ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

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

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Моніторинг та менеджмент інформаційної безпеки
Назва дисципліни

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.02
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**	**34**	**18**		**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. Віра ТІТОВА
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 «Моніторинг та менеджмент інформаційної безпеки» 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, теорія проєктування та тестування безпеки захищених систем.

Постреквізити – теорія проєктування та тестування безпеки захищених систем, 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. ФК04. Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог. 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. ФК07. 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. ФК09. 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. 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. УК01. Здатність виявляти вторгнення на базі хоста та мережі за допомогою технологій виявлення вторгнень, характеризувати та аналізувати мережевий трафік для виявлення аномальної активності, шкідливих дій, потенційних загроз мережевим ресурсам, слабких місць, методів експлуатації, впливу на систему та інформацію, збирати та аналізувати артефакти вторгнення.

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. ПРН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах. ПРН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки. ПРН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення. 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. ПРН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки. 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. ПРН12. 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. ПРН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому. 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. ПРН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки. 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. ПРН24. Виявляти вторгнення на базі хоста та мережі за допомогою технологій виявлення вторгнень, характеризувати та аналізувати мережевий трафік для виявлення аномальної активності, шкідливих дій, потенційних загроз мережевим ресурсам, слабких місць, методів експлуатації, впливу на систему та інформацію, збирати та аналізувати артефакти вторгнення.

Мета дисципліни. Формування у здобувачів системних знань і практичних навичок з аудиту, моніторингу та менеджменту інформаційної безпеки у комп'ютерних та інформаційно-комунікаційних системах і управління інцидентами та ризиками інформаційної та/або кібербезпеки в умовах широкого використання сучасних інформаційних технологій.

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; інформаційні ресурси різних класів (в т.ч. державні інформаційні ресурси); програмне та програмно-апаратне забезпечення (засоби) кіберзахисту; системи управління

інформаційною безпекою та/або кібербезпекою; технології, методи, моделі та засоби інформаційної безпеки та/або кібербезпеки; системи та комплекси створення, обробки, передачі, зберігання, знищення, захисту та відображення даних (інформаційних потоків).

Завдання дисципліни. Формування у майбутніх спеціалістів умінь, навичок та компетентностей для забезпечення аудиту, моніторингу та менеджменту інформаційної безпеки у комп'ютерних та інформаційно-комунікаційних системах і для управління інцидентами та ризиками інформаційної та/або кібербезпеки, в тому числі з використанням прикладного та спеціалізованого програмного та апаратного забезпечення.

Результати навчання. Здобувач, який успішно завершив вивчення дисципліни, повинен: вільно *спілкуватися* державною мовою для представлення результатів та обговорення питань аналізу, моніторингу, аудиту, менеджменту та реагування на інциденти ІБ; *планувати* навчання, *координувати* персонал у сфері соціотехнічної безпеки; чітко *доносити* висновки, *інтегрувати* теорію ризиків, *застосовувати* сучасні математичні моделі для оцінювання захищеності систем; *впроваджувати* світові стандарти, *досліджувати* та *супроводжувати* засоби ІБ, *управляти* проєктами з реагування на інциденти, *аналізувати* нормативні документи, *застосовувати* моделювання, *обґрунтовувати* вибір технічних засобів; *приймати* рішення в умовах невизначеності, *будувати* системи управління ІБ, *забезпечувати* безперервність бізнес-процесів, *виявляти* загрози, *аналізувати* трафік, артефакти, типи атак, *здійснювати* управління інцидентами, розслідування, аудит та оцінювання ефективності ІБ.

4. СТРУКТУРА ЗАЛІКОВИХ КРЕДИТІВ ДИСЦИПЛІНИ

I семестр

Назва теми	**Кількість годин відведених на:**		
	лекції	**лабораторні роботи**	**СРС**
Тема 1. Моніторинг інформаційної безпеки	6	24	48
Тема 2. Тактики, прийоми і процедури протидії кіберінцидентам	10	10	52
Разом:	**16**	**34**	**100**

