ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ЗАТВЕРДЖУЮ

Декан факультету інформаційних технологій

_____ Тетяна ГОВОРУЩЕНКО
Підпис Ім'я, ПРІЗВИЩЕ

29 серпня 2025 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Захист інформації в інформаційно-комунікаційних системах

Галузь знань – F Інформаційні технології
Спеціальність – F5 Кібербезпека та захист інформації
Рівень вищої освіти – Перший (бакалаврський)
Освітньо-професійна програма – Кібербезпека та захист інформації
Обсяг дисципліни – 13 кредитів ЄКТС
Шифр дисципліни – ОФП.05
Мова навчання – Українська
Статус дисципліни – Обов'язкова (фахової підготовки)
Факультет – Інформаційних технологій
Кафедра – Кібербезпеки

Форма здобуття освіти	Курс	Семестр	Загальний обсяг		Кількість годин						Курсовий проєкт*	Курсова робота	Форма семестрового контролю	
					Аудиторні заняття					Самостійна робота, у т.ч. ІРС				
			Кредити ЄКТС	Години	Разом	Лекції	Лабораторні роботи	Практичні заняття	Семінарські заняття				Залік	Іспит
Д	2	3	4	120	50	16	34	-	-	70	-	-	-	+
Д	2	4	4	120	50	16	34	-	-	70	+	-	-	+
Д	3	5	5	150	50	16	34	-	-	100	-	-	-	+
Разом ДФН			**13**	**390**	**150**	**48**	**102**	-	-	**240**	**1**	-	-	**3**

Примітка. *З навчальної дисципліни у 4 семестрі передбачений курсовий проєкт, зміст та вимоги до виконання якого регулюються відповідними методичними рекомендаціями.

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, доцент Юрій КЛЬОЦ
Підпис автора(ів) Науковий ступінь, вчене звання, Ім'я, ПРІЗВИЩЕ автора(ів)

_____ д-р філософії Микола СТЕЦЮК
Підпис автора(ів) Науковий ступінь, вчене звання, Ім'я, ПРІЗВИЩЕ автора(ів)

Схвалена на засіданні кафедри Кібербезпеки

Протокол від 29.08.2025 № 1. Зав. кафедри _____ 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

ЛИСТ ПОГОДЖЕННЯ

Посада	Назва кафедри	Підпис	Ініціали, прізвище
Завідувач кафедри, канд. техн. наук, доц.	Кібербезпеки		Юрій КЛЬОЦ
Гарант освітньо-професійної програми, канд. техн. наук, доц.	Кібербезпеки		Віктор ЧЕШУН

3. Пояснювальна записка

Дисципліна «Захист інформації в інформаційно-комунікаційних системах» є однією із дисциплін фахової підготовки і займає провідне місце у підготовці здобувачів першого (бакалаврського) рівня вищої освіти, очної (денної) (далі – денної) форми здобуття вищої освіти, які навчаються за освітньо-професійною програмою «Кібербезпека та захист інформації» в межах спеціальності F5 «Кібербезпека та захист інформації».

***Пререквізити*:** ОФП.01 Основи інформаційної безпеки; ОФП.03 Теорія інформації та кодування; ОФП.04 Сигнали і процеси в системах захисту інформації

***Постреквізити**:* ОФП.06 Захист інформації в інформаційно-комунікаційних системах (курсовий проєкт); ОФП.12 Комплексні системи захисту інформації; ОФП.13 Технології виявлення вразливостей та вторгнень; ОФП.15 Виробнича практика 1; ОФП.16 Виробнича практика 2.

Відповідно до освітньої програми дисципліна сприяє забезпеченню:

компетентностей: ІК Здатність розв'язувати складні спеціалізовані задачі і практичні завдання у галузі кібербезпеки та захисту інформації; ЗК01. Здатність застосовувати знання у практичних ситуаціях; ЗК02. Знання та розуміння предметної області і розуміння професійної діяльності; ФК02. Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації; ФК04. Здатність забезпечувати захист інформації в інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації; ФК05. Здатність відновлювати функціонування інформаційних та інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв і відмов різних класів та походження; УК01. Здатність налаштовувати та оптимізовувати мережеве обладнання, тестувати та підтримувати мережеву інфраструктуру включно із програмним та апаратним забезпеченням, діагностувати проблеми підключення до мережі та несправне апаратне забезпечення системи/сервера.

***програмних результатів навчання*:** ПРН04. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність; ПРН10. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності; ПРН12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки; ПРН13. Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних і програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних й інформаційно-комунікаційних систем та\або інфраструктури організації в цілому; ПРН14. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційних та інформаційно-комунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки і забезпечувати функціонування спеціального програмного забезпечення щодо захисту та відновлення інформації; ПРН22. Проводити планування, управління та обслуговування систем/серверів, встановлювати, налаштовувати, експлуатувати мережеве обладнання (маршрутизатори, комутатори, файрволи, сервери, засоби передачі та відповідне апаратне обладнання), налаштовувати маршрути в мережах організації та розмежовувати доступи до ресурсів; ПРН23. Використовувати інструменти управління мережею для аналізу структур мережевого трафіку, діагностувати несправні системні компоненти.

Мета дисципліни. Формування у здобувачів освіти глибоких знань і практичних навичок щодо принципів побудови, функціонування та захисту інформаційно-комунікаційних систем. Забезпечення розуміння архітектурних рішень, протоколів передачі даних, моделей взаємодії відкритих систем, сучасних методів і засобів забезпечення конфіденційності, цілісності та доступності інформації в телекомунікаційних мережах.

Предмет дисципліни. Архітектура, принципи функціонування, протоколи та сервіси інформаційно-комунікаційних систем, а також методи, технології та програмно-апаратні засоби захисту інформації, що обробляється і передається в таких системах.

Завдання дисципліни. Формування у здобувачів системного розуміння принципів побудови та функціонування інформаційно-комунікаційних систем, оволодіння знаннями щодо архітектур мереж, протоколів обміну даними, моделей взаємодії відкритих систем, методів захисту інформаційних потоків та програмно-апаратних засобів забезпечення безпеки. У процесі вивчення дисципліни здобувачі набувають практичних навичок проектування, конфігурування та адміністрування мережевих компонентів з урахуванням вимог інформаційної та кібербезпеки, реалізації механізмів автентифікації, авторизації та контролю доступу, застосування засобів шифрування, резервування і відновлення працездатності систем після інцидентів безпеки, а також моніторингу та аналізу трафіку з метою виявлення аномальної активності..

