої освіти, який набрав з будь-якого виду навчальної роботи, суму балів нижчу за 60 відсотків від максимального балу, ***не допускається*** до семестрового контролю поки не виконає весь обсяг, передбачений Робочою програмою для цього виду роботи. Здобувач вищої освіти, який набрав позитивний середньозважений бал (60 відсотків і більше від максимального балу, встановленого для кожної структурної одиниці) з усіх видів поточного контролю і не склав іспит, вважається таким, який ***має*** академічну заборгованість. Ліквідація академічної заборгованості із семестрового контролю здійснюється у період екзаменаційної сесії або за графіком, встановленим деканатом відповідно до «Положення про контроль і оцінювання результатів навчання здобувачів вищої освіти у ХНУ».

8. ПОЛІТИКА ДИСЦИПЛІНИ

Політика навчальної дисципліни загалом визначається системою вимог до здобувача вищої освіти, що передбачені чинними положеннями Університету про організацію і навчально-методичне забезпечення освітнього процесу. Зокрема, проходження інструктажу з техніки безпеки; відвідування занять з дисципліни є обов'язковим. За об'єктивних причин (підтверджених документально) теоретичне навчання за погодженням із лектором може відбуватись в он-лайн режимі. Успішне опанування дисципліни і формування фахових компетентностей і програмних результатів навчання передбачає необхідність підготовки до лабораторних занять (вивчення теоретичного матеріалу з теми, попередню підготовку протоколу роботи, активно працювати на занятті, якісно підготувати звіт (відповідно до теми роботи), захистити результати виконаної роботи, брати участь у дискусіях щодо прийнятих конструктивних рішень при виконанні здобувачами лабораторних робіт тощо).

Здобувачі вищої освіти зобов'язані дотримуватися термінів виконання усіх видів робіт у встановлені терміни, передбачених робочою програмою навчальної дисципліни. Термін захисту лабораторної роботи вважається своєчасним, якщо здобувач захистив її на наступному після виконання роботи занятті. Пропущене лабораторне заняття здобувач зобов'язаний відпрацювати в лабораторіях кафедри у встановлений викладачем термін, але не пізніше, ніж за два тижні до кінця теоретичних занять у семестрі.

Засвоєння здобувачем теоретичного матеріалу з дисципліни оцінюється за результатами тестування.

Здобувач вищої освіти, виконуючи лабораторні роботи та тестування, має дотримуватися політики доброчесності (заборонені списування, плагіат (в т.ч. із використанням мобільних девайсів)). У разі виявлення плагіату в будь-яких видах навчальної роботи здобувач вищої освіти отримує незадовільну оцінку і має повторно виконати завдання з відповідної теми (виду роботи), що передбачені робочою програмою. Будь-які форми порушення академічної доброчесності ***не допускаються.***

У межах вивчення навчальної дисципліни здобувачам вищої освіти передбачено визнання і зарахування результатів навчання, набутих шляхом неформальної освіти, що розміщені на доступних платформах (за наявності такого переліку, доцільно вказати рекомендовані курси), які сприяють формування компетентностей і поглибленню результатів навчання, визначених робочою програмою дисципліни, або забезпечують вивчення відповідної теми та/або виду робіт з програми навчальної дисципліни (детальніше у Положенні про порядок визнання та зарахування результатів навчання здобувачів вищої освіти у ХНУ).

9. ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ ЗДОБУВАЧІВ ОСВІТИ

Оцінювання академічних досягнень здобувача вищої освіти здійснюється відповідно до «Положення про контроль і оцінювання результатів навчання здобувачів вищої освіти у ХНУ». Залежно від важливості окремих видів навчальної роботи, і їх ролі у формуванні компетентностей і результатів навчання, визначених освітньою програмою, розробники Робочої програми присвоюють кожному виду навчальної роботи (структурній одиниці) з дисципліни певну кількість балів. При поточному оцінюванні виконаної здобувачем роботи з кожної структурної одиниці і отриманих ним результатів викладач виставляє йому певну кількість балів із встановлених Робочою програмою для цього виду роботи. При цьому кожна структурна одиниця навчальної роботи може бути зарахована, якщо здобувач набрав не менше 60 відсотків (мінімальний рівень для позитивної оцінки) від максимально можливої суми балів, призначеної структурній одиниці.

Будь-які форми порушення академічної доброчесності ***не допускаються***.