II семестр

Назва теми	**Кількість годин відведених на:**		
	лекції	**практичні заняття**	**СРС**
Тема 1. Менеджмент та аудит інформаційної безпеки	8	8	40
Тема 2. Моделювання та оцінювання захищеності систем	8	10	46
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. Моніторинг інформаційної безпеки		**6**
1	**Методології та прийоми виявлення атак/вторгнень** Аналіз джерел даних для систем виявлення атак/вторгнень. Дослідження ознак атак/вторгнень. Методи їх виявлення. Інтеграція засобів виявлення і запобігання атак/вторгнень в єдину систему. Прогнозування результатів атак/вторгнень. Літ.: [1] с. 20-28, 206-227; [28]; [29]	2
2	**Особливості організації моніторингу інформаційно-комунікаційних систем та їх компонентів** Моніторинг файлової системи, процесів та журналів операційних систем. Моніторинг хостів. Моніторинг мережевої архітектури. Мережеві протоколи Netflow та SFlow. Passive DNS. Автоматизація моніторингу за допомогою скриптів. Літ.: [1] с. 166-206; [2] с. 154-205	2
3	**Особливості розробки та супроводу системи моніторингу на об'єктах інформаційної діяльності** Проєктування, впровадження та супровід систем моніторингу. Підходи до збору інформації про події з різних пристроїв забезпечення інформаційної безпеки і мережевих пристроїв, аналіз поведінки користувачів. Аутсорсинг інформаційної безпеки, як інструмент моніторингу, його переваги, недоліки та ризики. Структура звітності постачальника послуг кіберзахисту. Оцінювання надійності постачальника та/або продукту. Літ.: [1] с. 166-206; [2] с. 154-205; [28]; [29]	2
Тема 2. Тактики, прийоми і процедури протидії кіберінцидентам		**10**
4	**Аналіз кіберінцидентів** Класифікація кіберінцидентів відповідно до міжнародних стандартів та рекомендацій. Модель PDCA опису життєвого циклу процесів кіберінцидентів. Етапи управління інцидентами відповідно до ISO/IEC 27035. Особливості менеджменту інцидентів відповідно до ITIL. Концепція та структура автоматизованої системи управління інцидентами. Літ.: [14]; [15]	2
5	**Методологія реагування на інциденти та їх обробки** Особливості організації та функціонування команд (груп) CERT/CSIRT. Механізми реагування на інциденти. Підходи до розслідування інцидентів та їх обробки. Літ.: [14]; [15]	2
6	**Соціотехнічна безпека** Методи соціального інжинірингу. Основні алгоритми соціотехнічних атак на інформаційні ресурси, етапи їх проведення. Рекомендації щодо захисту від соціотехнічних атак. Менеджмент та навчання персоналу у сфері соціотехнічної безпеки. Літ.: [4] с. 127-267	2
7	**Планування безперервності роботи** Операційні впливи за недостатності заходів з кібербезпеки. Планування безперервності роботи бізнес/операційних процесів. Розробка відмовостійкого кластеру (вимоги до структури, принципи проєктування, дослідження надійності вузлів, алгоритми відновлення при відмовах та кіберінцидентах). Літ.: [14]; [15]	2
8	**Аналіз розвідувальних даних щодо кіберзагроз та кіберінцидентів (CTI)** Особливості процесу розвідувальної роботи з точки зору інформаційної та кібербезпеки. Джерела поширення інформації про вразливості (попередження, рекомендації, помилки та бюлетені). Формування вимог	2

	та розробка аналітичного плану. Дослідження етапів проведення аналізу (збір даних, обробка, поширення інформації). Інтеграція розвідувальної роботи в управління кіберінцидентами. Літ.: [14]; [15]	
	Разом за семестр:	**16**

Перелік лекцій (II семестр)