Результати навчання. Після вивчення дисципліни студент повинен: *знати* принципи побудови та функціонування інформаційно-комунікаційних систем, методи організації захисту даних на рівнях мережевих протоколів, обладнання та сервісів; *застосовувати* знання і навички з проектування, налаштування та адміністрування мереж із забезпеченням безпеки передавання інформації; *діяти* на основі технічних вимог і стандартів інформаційної безпеки під час реалізації систем виявлення вторгнень, контролю доступу та фільтрації трафіку; *організовувати* процеси моніторингу та управління безпечним функціонуванням мережевої інфраструктури; *впроваджувати* методи аналізу, класифікації та реагування на аномальну мережеву активність; *володіти знаннями* сучасних засобів захисту, шифрування, сегментації трафіку, виявлення та усунення вразливостей; *бути здатним* проводити технічну оцінку стану інформаційної безпеки мережевих систем і приймати рішення щодо відновлення їх працездатності після інцидентів; *аналізувати, аргументувати, приймати рішення* при вирішенні складних задач захисту мережевої інфраструктури; *застосовувати знання* сучасних методів і технологій моніторингу та управління інформаційними потоками, а також *використовувати* технічну термінологію англійською мовою для забезпечення ефективної професійної комунікації у сфері інформаційної та кібербезпеки.

4. Структура залікових кредитів дисципліни

Назва теми	Кількість годин, відведених на:		
	лекції	**лабораторні роботи**	**СРС**
Третій семестр			
Тема 1. Основні поняття комп'ютерних мереж	6	12	37
Тема 2. Організація роботи мережі	8	16	49
Тема 3. Автентифікація, авторизація та облік	2	6	14
Разом за 3-й семестр:	**16**	**34**	**100**
Четвертий семестр			
Тема 4. Безпека локальних та віртуальних приватних мереж (LAN, VPN)	10	20	62
Тема 5. Моніторинг та управління безпекою мережі	6	14	38
Разом за 4-й семестр:	**16**	**34**	**100**
П'ятий семестр			
Тема 6: Основні проблеми, вимоги та принципи захисту безпроводових технологій	4	4	11
Тема 7. Проблеми безпеки мобільних пристроїв, систем і додатків	10	12	26
Тема 8. Безпека Інтернету речей.	12	12	31
Тема 9. Управління та підтримка даних в хмарних технологіях для ефективного їх захисту	6	6	16
Разом за 5-й семестр:	32	34	84

5. Програма навчальної дисципліни

5.1 Зміст лекційного курсу

Номер лекції	**Перелік змістових модулів, тем лекцій, їх анотації**	**Кількість годин**
	Третій семестр	
	Тема 1. Основні поняття комп'ютерних мереж	**6**
1	**Сучасні мережні технології.** Компоненти мережі. Зображення мереж і топології. Основні типи мереж. Інтернет-з'єднання. Тенденції розвитку мереж. Літ.: [1] с.132-183	2
2	**Протоколи та моделі.** Правила. Протоколи. Стеки протоколів. Організації зі стандартизації. Еталонні моделі. Літ.: [2] с. 131-144	2
3	**Мережний рівень.** Характеристики мережного рівня. Пакет IPv4. Пакет IPv6. Методи маршрутизації хостів. Вступ до маршрутизації. Літ.: [2] с.67-96	2
	Тема 2. Організація роботи мережі	**8**
4	**Комутація Ethernet. Визначення адрес.** Кадри Ethernet. MAC-адреса Ethernet. Таблиця MAC-адрес. Швидкості комутатора і методи пересилання. Літ.: [3] с. 5-18; [10] с. 46-109	2
5	**Мережні сервіси.** DHCP. DNS. NAT. MAIL. HTTP. Літ.: [9] с.166-206; [11] с. 372-399	2
6	**Адресація IPv4 та IPv6.** Структура адреси IPv4. Одноадресна, широкомовна та групова розсилки IPv4. Типи адрес IPv4. Сегментація мережі. Розподіл на підмережі відповідно до вимог. Маска підмережі змінної довжини (VLSM). Проблеми з IPv4. Подання адрес IPv6. Типи адрес IPv6. Статична та динамічна адресація для глобальних	2

	індивідуальних адрес (GUA) IPv6. Розподіл мережі IPv6 на підмережі Літ.: [8] с. 142-168; [10] с. 111-216;[11] с. 399-466	
7	**Базові налаштування ACL.** Призначення ACL. Шаблонні маски в ACL. Рекомендації щодо створення ACL. Типи ACL для IPv4. Налаштування стандартних ACL для IPv4. Зміна ACL для IPv4.Літ.: [8] с. 169-197	2
Тема 3. Автентифікація, авторизація та облік		**2**
8	**Автентифікація, авторизація та облік.** Призначення AAA. Локальна аутентифікація AAA. Серверна аутентифікація AAA. Автентифікація RADIUS. Літ.: [8] с. 115-166	2
	Разом за 3-й семестр:	**16**
Четвертий семестр		
Тема 4. Безпека локальних та віртуальних приватних мереж (LAN, VPN)		**10**
9	**Віртуальні локальні мережі.** Огляд VLAN. VLAN у мережі з кількома комутаторами. Налаштування VLAN. Магістральні (транкові) канали у VLAN. Протокол динамічного транкування DTP. Літ.: [11] с.382-399	2
10	**Маршрутизація.** Визначення маршруту. Пересилання пакетів. Огляд базової конфігурації маршрутизатора. Таблиця IP-маршрутизації. Статична та динамічна маршрутизація. Принципи маршрутизації між VLAN. Маршрутизація між VLAN методом Router-on-a-Stick. Маршрутизація між VLAN за допомогою комутаторів Рівня 3. Виявлення і усунення несправностей із маршрутизацією між VLAN. Літ.: [3] с. 43-67; [9] с. 92-115	2
11	**Доступність та надійність мережі.** Протоколи резервування першого переходу. HSRP. Механізми QoS. Літ.: [3] с. 68-81; [9] с. 116-127	2
12	**Безпека LAN.** Безпека кінцевих точок. Керування доступом. Загрози безпеці Рівня 2. Атаки на таблиці MAC-адрес. Атаки на локальну мережу. Літ.: [3] с. 76-92; [9] с. 79-91	2
13	**Функціонування VPN та IPsec.** Компоненти мережі IPsec. VPN і їх функціонування Літ.: [3] с. 93-113; [9] с. 92-115	2
Тема 5. Моніторинг та управління безпекою мережі		**6**
14	**Інфраструктура мережної безпеки.** Пристрої безпеки. Служби безпеки. Системи керування мережею. Протокол SNMP. Літ.: [3] с. 114-127	2
15	**Джерела даних про кіберінциденти.** Типи даних про безпеку. Журнали кінцевих пристроїв. Мережні журнали. Джерела сповіщень. Дослідження даних мережі. Активізація роботи аналітика з кібербезпеки. Робота з даними про безпеку мережі. Літ.: [10] с. 217-248	2
16	**Цифрова технічна експертиза, аналіз інцидентів і реагування.** Робота з доказами та атрибуція атаки. Ланцюжок кібершахрайства. Ромбоподібна модель аналізу вторгнення. Реагування на інциденти. Літ.: [10] с. 249-297	2
	Разом за 4-й семестр:	**16**
П'ятий семестр		
Тема 6. Основні проблеми, вимоги та принципи захисту безпроводових технологій		**4**
17	**Загрози та атаки на безпроводові мережі.** Класифікація атак на безпроводові мережі та їх характеристики. Моделі та критерії загроз у безпроводових мережах. Методи оцінки загроз у безпроводових мережах. Літ.: [11] с. 20-30; [8] с. 120-135	2
18	**Захист безпроводових мереж.** Технології побудови безпроводових мереж .Шляхи захисту безпроводових мереж. Літ.: [11] с. 35-60; [8] с. 140-160	2
Тема 7. Проблеми безпеки мобільних пристроїв, систем і додатків		**10**