При оцінюванні результатів навчання здобувачів вищої освіти з будь-якого виду навчальної роботи (структурної одиниці) рекомендується використовувати наведені нижче узагальнені критерії:

Таблиця – Критерії оцінювання навчальних досягнень здобувача вищої освіти

Оцінка та рівень досягнення здобувачем запланованих ПРН та сформованих компетентностей	Узагальнений зміст критерія оцінювання
Відмінно (високий)	Здобувач вищої освіти глибоко і у повному обсязі опанував зміст навчального матеріалу, легко в ньому орієнтується і вміло використовує понятійний апарат; уміє пов'язувати теорію з практикою, вирішувати практичні завдання, впевнено висловлювати і обґрунтовувати свої судження. Відмінна оцінка передбачає логічний виклад відповіді мовою викладання (в усній або у письмовій формі), демонструє якісне оформлення роботи і володіння спеціальними приладами та інструментами, прикладними програмами. Здобувач не вагається при видозміні запитання, вміє робити детальні та узагальнюючі висновки, демонструє практичні навички з вирішення фахових завдань. При відповіді допустив дві–три несуттєві ***похибки***.
Добре (середній)	Здобувач вищої освіти виявив повне засвоєння навчального матеріалу, володіє понятійним апаратом, орієнтується у вивченому матеріалі; свідомо використовує теоретичні знання для вирішення практичних задач; виклад відповіді грамотний, але у змісті і формі відповіді можуть мати місце окремі неточності, нечіткі формулювання правил, закономірностей тощо. Відповідь здобувача вищої освіти будується на основі самостійного мислення. Здобувач вищої освіти у відповіді допустив дві–три ***несуттєві помилки***.
Задовільно (достатній)	Здобувач вищої освіти виявив знання основного програмного матеріалу в обсязі, необхідному для подальшого навчання та практичної діяльності за професією, справляється з виконанням практичних завдань, передбачених програмою. Як правило, відповідь здобувача вищої освіти будується на рівні репродуктивного мислення, здобувач вищої освіти має слабкі знання структури навчальної дисципліни, допускає неточності і ***суттєві помилки*** у відповіді, вагається при відповіді на видозмінене запитання. Разом з тим, набув навичок, необхідних для виконання нескладних практичних завдань, які відповідають мінімальним критеріям оцінювання і володіє знаннями, що дозволяють йому під керівництвом викладача усунути неточності у відповіді.
Незадовільно (недостатній)	Здобувач вищої освіти виявив розрізнені, безсистемні знання, не вміє виділяти головне і другорядне, допускається помилок у визначенні понять, перекручує їх зміст, хаотично і невпевнено викладає матеріал, не може використовувати знання при вирішенні практичних завдань. Як правило, оцінка «незадовільно» виставляється здобувачеві вищої освіти, який не може продовжити навчання без додаткової роботи з вивчення навчальної дисципліни.

Структурування дисципліни за видами навчальної роботи і оцінювання результатів навчання здобувачів у І семестрі

Аудиторна робота								Контрольні заходи	Семестровий контроль	
Лабораторні роботи №:								Тестовий контроль:	Іспит	Разом балів
1	2	3	4	5	6	7	8	Т 1-2		
Кількість балів за вид навчальної роботи (мінімум-максимум)										
3-5	3-5	3-5	3-5	3-5	3-5	3-5	3-5	12-20	24-40	**60-100***
24-40								**12-20**	**24-40**	

Примітки: Т – тема навчальної дисципліни.

Структурування дисципліни за видами навчальної роботи і оцінювання результатів навчання здобувачів у ІІ семестрі

Аудиторна робота								Контрольні заходи	Семестровий контроль	
Лабораторні роботи №:								Тестовий контроль:	Іспит	Разом балів
1	2	3	4	5	6	7	8	Т 1-2		
Кількість балів за вид навчальної роботи (мінімум-максимум)										
3-5	3-5	3-5	3-5	3-5	3-5	3-5	3-5	12-20	24-40	**60-100***
24-40								**12-20**	**24-40**	

Примітки: Т – тема навчальної дисципліни;

[*]За набрану з будь-якого виду навчальної роботи з дисципліни кількість балів, нижче встановленого мінімуму, здобувач отримує незадовільну оцінку і має її перездати у встановлений викладачем (деканом) термін. Інституційна оцінка встановлюється відповідно до таблиці «**Співвідношення інституційної шкали оцінювання і шкали оцінювання ЄКТС»**.