Номер лекції	Перелік тем лекцій, їх анотація	Години
Тема 1. Менеджмент та аудит інформаційної безпеки		**8**
1	**Аналіз загроз безпеки** Аналіз загроз інформаційної безпеки на об'єктах інформаційної діяльності. Особливості формування концепції і політики інформаційної безпеки на основі аналізу загроз. Оцінювання політики безпеки на відповідність стандартам. Літ.: [11]; [25]; [27]	2
2	**Ризик-менеджмент інформаційної безпеки** Процеси управління ризиками згідно NIST 800-30 та ISO 27005. Процеси розробки контрзаходів для виявлених ризиків безпеки. Методика, технології та сучасні інструментальні засоби аналізу ризиків. Літ.: [6]; [7]	2
3	**Управління інформаційною безпекою** Концепції в управлінні безпекою (Release Management, Patch Management, ISO 27xxx). Розробка системи менеджменту інформаційної безпеки (СМІБ). Формування правил, положень та функцій технологічного управління безпекою організації. Літ.: [3] с. 177-201; [8]; [9]; [10]	2
4	**Внутрішній та комплексний аудит інформаційної безпеки** Принципи проведення внутрішнього аудиту. Управління програмою аудиту. Аудит інформаційної безпеки на основі аналізу ризиків. Компетентність аудиторів та особливості її оцінювання. Основні етапи комплексного аудиту безпеки інформаційних систем. Оцінка діяльності з управління інформаційною безпекою організації. Удосконалення інформаційної безпеки організації за допомогою передачі та страхування ризиків. Літ.: [1] с. 210-251; [24]	2
Тема 2. Моделювання та оцінювання захищеності систем		**8**
5	**Моделіювання систем та засобів кіберзахисту** Моделі аналізу, синтезу та управління систем захисту інформації. Системний підхід в моделях захисту інформації, ідентифікація системи і процесу. Оцінювання повноти та достовірності вихідних даних при моделюванні систем і засобів кіберзахисту. Особливості застосування граф-моделей (дерева атак і контрзаходів, графи шляхів реалізації атаки, графи загроз тощо). Літ.: [11]; [12]; [13]; [26]	2
6	**Моделі оцінювання захищеності систем** Модель з повним перекриттям загроз. Інформаційно-аналітична модель оцінки захисту інформації від загроз несанкціонованого доступу. Вартісна модель. Логіко-ймовірнісна модель захисту інформаційних систем, функція імовірності захищеності. Особливості моделей динаміки розповсюдження хробаків. Епідемічна модель та її різновиди. Літ.: [11]; [12]; [13]	2
7	**Задачі і методи оцінювання захищеності систем** Постановка задачі оцінювання захищеності систем. Вибір критеріїв	2

	оцінювання. Аналітичний, теоретичний та аналітико-емпіричний методи оцінювання захищеності систем. Оцінювання захищеності систем методами теорії ігор. Оцінювання захищеності інформації на основі «Матриці» Домарєва. Літ.: [1] с. 8-26; [12]; [13]	
8	**Міжнародні стандарти і практики оцінювання захищеності систем** Критерії оцінювання методів захисту інформаційних технологій відповідно до ISO/IEC 15408. Оцінювання захищеності інформації відповідно до ISO 13335. Методика оцінювання захищеності від Microsoft. Оцінювання за методом STRIDE. Модель оцінювання DREAD. Літ.: [1] с. 8-26; [12]; [13]	2
	Разом за семестр:	**16**

5.2 Зміст лабораторних робіт/практичних занять

Перелік лабораторних робіт (I семестр)

№ п/п	Теми лабораторних робіт	Кількість годин
Тема 1. Моніторинг інформаційної безпеки		**24**
1	Моніторинг та аналіз пакетів в комутованому середовищі Літ.: [1] с. 166-206; [2] с. 154-205; [17]; [18]	4
2	Моніторинг та аналіз зараження ARP-кешу Літ.: [1] с. 166-206; [2] с. 154-205; [17]; [18]	4
3	Моніторинг та аналіз мережного трафіку (системи Snort та Suricata) Літ.: [1] с. 166-206; [2] с. 154-205; [19]; [20]	4
4	Моніторинг та аналіз процесів операційних систем Linux та Windows Літ.: [1] с. 166-206; [2] с. 154-205	4
5	Створення та дослідження ізольованих програмних середовищ (побудова контейнерів). Літ.: [1] с. 166-206; [2] с. 154-205; [21]	4
6	Моніторинг та аналіз шкідливого програмного забезпечення Літ.: [1] с. 166-206; [2] с. 154-205; [21]	4
Тема 2. Тактики, прийоми і процедури протидії кіберінцидентам		**10**
7	Моніторинг та аналіз інцидентів на основі платформи MISP Літ.: [1] с. 166-206; [2] с. 154-205; [22]	4
8	Аналіз подій та інцидентів, ведення журналів реєстрації, реагування та відновлення Літ.: [14]; [15]; [16]	4
9	Узагальнення матеріалу. Тестування	2
	Разом за семестр:	**34**

Перелік практичних занять (II семестр)