19	**Загрози та вразливості мобільних пристроїв.** Загальні положення. Класифікація загроз та вразливостей мобільних пристроїв Літ.: [10] с. 15-30; [8] с. 170-190	2
20	**Управління мобільними пристроями.** Управління з метою забезпечення захисту. Життєвий цикл рішень з безпеки мобільних пристроїв Літ.: [10] с. 35-50; [9] с. 50-70	2
21	**Загрози та вразливості мобільних телекомунікаційних систем.** Загрози та вразливості стандартів 3G. Загрози та вразливості стандартів 4G. Загрози та вразливості стандартів 5G. Літ.: [7] с. 45-60; [11] с. 80-100	2
22	**Загрози та вразливості Wi-Fi-мереж.** Класифікація загроз та вразливостей Wi-Fi-мереж. Методи захисту Wi-Fi-мереж. Літ.: [7] с. 20-40; [11] с. 120-135	2
23	**Загрози та вразливості мобільних додатків.** Класифікація загроз та вразливостей мобільних додатків. Аналіз захищеності мобільних додатків. Літ.: [11] с. 75-90; [6] с. 150-170	2
Тема 8. Безпека Інтернету речей		**12**
24	**Вступ до Інтернету речей.** Загальні принципи побудови та архітектура IoT. Класифікація систем IoT. Літ.: [6] с. 10-30; [10] с. 40-70	2
25	**Засоби ідентифікації.** Класифікація засобів автоматичної ідентифікації. MAC-адреса. Радіочастотна ідентифікація (RFID). Система позиціонування в режимі реального часу RTLS. Оптичні ідентифікатори. Літ.: [5] с. 35-50; [8] с. 80-100	2
26	**Технології передачі даних в IoT (частина 1).** Стандарт IEEE 802.15.4. Bluetooth (IEEE 802.15.1). ZigBee. Wi-Fi та IEEE 802.11. Літ.: [6] с. 15-35; [8] с. 110-140	2
27	**Технології передачі даних в IoT (частина 2).** Технологія LPWAN. Технологія PLC. Літ.: [6] с. 40-55; [8] с. 150-170	2
28	**Забезпечення безпеки в IoT (частина 1).** Проблема безпеки IoT. Проблеми конфіденційності в IoT. Літ.: [6] с. 80-95; [8] с. 190-210	2
29	**Забезпечення безпеки в IoT (частина 2).** Анатомія кібератак на IoT-пристрої. Фізична і апаратна безпека. Криптографія, як складова безпеки в IoT. Блокчейн і криптовалюта в Інтернеті речей Літ.: [6] с. 100-120; [8] с. 220-240	2
Тема 9. Управління та підтримка даних в хмарних технологіях для ефективного їх захисту		**6**
30	**Топологія хмарних обчислень.** Модель хмарних сервісів. Види хмар та хмарна архітектура. Хмарна архітектура OpenStack. Обмеження хмарних архітектур Літ.: [3] с. 25-45; [9] с. 70-90	2
31	**Топологія туманних обчислень.** Туманні обчислення. Архітектура OpenFog RA. Amazon Greengrass і лямбда-функції. Туманні топології Літ.: [3] с. 50-70; [9] с. 100-120	2
32	**Технології Big Data.** Поняття Big Data, їх характеристики та сфери застосування. Категорії даних (грані даних) та процес data science. Технології та тенденції роботи з Big Data Літ.:[3] с. 75-90; [9] с. 130-150	2
	Разом за 5-й семестр:	**32**

5.2 Зміст лабораторних/практичних/семінарських занять

№ п/п	Тема лабораторної роботи	К-ть годин
Третій семестр		
1	Основи роботи з середовищем моделювання та мережним обладнанням. Літ.:[1] с. 155-159.	4
2	Протоколи та моделі прикладного і транспортного рівнів. Літ.:[1] с. 50-61.	4
3	Мережний рівень. IP4- та IP6- адресація, VLSM-адресація. Літ.: [1] с. 39-47, 205-228.	4
4	Канальний рівень, забезпечення безпеки мережі на канальному рівні. Літ.: [1] с. 26-	4

	33	
5	DHCP сервер та клієнт. Літ.: [1] с. 86-94	4
6	Налаштування базових параметрів безпеки маршрутизатора і комутатора. Літ.: [1] с. 331-341, [2] с. 309 – 326, [3] с. 151-161.	4
7	Списки контролю доступу. Налаштування служби NAT Літ.: [2] с. 122 – 127, [3] с.166 – 177, 188-194.	4
8	Проектування малої мережі. Літ.: [1] с. 364 – 384	4
9	Підсумкове заняття. Тестування.	2
	Разом за 3-й семестр:	**34**
	Четвертий семестр	
10	Налаштування VPN тунелю між двома мережами. Літ.: [2] с. 225 – 232	4
11	Дослідження протоколу IPsec. Літ.: [1] с.199-221	4
12	Створення мережі IPsec VPN. Літ.: [3] с. 93-11	4
13	Налаштування Cisco IOS IPS Літ.: https://contenthub.netacad.com/sec/8.4.1#8.4.3	4
14	Налаштування політики доступу на Cisco ASA Літ.: https://contenthub.netacad.com/sec/9.2.1#9.2.4	4
15	Налаштування брандмауера на основі ідентифікації Cisco ASA Літ.: https://contenthub.netacad.com/sec/9.3.1#9.3.5	4
16	Моніторинг мережевого обладнання з використанням протоколу SNMP. Літ.: https://contenthub.netacad.com/sec/9.3.1#9.3.5	4
17	Дослідження інструментів тестування мережевої безпеки. Літ.: [2] с.183-186	4
18	Підсумкове заняття. Тестування	2
	Разом за 4-й семестр:	**34**
	П'ятий семестр	
19	Розгортання робочого середовища для проведення аудиту безпеки безпроводових мереж Літ.: [1] с. 15-30; [2] с. 40-55; [6] с. 10-20	4
20	Сканування мережевих протоколів. Літ.: [1] с. 31-45; [2] с. 56-70;	4
21	Збирання технічної та чуттєвої інформації в безпроводових мережах Літ.: Літ.: [3] с. 15-30; [6] с. 36-50	4
22	Дослідження вразливостей безпроводових мереж. Літ.: [2] с. 71-85; [3] с. 31-45;	4
23	Дослідження технологій злому безпроводових мереж Літ.: Літ.: [4] с. 20-35; [7] с. 56-70	4
24	Дослідження способів здійснення атак на відмову Літ.: [2] с. 101-115; [7] с. 71-85	4
25	Програмування пристроїв Інтернету речей засобами Cisco Packet Tracer Літ.: [3] с. 10-25; [5] с. 30-45; [8] с. 15-30	4
26	Захист хмарних сервісів Інтернету речей Літ.: Літ.: [5] с. 46-60; [8] с. 31-40	4
27	Підсумкове заняття. Тестування.	2
	Разом за 5-й семестр:	**34**