Оцінювання результатів захисту лабораторної роботи

Виконана й оформлена відповідно до встановлених Методичними рекомендаціями вимог лабораторна робота комплексно оцінюється викладачем при її захисті з урахуванням таких критеріїв: самостійність та правильність виконання; якість оформлення звіту; вільне володіння здобувачем спеціальною термінологією і уміння професійно обґрунтувати прийняті конструктивні рішення.

Результат виконання і захисту здобувачем вищої освіти кожної лабораторної роботи оцінюється відповідно до таблиці Критеріїв оцінювання навчальних досягнень здобувача вищої освіти та рівня досягнення здобувачем запланованих ПРН та сформованих компетентностей з присвоєнням йому відповідної суми балів.

У випадку виявлення здобувачем рівня знань, нижчого ніж 60 відсотків від максимального балу, встановленого Робочою програмою для кожної структурної одиниці, лабораторна робота йому ***не зараховується*** і для її захисту він має детальніше опрацювати матеріал з теми роботи, методику її виконання, виправити грубі помилки та повторно вийти на її захист у призначений для цього викладачем час.

Оцінювання результатів навчання з теоретичного матеріалу

Тест, передбачений Робочою програмою, складається із 20 тестових завдань, кожне з яких є рівнозначним. Максимальна сума балів, яку може набрати здобувач, складає 20.

Відповідно до таблиці структурування видів робіт за тематичний контроль здобувач залежно від кількості правильних відповідей може отримати від 12 до 20 балів.

Розподіл балів в залежності від наданих правильних відповідей на тестові завдання

Кількість правильних відповідей	0-11	12	13	14	15	16	17	18	19	20
Відсоток правильних відповідей	0-59	60-65		66-72	73-82		83-89	90-100		
Кількість балів	-	12	13	14	15	16	17	18	19	20

На тестування відводиться 20 хвилин. Правильні відповіді записуються у талоні відповідей. Здобувач може також пройти тестування і в он-лайн режимі у Модульному середовищі для навчання. При отриманні негативної оцінки тест слід перездати до терміну ***наступного*** контролю.

Оцінювання результатів підсумкового семестрового контролю (іспит)

Освітня програма передбачає підсумковий семестровий контроль з дисципліни у формі іспиту, завданням якого є системне й об'єктивне оцінювання підготовки здобувача з навчальної дисципліни. Складання іспиту відбувається за попередньо розробленими і затвердженими на засіданні кафедри білетами.

Таблиця – Оцінювання результатів підсумкового семестрового контролю здобувачів вищої освіти (40 балів для підсумкового контролю)

Види завдань	**Для кожного окремого виду завдань**		
	Мінімальний (достатній) бал (задовільно)	**Потенційні позитивні бали[*] (середній бал) (добре)**	**Максимальний (високий) бал (відмінно)**
Питання № 1	12	16	20
Питання № 2	12	16	20
Разом:	**24**		**40**

<u>Примітка</u>. [*]Позитивний бал за іспит, відмінний від мінімального (24 бали) та максимального (40 балів), знаходиться в межах 25-39 балів та розраховується як сума балів за усі структурні елементи (завдання) іспиту.

Для кожного окремого виду завдань підсумкового семестрового контролю застосовуються критерії оцінювання навчальних досягнень здобувача вищої освіти, наведені вище (**Таблиця – Критерії оцінювання навчальних досягнень здобувача вищої освіти)**.