№ п/п	Теми практичних занять	Кількість годин
Тема 1. Менеджмент та аудит інформаційної безпеки		**8**
1	Забезпечення безпеки інформаційних мереж та систем на базі міжнародного стандарту ISO/IEC 27002 Літ.: [5]	2
2	Управління ризиками інформаційної безпеки з використанням програмних засобів Літ.: [6]; [7]; [23]	2
3	Розробка системи управління інформаційною безпекою організації Літ.: [3] с. 177-201; [8]; [9]; [10]; [23]	2
4	Проведення аудиту безпеки інформаційної системи	2

	Літ.: [5]	
Тема 2. Моделювання та оцінювання захищеності систем		**10**
5	Моделювання атак і контрзаходів Літ.: [5]	2
6	Оцінювання захищеності інформації при несанкціонованому доступі Літ.: [10]	2
7	Моделювання і оцінювання роботи систем захисту із застосуванням методів нечіткої логіки Літ.: [10]; [11]; [12]	2
8	Оцінювання ефективності систем та засобів кіберзахисту Літ.: [1] с. 8-26; [12]; [13]	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, здачі практичних завдань, 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 практичного заняття №1.	5
2	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №1. Виконання та здача практичного завдання №1.	5
3	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №2. Підготовка до практичного заняття №2.	5
4	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №2. Виконання та здача практичного завдання №2.	5
5	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №3. Підготовка до практичного заняття №3.	5
6	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №3. Виконання та здача практичного завдання №3.	5
7	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №4. Підготовка до практичного заняття №4.	5
8	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №4. Виконання та здача практичного завдання №4.	5
9	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №5. Підготовка до практичного заняття №5.	5
10	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №5. Виконання та здача практичного завдання №5.	5
11	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №6. Підготовка до практичного заняття №6.	5
12	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №6. Виконання та здача практичного завдання №6.	5
13	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №7. Підготовка до практичного заняття №7.	5
14	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №7. Виконання та здача практичного завдання №7.	5
15	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №8. Підготовка до практичного заняття №8.	5
16	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №8. Виконання та здача практичного завдання №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; практичні заняття – з використанням практичних методів та із застосуванням технологій моделювання; 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 та практичних 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;
- оцінювання результатів виконання практичних завдань.

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 (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) та практичних занять (вивчення теоретичного матеріалу з теми, активно працювати на занятті, розв'язувати задачі, брати участь у дискусіях щодо прийнятих рішень при виконанні здобувачами задач).

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 або практичне 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, практичні завдання, тестування з дисципліни, 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**	
Практичні заняття (мінімум 8 контрольних точок)								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 виконання практичних завдань

Оцінка, яка виставляється за практичне заняття, складається з таких елементів: усне опитування на знання теоретичного матеріалу з теми; вільне володіння спеціальною термінологією і уміння професійно обґрунтувати прийняті рішення при розв’язуванні завдань; самостійність та правильність виконання.

Результат виконання кожного практичного завдання 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.

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**

***Примітка**. *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

Оцінка ЄКТС	**Рейтингова шкала балів**	**Інституційна шкала (Опис рівня досягнення здобувачем вищої освіти запланованих результатів навчання з навчальної дисципліни**	
		Залік	**Іспит/диференційований залік**
A	90-100	Зараховано	***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
B	83-89		***Добре*/*Good*** – середній (максимально достатній) рівень досягнення запланованих результатів навчання з навчальної дисципліни та готовності до подальшого навчання та/або професійної діяльності за фахом
C	73-82		
D	66-72		***Задовільно*/*Satisfactory*** – Наявні мінімально достатні для подальшого навчання та/або професійної діяльності за фахом результати навчання з навчальної дисципліни
E	60-65		

FX	40-59	Незараховано	***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
F	0-39		***Незадовільно*/*Fail*** – Результати навчання відсутні