5.3 Зміст самостійної (у т. ч. індивідуальної) роботи здобувача вищої освіти

Самостійна робота студентів полягає у систематичному опрацюванні програмного матеріалу з відповідних джерел інформації, підготовці до виконання і захисту лабораторних робіт, роботу над курсовим проектом та підготовку до його захисту, тестування з теоретичного матеріалу тощо. Крім цього до послуг студентів сторінка дисципліни в Модульному середовищі для навчання, де розміщені Робоча програма дисципліни та необхідні матеріали з її навчально-методичного забезпечення та контролю результатів навчання.

Номер тижня	Теми самостійної роботи	Кількість годин
	Третій семестр	
1	Опрацювання лекційного матеріалу, підготовка до лабораторної роботи №1.	5
2	Опрацювання лекційного матеріалу, підготовка до захисту лабораторної роботи №1	6

3	Опрацювання лекційного матеріалу, підготовка до лабораторної роботи №2.	6
4	Опрацювання лекційного матеріалу, підготовка до захисту лабораторної роботи №2	6
5	Опрацювання лекційного матеріалу, підготовка до лабораторної роботи №3.	6
6	Опрацювання лекційного матеріалу, підготовка до захисту лабораторної роботи №3.	6
7	Опрацювання лекційного матеріалу, підготовка до лабораторної роботи №4.	6
8	Опрацювання лекційного матеріалу, підготовка до захисту лабораторної роботи №4.	6
9	Опрацювання лекційного матеріалу, підготовка до лабораторної роботи № 5.	6
10	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи № 5	6
11	Опрацювання лекційного матеріалу. Підготовка до лабораторної роботи № 6.	6
12	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи № 6	6
13	Опрацювання лекційного матеріалу. Підготовка до лабораторної роботи № 7.	6
14	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної №7	6
15	Опрацювання лекційного матеріалу. Підготовка до лабораторної роботи № 8.	6
16	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи № 8.	6
17	Опрацювання лекційного матеріалу. Тестування	5
Разом за 3-й семестр:		**100**
Четвертий семестр		
1	Опрацювання лекційного матеріалу, підготовка до лабораторної роботи №1.	5
2	Опрацювання лекційного матеріалу, підготовка до захисту лабораторної роботи №1	6
3	Опрацювання лекційного матеріалу, підготовка до лабораторної роботи №2.	6
4	Опрацювання лекційного матеріалу, підготовка до захисту лабораторної роботи №2	6
5	Опрацювання лекційного матеріалу, підготовка до лабораторної роботи №3.	6
6	Опрацювання лекційного матеріалу, підготовка до захисту лабораторної роботи №3.	6
7	Опрацювання лекційного матеріалу, підготовка до лабораторної роботи №4.	6
8	Опрацювання лекційного матеріалу, підготовка до захисту лабораторної роботи №4.	6
9	Опрацювання лекційного матеріалу, підготовка до лабораторної роботи № 5.	6
10	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи № 5	6
11	Опрацювання лекційного матеріалу. Підготовка до лабораторної роботи № 6.	6
12	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи № 6	6
13	Опрацювання лекційного матеріалу. Підготовка до лабораторної роботи № 7.	6
14	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної №7	6
15	Опрацювання лекційного матеріалу. Підготовка до лабораторної роботи № 8.	6
16	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи № 8.	6
17	Опрацювання лекційного матеріалу. Тестування	5
	Разом за 4-й семестр:	**100**
П'ятий семестр		
1	Опрацювання лекційного матеріалу, **п**ідготовка до лабораторної роботи №1.	4
2	Опрацювання лекційного матеріалу, **п**ідготовка до захисту лабораторної роботи №1	5
3	Опрацювання лекційного матеріалу, **п**ідготовка до лабораторної роботи №2.	5
4	Опрацювання лекційного матеріалу, **п**ідготовка до захисту лабораторної роботи №2	5
5	Опрацювання лекційного матеріалу, **п**ідготовка до лабораторної роботи №3.	5
6	Опрацювання лекційного матеріалу, **п**ідготовка до захисту лабораторної роботи №3.	5
7	Опрацювання лекційного матеріалу, **п**ідготовка до лабораторної роботи №4.	5
8	Опрацювання лекційного матеріалу, **п**ідготовка до захисту лабораторної роботи №4.	5
9	Опрацювання лекційного матеріалу, **п**ідготовка до лабораторної роботи № 5.	5
10	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи № 5	5
11	Опрацювання лекційного матеріалу. Підготовка до лабораторної роботи № 6.	5
12	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи № 6	5
13	Опрацювання лекційного матеріалу. Підготовка до лабораторної роботи № 7.	5
14	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної №7	5
15	Опрацювання лекційного матеріалу. Підготовка до лабораторної роботи № 8.	5
16	Опрацювання лекційного матеріалу. Підготовка до захисту лабораторної роботи № 8**.**	5
17	Опрацювання лекційного матеріалу. **Тестування**	5
	Разом за 5-й семестр:	**84**

6. Технології та методи навчання

Процес навчання з дисципліни ґрунтується на використанні традиційних та сучасних технологій та методів. Зокрема, лекції проводяться з використанням словесних, наочних, інтерактивних та проблемних методів з супроводом мультимедійних технологій та презентаційних

матеріалів; лабораторні роботи – з використанням практичних та частково-пошукових методів, із застосуванням сучасних інформаційно-комп'ютерних технологій; самостійна робота – з використанням пояснювально-ілюстративних та частково-пошукових методів.

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 засвоєння теоретичного та практичного матеріалу.

При виведенні підсумкової семестрової оцінки враховуються результати як поточного контролю, так і підсумкового контролю, 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 обсяг роботи, передбачений Робочою програмою. Здобувач вищої освіти, який набрав позитивний середньозважений бал (60 відсотків і більше від максимального балу) 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), активно працювати на занятті, виконати поставлене завдання тощо.

Здобувачі вищої освіти мають дотримуватися встановлених термінів виконання всіх видів навчальної роботи відповідно до робочої програми навчальної дисципліни. Пропущене лабораторне заняття студент зобов'язаний відпрацювати у встановлений викладачем термін, але не пізніше, ніж за два тижні до кінця теоретичних занять у семестрі.