Таблиця – Співвідношення інституційної шкали оцінювання і шкали оцінювання ЄКТС

<table>
<tr><th rowspan="2">Оцінка ЄКТС</th><th rowspan="2">Рейтингова шкала балів</th><th colspan="2">Інституційна шкала (Опис рівня досягнення здобувачем вищої освіти запланованих результатів навчання з навчальної дисципліни</th></tr>
<tr><th>Залік</th><th>Іспит/диференційований залік</th></tr>
<tr><td>A</td><td>90-100</td><td rowspan="5">Зараховано</td><td>Відмінно/Excellent – високий рівень досягнення запланованих результатів навчання з навчальної дисципліни, що свідчить про безумовну готовність здобувача до подальшого навчання та/або професійної діяльності за фахом</td></tr>
<tr><td>B</td><td>83-89</td><td rowspan="2">Добре/Good – середній (максимально достатній) рівень досягнення запланованих результатів навчання з навчальної дисципліни та готовності до подальшого навчання та/або професійної діяльності за фахом</td></tr>
<tr><td>C</td><td>73-82</td></tr>
<tr><td>D</td><td>66-72</td><td rowspan="2">Задовільно/Satisfactory – Наявні мінімально достатні для подальшого навчання та/або професійної діяльності за фахом результати навчання з навчальної дисципліни</td></tr>
<tr><td>E</td><td>60-65</td></tr>
<tr><td>FX</td><td>40-59</td><td rowspan="2">Незараховано</td><td>Незадовільно/Fail – Низка запланованих результатів навчання з навчальної дисципліни відсутня. Рівень набутих результатів навчання є недостатнім для подальшого навчання та/або професійної діяльності за фахом</td></tr>
<tr><td>F</td><td>0-39</td><td>Незадовільно/Fail – Результати навчання відсутні</td></tr>
</table>

Підсумкова семестрова оцінка за інституційною шкалою і шкалою ЄКТС визначається в автоматизованому режимі після внесення викладачем результатів оцінювання з усіх видів робіт до електронного журналу. Співвідношення інституційної шкали оцінювання і шкали оцінювання ЄКТС у наведеній вище таблиці.

Семестровий іспит виставляється, якщо загальна сума балів, яку набрав здобувач з дисципліни за результатами поточного та підсумкового контролю, знаходиться у межах від 60 до 100 балів. При цьому за інституційною шкалою ставиться оцінка «відмінно/добре/задовільно», а за шкалою ЄКТС – буквене позначення оцінки, що відповідає набраній здобувачем сумі балів відповідно до таблиці Співвідношення.

10. ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ РЕЗУЛЬТАТІВ НАВЧАННЯ

1. Підходи до виявлення вразливостей.
2. Підходи до оцінювання безпеки інформаційних систем.
3. Методологія організації атак на інформаційну безпеку.
4. Методика оцінювання безпеки брандмауера.
5. Методика оцінювання безпеки маршрутизатора.
6. Методика оцінювання безпеки комутатора.
7. Методика оцінювання безпеки систем виявлення вторгнень.
8. OSINT через Всесвітню павутину (WWW)
9. Аналіз веб-сайтів
10. DNS-опитування.
11. Автоматизація роботи з OSINT за допомогою інструментів/фреймворків/скриптів.
12. Інформація зовнішньої мережі, розвідка, сканування вразливостей.
13. Внутрішня мережна інформаційна розвідка, сканування вразливостей.
14. Дослідження вразливостей локальної системи.
15. Дослідження вразливостей віддаленої системи.
16. Дослідження вразливостей WLAN.
17. Процес аналізу трафіка WLAN.

18. Методологія проведення атаки на WLAN.
19. Атаки на Bluetooth.
20. Дослідження вразливостей IoT.
21. Дослідження вразливостей OT/SCADA.
22. Проблеми безпеки в IoT.
23. Проблеми безпеки OT/SCADA.
24. Поверхня атаки і пов’язані загрози.
25. Спеціальні методики виявлення вразливостей IoT.
26. Спеціальні методики виявлення вразливостей OT/SCADA.
27. Дослідження вразливостей хмари.
28. Обмеження хмарних архітектур з точки зору інформаційної безпеки.
29. Спеціальні методики виявлення вразливостей хмари.
30. Принципи та підходи бінарного аналізу програмного забезпечення.
31. Інструментарій бінарного аналізу.
32. Дослідження вразливостей програмного забезпечення.
33. Безпека та тестування на проникнення.
34. Види тестування на проникнення.
35. Цілі тестування на проникнення.
36. Класифікація тестування на проникнення.
37. Юридичні причини тестування на проникнення.
38. Правові рамки тестування на проникнення.
39. Важливі умови договору між тестером на проникнення та клієнтом.
40. Організаційні вимоги до тестування на проникнення.
41. Вимоги до персоналу.
42. Технічні вимоги тестування на проникнення.
43. Етичні питання тестування на проникнення.
44. Вимоги до методики випробування на проникнення.
45. П'ять фаз тесту на проникнення.
46. Етап підготовки тестування.
47. Етап розвідки.
48. Етап аналізу інформації/ризиків.
49. Етап активних спроб вторгнення.
50. Етап остаточного аналізу.
51. Етап написання звітів.
52. Принципи створення захищених ОС.
53. Розробка захищених ОС “з нуля”.
54. Побудова “довірених” версій шляхом модернізації існуючих ОС.
55. Визначення вимог до архітектури комплексу засобів захисту в залежності від задач, які виконує ОС.
56. Адміністративні заходи захисту ОС.
57. Принципи організації безпеки мережної інфраструктури.
58. Моделі управління мережними ресурсами.
59. Безпека міжмережної взаємодії.
60. Технології побудови захищених корпоративних мереж.
61. Проєктування мереж, включаючи розуміння цілей безпеки, операційних цілей та компромісів між ними.
62. Переваги та недоліки застосування технологій Sandboxing у мережній інфраструктурі.
63. Переваги та недоліки застосування технологій Honeypots та Honeynets у мережній інфраструктурі.
64. Переваги та недоліки застосування технологій Deception у мережній інфраструктурі.
65. Підвищення мережної безпеки за рахунок впровадження Honeynet- та Deception-технологій.
66. Аналіз недоліків систем DLP.