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 нижче 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. Аналіз джерел даних для систем виявлення атак/вторгнень.
2. Дослідження ознак атак/вторгнень. Методи їх виявлення.
3. Інтеграція засобів виявлення і запобігання атак/вторгнень в єдину систему.
4. Прогнозування результатів атак/вторгнень.
5. Моніторинг файлової системи, процесів та журналів операційних систем.
6. Моніторинг хостів.
7. Моніторинг мережевої архітектури.
8. Мережеві протоколи Netflow та SFlow.
9. Passive DNS.
10. Автоматизація моніторингу за допомогою скриптів.
11. Проєктування, впровадження та супровід систем моніторингу.
12. Підходи до збору інформації про події з різних пристроїв забезпечення інформаційної безпеки і мережевих пристроїв, аналіз поведінки користувачів.
13. Аутсорсинг інформаційної безпеки, як інструмент моніторингу, його переваги, недоліки та ризики.
14. Структура звітності постачальника послуг кіберзахисту. Оцінювання надійності постачальника та/або продукту.
15. Класифікація кіберінцидентів відповідно до міжнародних стандартів та рекомендацій.
16. Модель PDCA опису життєвого циклу процесів кіберінцидентів.
17. Етапи управління інцидентами відповідно до ISO/IEC 27035.
18. Особливості менеджменту інцидентів відповідно до ITIL.
19. Концепція та структура автоматизованої системи управління інцидентами.
20. Особливості організації та функціонування команд (груп) CERT/CSIRT.
21. Механізми реагування на інциденти.
22. Підходи до розслідування інцидентів та їх обробки.
23. Методи соціального інжинірингу.
24. Основні алгоритми соціотехнічних атак на інформаційні ресурси, етапи їх проведення.
25. Рекомендації щодо захисту від соціотехнічних атак.
26. Менеджмент та навчання персоналу у сфері соціотехнічної безпеки.
27. Операційні впливи за недостатності заходів з кібербезпеки.
28. Планування безперервності роботи бізнес/операційних процесів.
29. Розробка відмовостійкого кластеру (вимоги до структури, принципи проєктування, дослідження надійності вузлів, алгоритми відновлення при відмовах та кіберінцидентах).
30. Особливості процесу розвідувальної роботи з точки зору інформаційної та кібербезпеки.
31. Джерела поширення інформації про вразливості (попередження, рекомендації, помилки та бюлетені).

32. Формування вимог та розробка аналітичного плану.
33. Дослідження етапів проведення аналізу (збір даних, обробка, поширення інформації).
34. Інтеграція розвідувальної роботи в управління кіберінцидентами.
35. Аналіз загроз інформаційної безпеки на об’єктах інформаційної діяльності.
36. Особливості формування концепції і політики інформаційної безпеки на основі аналізу загроз.
37. Оцінювання політики безпеки на відповідність стандартам.
38. Процеси управління ризиками згідно NIST 800-30 та ISO 27005.
39. Процеси розробки контрзаходів для виявлених ризиків безпеки.
40. Методика, технології та сучасні інструментальні засоби аналізу ризиків.
41. Концепції в управлінні безпекою (Release Management, Patch Management, ISO 27xxx).
42. Розробка системи менеджменту інформаційної безпеки (СМІБ).
43. Формування правил, положень та функцій технологічного управління безпекою організації.
44. Принципи проведення внутрішнього аудиту.
45. Управління програмою аудиту.
46. Аудит інформаційної безпеки на основі аналізу ризиків. Компетентність аудиторів та особливості її оцінювання.
47. Основні етапи комплексного аудиту безпеки інформаційних систем.
48. Оцінка діяльності з управління інформаційною безпекою організації. Удосконалення інформаційної безпеки організації за допомогою передачі та страхування ризиків.
49. Моделі аналізу, синтезу та управління систем захисту інформації.
50. Системний підхід в моделях захисту інформації, ідентифікація системи і процесу.
51. Оцінювання повноти та достовірності вихідних даних при моделюванні систем і засобів кіберзахисту.
52. Особливості застосування граф-моделей (дерева атак і контрзаходів, графи шляхів реалізації атаки, графи загроз тощо).
53. Модель з повним перекриттям загроз.
54. Інформаційно-аналітична модель оцінки захисту інформації від загроз несанкціонованого доступу.
55. Вартісна модель.
56. Логіко-ймовірнісна модель захисту інформаційних систем, функція імовірності захищеності.
57. Особливості моделей динаміки розповсюдження хробаків.
58. Епідемічна модель та її різновиди.
59. Постановка задачі оцінювання захищеності систем. Вибір критеріїв оцінювання.
60. Аналітичний, теоретичний та аналітико-емпіричний методи оцінювання захищеності систем.
61. Оцінювання захищеності систем методами теорії ігор.
62. Оцінювання захищеності інформації на основі «Матриці» Домарєва.
63. Критерії оцінювання методів захисту інформаційних технологій відповідно до ISO/IEC 15408.
64. Оцінювання захищеності інформації відповідно до ISO 13335.
65. Методика оцінювання захищеності від Microsoft.
66. Оцінювання за методом STRIDE.
67. Модель оцінювання DREAD.

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=7526; II семестр – https://msn.khmnu.edu.ua/course/view.php?id=7863.