Засвоєння студентом теоретичного матеріалу з дисципліни оцінюється за результатами опитування під час захисту лабораторних робіт та тестування.

Здобувач вищої освіти, виконуючи завдання лабораторних занять з дисципліни, має дотримуватися політики доброчесності (заборонені списування, плагіат (в т.ч. із використанням мобільних девайсів). У разі виявлення порушення політики академічної доброчесності 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, 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 студентів у семестрі

Оцінювання академічних досягнень здобувача вищої освіти здійснюється відповідно до «Положення про контроль і оцінювання результатів навчання здобувачів вищої освіти у ХНУ». 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.

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. 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 студентів

<table>
<tr><th colspan="8">Аудиторна робота</th><th>Контрольні заходи</th><th>Семестровий контроль</th></tr>
<tr><td colspan="10">III семестр</td></tr>
<tr><td colspan="8">Захист лабораторних робіт</td><td rowspan="2">Тестовий контроль</td><td rowspan="2">Іспит</td><td rowspan="3">Разом балів</td></tr>
<tr><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td></tr>
<tr><td colspan="8">Кількість балів за вид навчальної роботи (мінімум-максимум)</td></tr>
<tr><td>3-5</td><td>3-5</td><td>3-5</td><td>3-5</td><td>3-5</td><td>3-5</td><td>3-5</td><td>3-5</td><td>12-20</td><td>24-40</td><td rowspan="2">60-100*</td></tr>
<tr><td colspan="8">24-40</td><td>12-20</td><td>24-40</td></tr>
<tr><td colspan="10">IV семестр</td></tr>
<tr><td colspan="8">Захист лабораторних робіт</td><td rowspan="2">Тестовий контроль</td><td rowspan="2">Іспит</td><td rowspan="3">Разом балів</td></tr>
<tr><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td></tr>
<tr><td colspan="8">Кількість балів за вид навчальної роботи (мінімум-максимум)</td></tr>
<tr><td>3-5</td><td>3-5</td><td>3-5</td><td>3-5</td><td>3-5</td><td>3-5</td><td>3-5</td><td>3-5</td><td>12-20</td><td>24-40</td><td rowspan="2">60-100*</td></tr>
<tr><td colspan="8">24-40</td><td>12-20</td><td>24-40</td></tr>
<tr><td colspan="10">V семестр</td></tr>
<tr><td colspan="8">Захист лабораторних робіт</td><td rowspan="2">Тестовий контроль</td><td rowspan="2">Іспит</td><td rowspan="3">Разом балів</td></tr>
<tr><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td></tr>
<tr><td colspan="8">Кількість балів за вид навчальної роботи (мінімум-максимум)</td></tr>
<tr><td>3-5</td><td>3-5</td><td>3-5</td><td>3-5</td><td>3-5</td><td>3-5</td><td>3-5</td><td>3-5</td><td>12-20</td><td>24-40</td><td rowspan="2">60-100*</td></tr>
<tr><td colspan="8">24-40</td><td>12-20</td><td>24-40</td></tr>
</table>

Примітки: *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; повнота відповіді.

Результат виконання і захисту здобувачем вищої освіти кожної лабораторної роботи оцінюється відповідно до таблиці **«Критерії оцінювання навчальних досягнень здобувача вищої освіти»** (мінімальний позитивний бал – 3 бали, максимальний – 5 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.

Оцінку, отриману за лабораторну роботу, викладач оголошує студенту одразу після захисту лабораторної роботи і проставляє в електронний журнал дисципліни.

Оцінювання результатів тестового контролю

Кожний з тестів, передбачених Робочою програмою, складається із 20 тестових завдань, кожне з яких є рівнозначним.

Відповідно до таблиці структурування видів робіт за тестовий 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	**0-50**	**60**	**65**	**70**	**75**	**80**	**85**	**90**	**95**	**100**
Кількість отриманих балів	0	12	13	14	15	16	17	18	19	20

На тестування відводиться 20 хвилин. Студент проходить тестування в он-лайн режимі у Модульному середовищі для навчання. Також, студент може проходити тестування письмово, записуючи правильні відповіді у талоні відповідей. 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 як теоретичної, так і практичної підготовки

здобувача з навчальної дисципліни. Складання іспиту відбувається за попередньо розробленими і затвердженими на засіданні кафедри білетами. Відповідно до цього в екзаменаційному білеті пропонується поєднання питань як теоретичного (в т.ч. у тестовій формі), так і практичного характеру.

Таблиця – Оцінювання результатів підсумкового семестрового контролю здобувачів денної форми навчання (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)**
Теоретичне питання № 1	6	8	10
Теоретичне питання № 2	6	8	10
Практичне завдання №1	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)**.

Підсумкова семестрова оцінка за інституційною шкалою і шкалою ЄКТС визначається в автоматизованому режимі після внесення викладачем результатів оцінювання у балах з усіх видів навчальної роботи до електронного журналу. Співвідношення інституційної шкали оцінювання і шкали оцінювання ЄКТС наведені нижче у таблиці «Співвідношення».

Семестровий іспит виставляється, якщо загальна сума балів, яку набрав студент з дисципліни за результатами поточного 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 студентом сумі балів відповідно до таблиці Співвідношення.

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

10. Питання для самоконтролю результатів навчання

Третій семестр

1. Завдання безпеки комп’ютерних мереж. Фізичний захист мереж.
2. Програмні та апаратні засоби захисту мереж.
3. Адміністративні заходи безпеки комп’ютерних мереж.
4. Поняття комп’ютерних мереж.
5. Типи мереж.
6. Апаратні та програмні компоненти комп’ютерних мереж.
7. Мережні топології.
8. Модель OSI.
9. Модель TCP.
10. Мережеві протоколи.
11. Протоколи дротових і бездротових мереж.
12. Стандартні порти.
13. Протоколи WLAN.
14. Протоколи Bluetooth, NFC і RFID.
15. Протоколи Zigbee і Z-Wave.
16. Покоління систем стільникового зв'язку.
17. Мережеві служби.
18. Клієнт-серверна архітектура.
19. DHCP-сервер.
20. DNS сервер.
21. Сервер друку.
22. Файловий сервер.
23. Веб сервер.
24. Поштовий сервер.
25. Проксі сервер.
26. Сервер автентифікації.
27. Syslog сервер.
28. Основні мережеві пристрої.
29. Мережева інтерфейсна карта.
30. Повторювачі, мости та концентратори.
31. Керовані та некеровані комутатори.
32. Бездротові точки доступу.
33. Маршрутизатори.
34. Міжмережеві екрани.
35. Системи виявлення вторгнень IDS.
36. Системи запобігання вторгненням IPS.
37. Пристрої UTM.
38. MAC адреси.
39. IP адреси.
40. Мережеві протоколи. SSL. TSL. SOCS.
41. Безпека мережевих пристроїв
42. Мережеві загрози
43. Нейтралізація мережевих загроз
44. Захист доступу до пристроїв
45. Призначення адміністративних ролей
46. Моніторинг пристроїв і керування ними
47. Використання автоматичних функцій забезпечення безпеки
48. Захист площини управління
49. Технології брандмауера.
50. Списки контролю доступу (ACL).
51. Зональні міжмережеві екрани
52. Автентифікація, авторизація та облік
53. Призначення AAA.