67. Методи для підвищення ефективності та законності DLP-систем.
68. Особливості проєктування систем DLP.
69. Архітектура, функціонування та механізми безпеки веб-додатків і веб-серверів.
70. Взаємодія між веб-сервісами як елемент інформаційної безпеки.
71. REST-інтерфейс та його безпека.
72. Особливості застосування баз даних для побудови захищених веб-рішень
73. Відкритий проект по забезпеченню безпеки веб-додатків (OWASP).
74. Перспективи організації та виконання тестування рівня безпеки для певного веб-ресурсу.
75. Аналіз існуючих підходів до вирішення задач аутентифікації
76. Біометрична аутентифікація на основі розпізнавання зображень (штучні нейронні та капсульні мережі, алгоритм розпізнавання облич Eigenface та його реалізація).
77. Визначення вимог до СКУД відповідно до політики інформаційної безпеки. Обґрунтування моделі управління доступом.
78. Концепція та етапи створення СКУД. Розробка технічного завдання, проєктування, дослідна експлуатація, супровід.
79. Ідентифікація та дослідження каналів витоку інформації.
80. Організаційно-технічні заходи щодо блокування каналів витоку інформації на об'єкті.
81. Проєктування систем захисту від витоку інформації.
82. Визначення інформації, що потребує захисту на об'єктах критичної інфраструктури (ОКІ).
83. Канали витоку інформації на ОКІ та підстави їх утворення.
84. Засоби та комплекси виявлення прихованого підключення до інформаційних мереж.
85. Види прихованого підключення до інформаційних мереж (радіозакладні пристрої, приховане під'єднання до ліній зв'язку, приховані відеокамери, прихований майнінг тощо).
86. Порядок проведення обстеження і аналізу ОКІ з метою забезпечення захисту інформації.
87. Робота з документами та документованою інформацією.
88. Організація розробки і використання документів та носіїв конфіденційної інформації.
89. Облік документів та документованої інформації.
90. Виконання та повернення документів та документованої інформації.
91. Зберігання і знищення документів та документованої інформації.
92. Використання технічних засобів збору, обробки, накопичення і зберігання конфіденційної інформації.
93. Підбір та розстановка персоналу.
94. Навчання персоналу.
95. Контроль за роботою персоналу.
96. Відповідальність за порушення правил захисту інформації.

11. МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ

Навчальний процес з дисципліни повністю і в достатній кількості забезпечений необхідною навчально-методичною літературою, яка розміщена в модульному середовищі для навчання: I семестр – https://msn.khmnu.edu.ua/course/view.php?id=8037; II семестр – https://msn.khmnu.edu.ua/course/view.php?id=7862.

12. МАТЕРІАЛЬНО-ТЕХНІЧНЕ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ

Інформаційна та комп'ютерна підтримка: ПК, ноутбук, планшет, смартфон або інший мобільний пристрій, проєктор, доступ до мережі Інтернет, робота з презентаціями.

Спеціальне та прикладне програмне забезпечення: OS Kali Linux, OS Ubuntu, OS MS Windows 10 або вище, OS FreeBSD, Oracle Virtual Box, Cisco Packet Tracer, Honeyd, Metasploit,

YARA, MS Visual Studio 19 або вище, MS Visio 2019 або вище, Web Application Firewall, OpenCV Eigenfaces тощо.