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, Oracle Virtual Box, Ettercap, Wireshark, Nessus, Snort/Suricata, Nmap (Zenmap), MS Visual Studio 19 або вище, Docker, MISP Threat Sharing, CORAS Tools тощо.

Спеціальне апаратне забезпечення: маршрутизатори Cisco S4400, комутатори C2960, міжмережні екрани Cisco ASA/CISCO Fortinet та інше мережеве обладнання.

13. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

1. 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.
2. Інформаційна безпека в комп'ютерних мережах: навч. посіб./ О.А. Смірнов, Конопліцька-О.К. Слободенюк, С.А. Смірнов, К.О. Буравченко, Т.В. Смірнова, Л.І. Поліщук. Кропивницький: Видавець Лисенко В. Ф., 2020. 295 с.
3. Information Security Handbook/ Noor Zaman Jhanjhi, Khalid Hussain, Mamoona Humayun, Azween Bin Abdullah, João Manuel R.S. Tavares. CRC Press, 2022. 250 p.
4. Інформаційна безпека. Підручник/ В. В. Остроухов, М. М. Присяжнюк, О. І. Фармагей, М. М. Чеховська та ін.; під ред. В. В. Остроухова. К.:Видавництво Ліра-К, 2021. 412 с.
5. Інформаційні мережі: навчальний посібник / Ю. В. Коваль, А. Б. Ставровський. Київ, 2021. 84 с.

Додаткова

6. NIST SP 800-30. Guide for Conducting Risk Assessments.
7. ISO/IEC 27005. Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки.
8. ISO/IEC 27000. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Огляд та словник термінів.
9. ISO/IEC 27001. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою.
10. ISO/IEC 27003. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Керівництво.
11. ISO/IEC 27002. Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою.
12. ISO/IEC 15408. Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки IT.
13. ISO/IEC 13335. Інформаційні технології. Настанови з керування безпекою інформаційних технологій (IT)
14. NIST SP 800-61. Computer Security Incident Handling Guide.
15. ISO/IEC 27035. Інформаційні технології. Методи захисту. Керування інцидентами інформаційної безпеки.
16. CISA Посібник з додаткових ресурсів CRR. Том 5. Управління кіберінцидентами.
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. Snort. Documents [Електронний ресурс]. Режим доступу: https://www.snort.org/documents
20. Suricata [Електронний ресурс]. Режим доступу: https://suricata.io
21. Інструменти для аналізу шкідників. Інструменти динамічного аналізу та пісочниці [Електронний ресурс]. Режим доступу: https://surl.li/bunfov
22. Що таке платформа MISP і як нею користуватися? [Електронний ресурс]. Режим доступу: https://kr-labs.com.ua/blog/shcho-take-platforma-misp

23. CORAS A risk modeling approach [Електронний ресурс]. Режим доступу: https://coras.tools/#/try-it

24. Методика ідентифікації та оцінювання важливості інформаційних активів/ Віра Тітова, Юрій Кльоц, Богдан Кальчун, Анна Кувіла, Ірина Рак// Вісник Хмельницького національного університету, 2024. №5. С. 521-525

25. 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

26. Порівняльний аналіз моделей атак на інформаційну безпеку/ В. Тітова, Ю. Кльоц, З. Лакоценін, О. Шлапак, В. Троц// Вісник Хмельницького національного університету, 2024.

27. Fuzzy inference subsystem for classifying threats to computer information/ Віра Тітова, Юрій Кльоц, Наталія Петляк, Марія Капустян// Measuring and computing devices in technological processes, 2022. №1. С. 57-61.

28. Detection of network attacks in cyber-physical systems using a rule-based logical neural network/ Titova, V., Klots, Y., Cheshun, V., Petliak, N., Salem, A.-B.M.// CEUR Workshop, 2024, 3736, P. 255–268

29. Research of the Neural Network Module for Detecting Anomalies in Network Traffic/ Klots, Y., Titova, V., Petliak, N., Cheshun, V., Salem, A.-B.M. //CEUR Workshop Proceedings, 2022, 3156, P. 378–389

14. ІНФОРМАЦІЙНІ РЕСУРСИ

1. Модульне середовище для навчання. URL : https://msn.khmnu.edu.ua/course/view.php?id=7526 https://msn.khmnu.edu.ua/course/view.php?id=7863
2. Електронна бібліотека ХНУ. URL: http://lib.khmnu.edu.ua/
3. Інституційний репозитарій ХНУ. URL : https://library.khmnu.edu.ua/