54. Локальна аутентифікація AAA
55. Серверне рішення AAA.
56. Серверна аутентифікація AAA.
57. Серверна авторизація та облік AAA.
58. Автентифікація RADIUS.

Четвертий семестр

1. Безпека локальних та віртуальних приватних мереж (LAN, VPN)
2. Безпека кінцевих пристроїв
3. Фактори безпеки локальної мережі
4. Мережі VPN
5. Протокол IPsec
6. Компоненти мережі IPsec VPN і їх функціонування
7. Реалізація мереж IPsec VPN між двома пунктами за допомогою CLI
8. Системи виявлення та запобігання вторгнень
9. Технології IDS
10. Технології IPS. Сигнатури IPS. Впровадження IPS
11. Пристрої забезпечення безпеки
12. Cisco Adaptive Security Appliance
13. Конфігурація брандмауера ASA
14. Об’єктні групи, списки контролю доступу, NAT на основі ASA
15. Конфігурація ASA VPN
16. Моніторинг мережі
17. Системи керування мережею (NMS)
18. Протокол SNMP
19. Протокол IP SLA
20. Управління безпекою мережею
21. Тестування безпеки мережі
22. Розробка комплексної політики безпеки
23. Класифікація загроз у комп’ютерних мережах
24. Методи аутентифікації користувачів у мережі
25. Механізми контролю доступу (ACL, RBAC, ABAC)
26. Шифрування даних у транспортних протоколах (SSL/TLS, SSH)
27. Протокол RADIUS і його роль у централізованій автентифікації
28. Використання TACACS+ у корпоративних мережах
29. Захист бездротових мереж Wi-Fi (WPA2, WPA3, 802.1X)
30. Архітектура мережевого екрану (Firewall)
31. Типи брандмауерів: фільтрація пакетів, станова, прикладна
32. NAT, PAT та їх роль у забезпеченні безпеки
33. Концепція Zero Trust у корпоративних мережах
34. Використання VLAN для сегментації мережі
35. Методи виявлення аномалій у мережевому трафіку
36. Використання NetFlow, sFlow та IPFIX для моніторингу трафіку
37. Системи збору журналів подій (Syslog, ELK Stack, Graylog)
38. SIEM-системи: принцип роботи та приклади (Splunk, Wazuh, OSSIM)
39. Реагування на інциденти безпеки (Incident Response)
40. Планування резервного копіювання та відновлення після збоїв
41. Захист серверів DNS і виявлення DNS-атак
42. Використання протоколів HTTPS, HSTS, DNSSEC для підвищення безпеки
43. Механізми захисту електронної пошти (SPF, DKIM, DMARC)
44. Архітектура корпоративного проксі-сервера та фільтрація контенту
45. Контроль доступу до вебресурсів і застосування URL-фільтрації
46. Віртуалізація мережевих функцій (NFV) і безпека SDN
47. Контейнеризація сервісів і захист у середовищі Docker/Kubernetes
48. Аудит мережевої інфраструктури
49. Використання Penetration Testing для оцінки безпеки мережі

50. Використання Metasploit Framework для тестування безпеки
51. Аналіз вразливостей із застосуванням OpenVAS, Nessus
52. Захист серверів Linux і Windows Server у корпоративному середовищі
53. Політики оновлень і патч-менеджмент
54. Розмежування прав доступу в Active Directory
55. Безпечна конфігурація комутаторів і маршрутизаторів
56. Механізми захисту від DDoS-атак
57. Захист від MITM, ARP-spoofing та IP-spoofing атак
58. Використання VPN Site-to-Site і Remote Access для захисту каналів
59. Побудова сегментованої безпечної топології корпоративної мережі
60. Практичні засоби контролю мережевої безпеки в середовищі SOC

П'ятий семестр

1. Які основні загрози притаманні безпроводовим мережам?
2. Як класифікуються атаки на безпроводові мережі?
3. У чому полягають особливості пасивних і активних атак на Wi-Fi?
4. Які критерії використовують для оцінки загроз у безпроводових мережах?
5. Основні принципи побудови безпечної безпроводової мережі?
6. Які технології забезпечують автентифікацію в безпроводових мережах?
7. Які підходи застосовують для виявлення вторгнень у безпроводових системах?
8. Які основні методи оцінки ризиків у безпроводових мережах?
9. Які основні категорії загроз для мобільних пристроїв?
10. У чому полягає поняття життєвого циклу рішень із безпеки мобільних пристроїв?
11. Які типові вразливості мають мобільні операційні системи Android та iOS?
12. Які механізми використовуються для централізованого управління мобільними пристроями (MDM)?
13. Які основні загрози реалізуються через мобільні додатки?
14. Як перевіряється захищеність мобільних додатків?
15. Які особливості мають загрози для телекомунікаційних систем 4G і 5G?
16. Які методи використовують для шифрування даних на мобільних пристроях?
17. Які основні архітектурні рівні систем IoT?
18. Які засоби автоматичної ідентифікації використовуються в IoT?
19. У чому полягає принцип роботи технології RFID?
20. Які особливості має технологія Bluetooth Low Energy (BLE)?
21. Які відмінності між технологіями ZigBee, Wi-Fi та LPWAN?
22. У чому полягають основні проблеми безпеки IoT?
23. Які типові вразливості властиві IoT-пристроям?
24. Як забезпечується конфіденційність даних у системах IoT?
25. Яку роль відіграє криптографія в архітектурі безпеки IoT?
26. Яким чином технологія блокчейн може підвищити безпеку IoT?
27. Які види кібератак найчастіше спрямовані на IoT-пристрої?
28. Які вимоги висуваються до фізичної безпеки IoT-пристроїв?
29. Які моделі сервісів використовуються в хмарних обчисленнях (IaaS, PaaS, SaaS)?
30. У чому полягає різниця між приватною, публічною та гібридною хмарою?
31. Які основні елементи архітектури OpenStack?
32. У чому переваги та ризики хмарної інфраструктури для безпеки даних?
33. Що таке туманні обчислення (Fog Computing) і де вони застосовуються?
34. Які функції реалізує архітектура OpenFog RA?
35. Як працює Amazon Greengrass і чим він відрізняється від традиційних хмарних сервісів?
36. Які ключові характеристики визначають технології Big Data?
37. У чому полягає процес Data Science і як він використовується у сфері безпеки?
38. Які загрози притаманні зберіганню великих даних у хмарі?
39. Як створити робоче середовище для аудиту безпеки безпроводових мереж?
40. Які етапи включає процес виявлення та аналізу вразливостей безпроводових мереж?
41. Які методи застосовують для запобігання несанкціонованому доступу до точок Wi-Fi?
42. У чому полягає роль сертифікатів і протоколів EAP у безпеці бездротових мереж?