Спеціальне апаратне забезпечення: маршрутизатори Cisco S4400, комутатори C2960, міжмережні екрани Cisco ASA/CISCO Fortinet та інше мережеве обладнання, генератор шумових сигналів МАРС-ТЗО-4-2, вібровипромінювач ВИ-4, вібровипромінювач ВИ-3, колонка акустична захищена МАРС-АКЗ, колонка акустична МАРС-АК, камери відеоспостереження HikVision, комплект обладнання для систем контролю і управління доступом ZKTeco, пристрій захисту від ПЕМВ «Базальт-5ГЕШ», генератор перешкод "СКОРПІОН PRO".

13. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

1. Тестування на проникнення: навч. посіб. Ч.1/ Є.О. Живило. П.: ПНТУ “Полтавська політехніка ім. Юрія Кондратюка”, 2024. 134 с.
2. Тестування на проникнення: навч. посіб. Ч.2/ Є.О. Живило. П.: ПНТУ “Полтавська політехніка ім. Юрія Кондратюка”, 2024. 239 с.
3. OSINT у кібербезпеці: навч. пос./ Ланде Д.В. Київ: ТОВ «Інжиніринг», 2024. 522 с.
4. Комплексна безпека інформаційних мережевих систем: навчальний посібник/ Укладачі: А.Г. Микитишин, М.М. Митник, О.С. Голотенко, В.В. Карташов. Тернопіль: ФОП Паляниця В.А., 2023. 324 с.
5. Організація баз даних: навчальний посібник/ Я.І. Соколовський, М.В. Дендюк, І.М. Крошний, І.Б.Пірко, М.М. Паславський. Видавництво Wydawnictwo GSW, 2023. 466 с.
6. Технічний захист інформації: теоретичні основи та організаційно-технічне забезпечення. Навч. посіб./ В.М.Богуш, В. Д. Бровко, О.С.Кобус, В.Д. Козюра. Київ: Видавництво Ліра-К, 2023. 508 с.

Додаткова

7. Penetration Testing For Dummies/ Robert Shimonski. John Wiley & Sons, Inc., Hoboken, New Jersey. 2020. 334 p.
8. Practical Binary Analysis/ Dennis Andriesse. San Francisco. 2020. 493 p.
9. OWASP Top 10 API Security Risks – 2023 [Електронний ресурс]. Режим доступу: https://surl.li/esffdo
10. Web Application Security Testing v4.2 [Електронний ресурс]. Режим доступу: https://surl.li/mjbsxb
11. A Guide to Penetration Testing [Електронний ресурс]. Режим доступу: https://surl.li/uoqvpd
12. Penetration Testing Execution Standard (PTES) [Електронний ресурс]. Режим доступу: http://www.pentest-standard.org/
13. NIST Technical Guide to Information Security Testing [Електронний ресурс]. Режим доступу: https://surl.li/hzlwdh
14. Пентест від А до Я: посібник з тестування на проникнення [Електронний ресурс]. Режим доступу: https://surl.li/vjvbgr
15. Maltego Handbook for Cyber Threat Intelligence [Електронний ресурс]. Режим доступу: https://surl.li/vzafzr
16. OSINT Академія [Електронний ресурс]. Режим доступу: https://surl.li/qufgzc
17. Kali Docs [Електронний ресурс]. Режим доступу: https://www.kali.org/docs/
18. Kali Tools [Електронний ресурс]. Режим доступу: https://www.kali.org/tools/
19. Metasploit Documentation [Електронний ресурс]. Режим доступу: https://docs.metasploit.com
20. Посібники про Honeypot. Від А до Я [Електронний ресурс]. Режим доступу: https://surl.li/oaizik
21. Приманки для лову хакерів (Комплексні системи розгортання приманок) [Електронний ресурс]. Режим доступу: https://surl.li/zxtiyg
22. ДСТУ 3396.1-96 Захист інформації. Технічний захист інформації. Порядок проведення