МОНІТОРИНГ ТА МЕНЕДЖМЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

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 *спілкуватися* державною мовою для представлення результатів та обговорення питань аналізу, моніторингу, аудиту, менеджменту та реагування на інциденти ІБ; *планувати* навчання, *координувати* персонал у сфері соціотехнічної безпеки; чітко *доносити* висновки, *інтегрувати* теорію ризиків, *застосовувати* сучасні математичні моделі для оцінювання захищеності систем; *впроваджувати* світові стандарти, *досліджувати* та *супроводжувати* засоби ІБ, *управляти* проєктами з реагування на інциденти, *аналізувати* нормативні документи, *застосовувати* моделювання, *обґрунтовувати* вибір технічних засобів; *приймати* рішення в умовах невизначеності, *будувати* системи управління ІБ, *забезпечувати* безперервність бізнес-процесів, *виявляти* загрози, *аналізувати* трафік, артефакти, типи атак, *здійснювати* управління інцидентами, розслідування, аудит та оцінювання ефективності ІБ.

Зміст навчальної дисципліни. Системи виявлення вторгнень (IDS). Системи попередження вторгнень (IPS). Методології та прийоми виявлення атак/вторгнень. Особливості організації моніторингу інформаційно-комунікаційних систем та їх компонентів. Особливості розробки та супроводу систем моніторингу на об'єктах інформаційної діяльності. Аутсорсинг інформаційної безпеки, як інструмент моніторингу. Структура звітності постачальника послуг кіберзахисту. Оцінювання надійності постачальника та/або продукту. Методологія реагування на інциденти та їх обробки. Тактики, прийоми і процедури протидії кіберінцидентам. Соціотехнічна безпека. Конкретні операційні впливи за недостатності заходів з кібербезпеки. Планування безперервності роботи. Джерела поширення інформації про загрози та вразливості. Аналіз розвідувальних даних щодо кіберзагроз та кіберінцидентів (CTI). Сучасні підходи в моделюванні систем і засобів кіберзахисту. Задачі і методи оцінювання безпеки систем. Міжнародні стандарти і практики оцінювання безпеки систем. Аналіз загроз безпеки. Моделі безпеки. Політики, процедури та правила кіберзахисту та інформаційної безпеки. Управління інформаційною безпекою, концепції управління. Ризик-менеджмент інформаційної безпеки. Розробка контрзаходів для виявлених ризиків безпеки. Внутрішній аудит інформаційної безпеки. Комплексний аудит інформаційної безпеки.

Пререквізити – вихідна, теорія проєктування та тестування безпеки захищених систем.

Постреквізити – теорія проєктування та тестування безпеки захищених систем, 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); практичні заняття (з використанням практичних методів та із застосуванням технологій моделювання); самостійна робота (з використанням пояснювально-ілюстративних та дослідницьких методів).

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

Вид семестрового контролю: іспит – 1,2 семестр

Навчальні ресурси:

1. 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.
2. Інформаційна безпека в комп'ютерних мережах: навч. посіб./ О.А. Смірнов, Конопліцька-О.К. Слободенюк, С.А. Смірнов, К.О. Буравченко, Т.В. Смірнова, Л.І. Поліщук. Кропивницький: Видавець Лисенко В. Ф., 2020. 295 с.
3. Information Security Handbook/ Noor Zaman Jhanjhi, Khalid Hussain, Mamoona Humayun, Azween Bin Abdullah, João Manuel R.S. Tavares. CRC Press, 2022. 250 p.
4. Інформаційна безпека. Підручник/ В. В. Остроухов, М. М. Присяжнюк, О. І. Фармагей, М. М. Чеховська та ін.; під ред. В. В. Остроухова. К.:Видавництво Ліра-К, 2021. 412 с.
5. Інформаційні мережі: навчальний посібник / Ю. В. Коваль, А. Б. Ставровський. Київ, 2021. 84 с.
6. Модульне середовище для навчання. Доступ до ресурсу: https://msn.khmnu.edu.ua/course/view.php?id=7526 https://msn.khmnu.edu.ua/course/view.php?id=7863
7. Електронна бібліотека ХНУ. Доступ до ресурсу: http://lib.khmnu.edu.ua

Викладач: канд. техн. наук, доц. Тітова В.Ю.