43. Як виявляються атаки типу Evil Twin у публічних бездротових мережах?
44. Яким чином механізм 802.1X забезпечує автентифікацію користувачів у Wi-Fi?
45. Які параметри сигналу аналізуються під час моніторингу безпеки бездротової мережі?
46. Які існують методи захисту від атак типу деаутентифікації (DeAuth)?
47. Як здійснюється розмежування доступу в гостьових бездротових мережах?
48. Які інструменти використовуються для аудиту безпеки бездротових мереж (наприклад, Aircrack-ng, Kismet)?
49. Як протоколи WPA2-Enterprise та WPA3 підвищують безпеку автентифікації?
50. Які основні відмінності між PSK і Enterprise-режимами бездротових мереж?
51. Як мобільні пристрої визначають безпечні з'єднання під час роумінгу між точками доступу?
52. Які ризики створюють відкриті точки доступу у публічних просторах?
53. Як використання VPN може підвищити рівень захисту у публічних Wi-Fi мережах?
54. Які стандарти визначають вимоги до безпеки мобільних мереж п'ятого покоління?
55. У чому полягає роль SIM-безпеки у мобільних мережах 4G/5G?
56. Які механізми виявлення аномалій використовуються в системах безпеки IoT?
57. Як можна реалізувати ізоляцію сегментів IoT у корпоративній мережі?
58. Які методи автентифікації застосовують для захисту комунікацій між IoT-пристроями?
59. Які ризики виникають при інтеграції IoT-пристроїв у хмарні екосистеми?
60. Які принципи потрібно враховувати під час проектування безпечної інфраструктури IoT?

11. Навчально-методичне забезпечення

Освітній процес з дисципліни «Захист інформації в інформаційно-комунікаційних системах» забезпечений необхідними навчально-методичними матеріалами, що розміщені в Модульному середовищі для навчання MOODLE:

1. Курс «Захист інформації в інформаційно-комунікаційних системах». https://msn.khmnu.edu.ua/course/view.php?id=5910

12. Матеріально-технічне та програмне забезпечення дисципліни (за потреби)

Інформаційна та комп'ютерна підтримка: ПК, планшет, смартфон або інший мобільний пристрій, мультимедійний проєктор. Програмне забезпечення: програми Microsoft Office або аналогічні, доступ до мережі Інтернет.

Спеціальне програмне забезпечення: Cisco Packet Tracer, Wireshark, Putty, Nmap, Kali Linux.

Обладнання: маршрутизатори Cisco 4000 серії, Mikrotik; міжмережеві екрани Cisco ASA, Fortinet; керовані L2,L3 комутатори Cisco Catalyst 2960, D-Link, TP-Link, Mikrotik, Ubiquiti; точки доступу Cisco, Ubiquiti, TP-Link.

13. Рекомендована література

Основна

1. Комп'ютерні мережі : навч. посіб. [Електронний ресурс] / А. В. Чепинога, А. А. Єфіменко, К. С. Рудаков, А. О. Лавданський, Є. В. Ланських, Е. В. Фауре ; М-во освіти і науки України, Черкас. держ. технол. ун-т, Державний університет «Житомирська політехніка». – Житомир : Державний університет «Житомирська політехніка», 2025. – 386 с.
2. Комп'ютерні мережі: [Книга 1. Технології комп'ютерних мереж] : навчальний посібник / С. П. Євсеєв, Н. В. Дженюк, М. Ю. Толкачов та ін. – Харків, – Львів : «Новий Світ – 2000», 2025. – 471 с.
3. Комплексна безпека інформаційних мережевих систем: навчальний посібник для студентів спеціальності 174 «Автоматизація, комп'ютерно-інтегровані технології та робототехніка» / Укладачі: А.Г. Микитишин, М.М. Митник, О.С. Голотенко, В.В. Карташов. – Тернопіль : ФОП Паляниця В.А., 2023. – 324 с.
4. Технології забезпечення безпеки мережевої інфраструктури/ В. Л. Бурячок, А. О. Аносов, В. В. Семко, В. Ю. Соколов, П. М. Складанний. – К.: КУБГ, 2019. – 218 с.
5. Інформаційна безпека: навч. посібник / Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник, А. П. Бондарєв, С. С. Войтусік, А. Я. Горпенюк, О. А. Нємкова, І. М. Журавель, Б. М. Березюк, Є. І. Яковенко, В. І. Отенко, І. Я. Тишик; за заг. ред. д-ра техн. наук, проф. Ю. Я. Бобала та д-ра техн. наук, доц. І. В. Горбатого. – Львів: Видавництво Львівської політехніки, 2019. – 580 с.

6. Основи кібербезпеки: Безпека бездротових та мобільних технологій / Іваненко О.П., Коваленко М.С. – Київ: Національний технічний університет України, 2022. – 240 с.
7. Мобільні мережі та бездротові комунікації: Теорія та практика захисту / Петров В.Л., Гончаренко Т.М. – Харків: Харківський національний університет радіоелектроніки, 2023. – 210 с.
8. Безпека інтернету промов: Лісовенко О.Г., Шевченко І.М. – Львів: Львівська політехніка, 2023. – 180 с.
9. Кібербезпека мобільних пристроїв та додатків / Дмитрук Н.С., Павленко Р.В. – Одеса: Одеський національний університет імені І.І. Мечникова, 2022. - 230 с.
10. Основи захисту даних у бездротових мережах / Козлов А.П., Ткаченко О.В. – Дніпро: Дніпровський національний університет імені Олеся Гончара, 2022. – 200 с.
11. Захист інформації в мережах Wi-Fi: сучасні методи та засоби / Михайленко В.С., Зубарєв І.В. – Київ: Київський політехнічний інститут, 2022. – 220 с.

Додаткова

12. Wireless Communication Security / (eds.) M. H. Afify, A. M. Eltawil – Hoboken: Wiley, 2023. - 288 с.
13. Internet of Things Security and Privacy: Practical and Management Perspectives / Ali Ismail Awad, Atif Ahmad, Kim-Kwang Raymond Choo, Saqib Hakak (eds.) – London: CRC Press (Routledge), 2024. - 258 с.
14. Holistic IoT Security, Privacy and Safety: Integrated Approaches Protecting a Highly Connected World / Konstantinos Loupos (ed.) – Boston / Delft: Now Publishers, 2025.
15. Secure Communication in Internet of Things: Emerging Technologies, Challenges, and Mitigation / T. Kavitha, M.K. Sandhya, V.J. Subashini, Prasidh Srikanth (eds.) – Boca Raton: CRC Press, 2024. - 338 с.
16. Security in IoT: The Changing Perspective / Rituparna Chaki, Debdutta Barman Roy (eds.) – London: Taylor & Francis / CRC Press, 2024. - 136 с.
17. Firmware Security Playbook: 2025 Edition – Practical Checklists, Tools and Templates for IoT & Embedded Systems Security / (compilation) – Independently published / practitioner guide, 2025. - 200 с.