робіт.
23. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в КС від НСД.
24. YARA's documentation [Електронний ресурс]. Режим доступу: https://yara.readthedocs.io/en/stable/
25. Система контролю та управління доступом на основі RFID-технологій/ Віра ТІТОВА, Юрій КЛЬОЦ, Вадим КОЛІСНИК, Віталій ВОЛИНЕЦЬ//MEASURING AND COMPUTING DEVICES IN TECHNOLOGICAL PROCESSES. №2. 2023. С. 384-388
26. Підвищення функціональності і стабільності завадостійких безпроводових інформаційно–комунікаційних систем/ В.М. Джулій, Ю.П. Кльоц, В.С. Орленко, В.Ю. Тітова, Ю.В. Хмельницький // Вісник Хмельницького національного університету, 2021. №1. С. 12-16
27. Контроль додатків інтернет-трафіка комп'ютерних мереж методами машинного навчання/ В.М. Джулій, Ю.П. Кльоц, І.В. Муляр, М.Л. Жилевич, А.В. Джулій// Вісник Хмельницького національного університету, 2021. №51. С. 22-26
28. Модель нелегітимного абонента забезпечення безпеки ip-телефонії/ О.С. Андрощук, В.М. Джулій, Ю.П. Кльоц, І.В. Муляр// MEASURING AND COMPUTING DEVICES IN TECHNOLOGICAL PROCESSES. №2. 2020. С. 39-45
29. Система виявлення аномалій У DNS-запитах/ Ю КЛЬОЦ, С МОСТОВИЙ, П СІКОРСЬКИЙ, І ОСТАПЧУК//Herald of Khmelnytskyi National University. Technical sciences Т. 345. Випуск 6 (2). С. 141-148
30. A model of a DDoS attack scenario on elements of specialized information technology and methods of combating cybercriminals./ M Stetsyuk, V Cheshun, Y Stetsyuk, leksandr Kozelskiy, ABM Salem// IntelITSIS, 2024 P. 260-269
31. Алгоритми прогнозування вразливостей та загроз інформаційної безпеки на основі тематичних інтернет-ресурсів/ Є Майор, В Джулій, В Чешун, Н ПЕТЛЯК// Measuring and computing devices in technological processes, 2023. С. 49-56
32. Використання інформаційних технологій для підвищення якості роботи та безпеки телекомунікаційних мереж/ Ю. Хмельницький, В. Чешун, А. Джулій, В. Чорненький//MEASURING AND COMPUTING DEVICES IN TECHNOLOGICAL PROCESSES. №2. 2022. С. 39-45
33. Імовірнісні алгоритми та методи забезпечення безпеки IP-телефонії/ В Джулій, В Чешун, А Джулій, В Чорненький// MEASURING AND COMPUTING DEVICES IN TECHNOLOGICAL PROCESSES. №1. 2021. С. 133-138
34. Удосконалення систем захисту інформації в комп'ютерних мережах державної прикордонної служби України/ Олександр Андрощук, Олександр Коваленко, Віра Тітова, Віктор Чешун, Андрій Поляков// Збірник наукових праць Національної академії Державної прикордонної служби України. Серія: військові та технічні науки, 2021. Том 85. Випуск 2-3. С. 5-21
35. Розроблення політики інформаційної безпеки приватного підприємства/ В. Тітова, Ю. Кльоц, В. Волинець, Н. Петляк, М. Огородник// Measuring and computing devices in technological processes, 2024. С. 79-83

14. ІНФОРМАЦІЙНІ РЕСУРСИ

1. Модульне середовище для навчання. URL :
   https://msn.khmnu.edu.ua/course/view.php?id=8037
   https://msn.khmnu.edu.ua/course/view.php?id=7862
2. Електронна бібліотека ХНУ. URL: http://lib.khmnu.edu.ua/
3. Інституційний репозитарій ХНУ. URL : https://library.khmnu.edu.ua/

ТЕОРІЯ ПРОЄКТУВАННЯ ТА ТЕСТУВАННЯ БЕЗПЕКИ ЗАХИЩЕНИХ СИСТЕМ

Тип дисципліни	Обов'язкова
Рівень вищої освіти	Другий (магістерський)
Мова викладання	Українська
Семестр	Перший, другий
Кількість встановлених кредитів ЄКТС	9
Форми здобуття освіти, для яких викладається дисципліна	Очна (денна)

Результати навчання. Здобувач, який успішно завершив вивчення дисципліни, повинен: вільно *володіти* державною мовою для представлення практичної діяльності та обговорення питань аналізу вразливостей, тестування на проникнення, технічного й організаційного захисту інформації, мережевої безпеки; *обґрунтовувати* та *доносити* висновки, знання та пояснення; *планувати* навчання, *супроводжувати* та *контролювати* персонал; *розробляти*, *впроваджувати*, *удосконалювати* ІТ у сфері безпеки; *проводити* дослідження, *реалізовувати* проєкти, *впроваджувати* стандарти та практики; *аналізувати* та *забезпечувати* управління доступом; *розробляти* та *оцінювати* методи захисту; *забезпечувати* безперервність процесів; *приймати* рішення, обґрунтовувати вибір ПЗ та інструментів; *адаптувати* методи тестування, *розробляти* сценарії, *класифікувати* вразливості, *демонструвати* їх використання; *забезпечувати* конфіденційність, цілісність, доступність, *адмініструвати* мережі та *проєктувати* їх з урахуванням цілей безпеки.