14. Інформаційні ресурси

1. Модульне середовище для навчання. URL : https://msn.khmnu.edu.ua/course/view.php?id=5910
2. Електронна бібліотека ХНУ. URL: https://library.khmnu.edu.ua/
3. Інституційний репозитарій ХНУ. URL : https://elar.khmnu.edu.ua

Захист інформації в інформаційно-комунікаційних системах

Тип дисципліни	Обов'язкова
Освітній рівень	Перший (бакалаврський)
Мова викладання	Українська
Семестр	Третій-п'ятий
Кредити ЄКТС	15
Форми навчання, для яких викладається дисципліна	Денна

Результати навчання. Після вивчення дисципліни студент повинен: знати принципи побудови та функціонування інформаційно-комунікаційних систем, методи організації захисту даних на рівнях мережевих протоколів, обладнання та сервісів; застосовувати знання і навички з проектування, налаштування та адміністрування мереж із забезпеченням безпеки передавання інформації; діяти на основі технічних вимог і стандартів інформаційної безпеки під час реалізації систем виявлення вторгнень, контролю доступу та фільтрації трафіку; організовувати процеси моніторингу та управління безпечним функціонуванням мережевої інфраструктури; впроваджувати методи аналізу, класифікації та реагування на аномальну мережеву активність; володіти знаннями сучасних засобів захисту, шифрування, сегментації трафіку, виявлення та усунення вразливостей; бути здатним проводити технічну оцінку стану інформаційної безпеки мережевих систем і приймати рішення щодо відновлення їх працездатності після інцидентів; аналізувати, аргументувати, приймати рішення при вирішенні складних задач захисту мережевої інфраструктури; застосовувати знання сучасних методів і технологій моніторингу та управління інформаційними потоками, а також використовувати технічну термінологію англійською мовою для забезпечення ефективної професійної комунікації у сфері інформаційної та кібербезпеки.

Зміст навчальної дисципліни: Комп'ютерні мережі. Типи та топології мереж. Апаратне й програмне забезпечення. Моделі OSI та TCP/IP. Мережеві протоколи дротових і бездротових систем. WLAN. Засоби та методи захисту мереж. Комутатори. Маршрутизатори. Міжмережеві екрани. Системи IDS/IPS. Моніторинг і керування мережевими пристроями. Технології брандмауера та ACL. AAA і RADIUS. VPN і IPsec. Безпека IoT. Конфіденційність у безпроводових мережах. Аналіз загроз і атак. Методи оцінки ризиків. Безпека хмарних і мобільних технологій. Управління даними та ідентифікацією. Вразливості Wi-Fi і мобільних систем.

Пререквізити: ОПП.02 Операційні системи та технології їх захисту; ОПП.05 Сигнали і процеси в системах захисту інформації.

Кореквізити: ОПП.11 Адміністрування та захист баз і сховищ даних; ОПП.12 Технології виявлення вразливостей та вторгнень; ОПП.14 Комплексні системи захисту інформації; ОПП.15 Виробнича практика 1; ОПП.16 Виробнича практика 2.

Запланована навчальна діяльність: лекцій 64 год., лабораторних занять 102 год., самостійної роботи 284 год., разом 450 год.

Форми (методи) навчання: лекції (з використанням словесних, наочних, інтерактивних та проблемних методів); лабораторні роботи (з використанням практичних та частково-пошукових методів); самостійна робота (з використанням пояснювально-ілюстративних та частково-пошукових методів).

Форми оцінювання результатів навчання: оцінювання результатів захисту лабораторних робіт;тестування.).

Вид семестрового контролю: іспит 1-3 семестри. Курсовий проект 2 семестр

Навчальні ресурси:

1. Комп'ютерні мережі : навч. посіб. [Електронний ресурс] / А. В. Чепинога, А. А. Єфіменко, К. С. Рудаков, А. О. Лавданський, Є. В. Ланських, Е. В. Фауре ; М-во освіти і науки України, Черкас. держ. технол. ун-т, Державний університет «Житомирська політехніка». – Житомир : Державний університет «Житомирська політехніка», 2025. – 386 с.
2. Комп'ютерні мережі: [Книга 1. Технології комп'ютерних мереж] : навчальний посібник / С. П. Євсеєв, Н. В. Дженюк, М. Ю. Толкачов та ін. – Харків, – Львів : «Новий Світ – 2000», 2025. – 471с.
3. Комплексна безпека інформаційних мережевих систем: навчальний посібник для студентів спеціальності 174 «Автоматизація, комп'ютерно-інтегровані технології та робототехніка» / Укладачі: А.Г. Микитишин, М.М. Митник, О.С. Голотенко, В.В. Карташов. – Тернопіль : ФОП Паляниця В.А., 2023. – 324 с.
4. Технології забезпечення безпеки мережевої інфраструктури/ В. Л. Бурячок, А. О. Аносов, В. В. Семко, В. Ю. Соколов, П. М. Складанний. – К.: КУБГ, 2019. – 218 с.
5. Інформаційна безпека: навч. посібник / Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник, А. П. Бондарєв, С. С. Войтусік, А. Я. Горпенюк, О. А. Нємкова, І. М. Журавель, Б. М. Березюк, Є. І. Яковенко, В. І. Отенко, І. Я. Тишик; за заг. ред. д-ра техн. наук, проф. Ю. Я. Бобала та д-ра техн. наук, доц. І. В. Горбатого. – Львів: Видавництво Львівської політехніки, 2019. – 580 с.
6. Основи кібербезпеки: Безпека бездротових та мобільних технологій / Іваненко О.П., Коваленко М.С. – Київ: Національний технічний університет України, 2022. – 240 с.
7. Мобільні мережі та бездротові комунікації: Теорія та практика захисту / Петров В.Л., Гончаренко Т.М. – Харків: Харківський національний університет радіоелектроніки, 2023. – 210 с.
8. Безпека інтернету промов: Лісовенко О.Г., Шевченко І.М. – Львів: Львівська політехніка, 2023. – 180 с.
9. Кібербезпека мобільних пристроїв та додатків / Дмитрук Н.С., Павленко Р.В. – Одеса: Одеський національний університет імені І.І. Мечникова, 2022. - 230 с.
10. Основи захисту даних у бездротових мережах / Козлов А.П., Ткаченко О.В. – Дніпро: Дніпровський національний університет імені Олеся Гончара, 2022. – 200 с.
11. Захист інформації в мережах Wi-Fi: сучасні методи та засоби / Михайленко В.С., Зубарєв І.В. – Київ: Київський політехнічний інститут, 2022. – 220 с.

Викладачі: канд. техн. наук, доц. Кльоц Ю.П., д-р філософії, ст. викл. Стецюк М.В.