Зміст навчальної дисципліни. Проєктування та розробка захищених операційних систем. Концепції та методологія безпеки мережної інфраструктури. Технології Honeypot та Deception, DLP-системи. Проєктування та розробка захищених веб-ресурсів. Аутентифікація і системи контролю та управління доступом. Методи та засоби захисту від витоку інформації. Захист інформації на об'єктах критичної інфраструктури. Організація режиму та охорони, робота з персоналом. Методи тестування безпеки систем. Розвідка на основі відкритих джерел (OSINT). Аналіз вразливостей та тестування на проникнення комп'ютерних мереж. Аналіз вразливостей та тестування на проникнення бездротових мереж, Інтернету речей, OT/SCADA та хмарних технологій. Аналіз вразливостей веб-ресурсів. Бінарний аналіз вразливостей програмного забезпечення. Підходи до тестування на проникнення та юридичні аспекти. Організаційне забезпечення тестування на проникнення. Методика та документаційне забезпечення тестування на проникнення.

Пререквізити – вихідна, моніторинг та менеджмент інформаційної безпеки.

Постреквізити – моніторинг та менеджмент інформаційної безпеки, переддипломна практика, кваліфікаційна робота.

Запланована навчальна діяльність: Мінімальний обсяг навчальних занять в одному кредиті ЄКТС навчальної дисципліни для другого (магістерського) рівня вищої освіти за денною формою здобуття освіти становить 8 годин на 1 кредит ЄКТС.

Форми (методи) навчання: лекції (з використанням словесних, наочних та проблемних методів з супроводом презентаційних матеріалів); лабораторні роботи (з використанням практичних, частково-пошукових та ігрових методів, із застосуванням сучасних інформаційно-комп'ютерних технологій); самостійна робота (з використанням пояснювально-ілюстративних та дослідницьких методів).

Форми оцінювання результатів навчання: оцінювання результатів захисту лабораторних робіт; тестовий контроль теоретичного матеріалу.

Вид семестрового контролю: іспит – 1,2 семестр.

Навчальні ресурси:

1. Тестування на проникнення: навч. посіб. Ч.1/ Є.О. Живило. П.: ПНТУ “Полтавська політехніка ім. Юрія Кондратюка”, 2024. 134 с.
2. Тестування на проникнення: навч. посіб. Ч.2/ Є.О. Живило. П.: ПНТУ “Полтавська політехніка ім. Юрія Кондратюка”, 2024. 239 с.
3. OSINT у кібербезпеці: навч. пос./ Ланде Д.В. Київ: ТОВ «Інжиніринг», 2024. 522 с.
4. Комплексна безпека інформаційних мережевих систем: навчальний посібник/ Укладачі: А.Г. Микитишин, М.М. Митник, О.С. Голотенко, В.В. Карташов. Тернопіль: ФОП Паляниця В.А., 2023. 324 с.
5. Організація баз даних: навчальний посібник/ Я.І. Соколовський, М.В. Дендюк, І.М. Крошний, І.Б.Пірко, М.М. Паславський. Видавництво Wydawnictwo GSW, 2023. 466 с.
6. Технічний захист інформації: теоретичні основи та організаційно-технічне забезпечення. Навч. посіб./ В.М.Богуш, В. Д. Бровко, О.С.Кобус, В.Д. Козюра. Київ: Видавництво Ліра-К, 2023. 508 с.
7. Модульне середовище для навчання. Доступ до ресурсу: https://msn.khmnu.edu.ua/course/view.php?id=8037 https://msn.khmnu.edu.ua/course/view.php?id=7862
8. Електронна бібліотека ХНУ. Доступ до ресурсу: http://lib.khmnu.edu.ua

Викладачі: канд. техн. наук, доц. Чешун В.М., канд. техн. наук, доц. Кльоц Ю.П.