ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ЗАТВЕРДЖУЮ

Декан факультету інформаційних технологій

_____ Тетяна ГОВОРУЩЕНКО
Підпис Ім'я, ПРІЗВИЩЕ

29 серпня 2025 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Основи інформаційної безпеки

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.01
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	1	1	7	210	66	16	34	16		144			+	
Д	1	2	6	180	66	32	34			114			+	
Разом ДФН			**13**	**390**	**132**	**48**	**68**	**16**		**258**			**2**	

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

Робоча програма складена _____ д-р філософії Наталія ПЕТЛЯК
Підпис(и) автора(ів) Науковий ступінь, учене 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 «Основи інформаційної безпеки» 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*;** вихідна.

***Постреквізити**;* ОФП.02 Математичні основи захисту інформації, ОФП.05 Захист інформації в інформаційно-комунікаційних системах, ОФП.06 Захист інформації в інформаційно-комунікаційних системах (курсовий проєкт), ОФП.08 Нормативно-правове забезпечення кібербезпеки

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; ЗК08 Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя; 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;

***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; ПРН06 Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат; ПРН07 Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення і передачі сигналів тощо, принципи, методи, поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності; 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; 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.

Мета дисципліни. Формування термінологічного фундаменту, знань та розуміння предметної області; ознайомлення студентів із основними методами, принципами та алгоритмами захисту інформації в інформаційних системах, забезпечення здатності студентів визначати загрози безпеці інформації в сучасних операційних системах, обґрунтовано обирати і грамотно налаштовувати засоби захисту в сучасних операційних системах.

Предмет дисципліни. Основи забезпечення інформаційної та кібербезпеки, основні методи та алгоритми захисту інформації в сучасних операційних системах, методи та засоби управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в операційних системах.

Завдання дисципліни. Формування практичних навичок використання базових методів і засобів інформаційної безпеки для забезпечення захисту даних в операційних системах та інформаційно-комунікаційних мережах, набуття досвіду виявлення та аналізу загроз, застосування програмно-апаратних комплексів захисту, а також розвиток аналітичного та критичного мислення у процесі розв'язання типових задач у сфері кібербезпеки та захисту інформації.

Результати навчання. Після вивчення дисципліни студент повинен: *виявляти* загальні знання та розуміння предметної області та розуміння професійної діяльності; *застосовувати* й адаптувати принципи, методи, поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності; *мати* базові знання та практичні навички з використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах; *використовувати* інформаційно-комунікаційних технології, базові знання сучасних методів і моделей інформаційної безпеки та/або кібербезпеки, теорії та методів захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем; *обирати* і *використовувати* методи та способи розв'язання спеціалізованих задач і практичних проблем у професійній діяльності; вирішувати базові задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження; *застосовувати* принципи, методи, поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності; *адаптуватися* до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.

4. Структура залікових кредитів дисципліни

Назва розділу (теми)	Кількість годин, відведених на:			
	лекції	лабораторні роботи	практичні заняття	СРС
	Перший семестр			
Тема 1. Основи інформаційної безпеки	6	4	10	51
Тема 2. Архітектура комп'ютерів	2	4	2	17
Тема 3. Безпека мереж	2	4	2	23
Тема 4. Особливості застосування інформаційної безпеки	6	22	2	53
Разом за 1-й семестр:	**16**	**34**	**16**	**144**
	Другий семестр			
Тема 5. Призначення, функції та архітектури операційних систем	14	12	-	43
Тема 6. Реалізація безпеки в операційній системі Windows	10	16	-	47
Тема 7. Реалізація безпеки в операційній системі Linux	4	6	-	14
Тема 8. Реалізація безпеки в мобільних операційних системах	4		-	10
Разом за 2-й семестр:	**32**	**34**	**-**	**114**

5. Програма навчальної дисципліни

5.1 Зміст лекційного курсу

Номер лекції	Перелік тем лекцій, їх анотації	Кількість годин
	Перший семестр	
	Тема 1. Основи інформаційної безпеки	**6**
1	**Загальні основи інформаційної безпеки** Основні поняття та стандарти інформаційної безпеки. Класифікація загроз інформаційної безпеки. Основні характеристики інформації Літ.: [1] с.10-81; [4] с.63-89; [5] с.22-89.	2
2	**Основні принципи кібербезпеки** Принципи кібербезпеки і приватності. Знання основних правил кібергігієни. Літ.: [1] с.84-107.	2
3	**Безпечне використання корпоративних систем обміну повідомленнями** Корпоративні системи обміну повідомленнями і відповідне програмне забезпечення. Вміння ними безпечно користуватися та адмініструвати їх. Літ.: [5] с.293-302.	2
	Тема 2. Архітектура комп'ютерів	**2**
4	**Архітектура комп'ютерів** Архітектура комп'ютерів (друковані плати, мікросхеми, процесори, елементи пам'яті тощо). Типи комп'ютерних архітектур. Літ.: [1] с.230-236; [5] с.182-187.	2
	Тема 3. Безпека мереж	**2**
5	**Комп'ютерні мережі** Принципи обміну інформацією в мережах. Мережа ETHERNET, типи мережевих пристроїв та їх призначення. Типи мереж. Мережева модель OSI. Основні протоколи стеку TCP/IP. Літ.: [1] с.197-225; [5] с.126-148.	2

	Тема 4. Особливості застосування інформаційної безпеки	**6**
6	**Основи безпеки даних в комп'ютерних системах** Основні поняття щодо захисту інформації в автоматизованих системах. Загрози безпеки даних та їх особливості. Канали проникнення та принципи побудови систем захисту. Основи фізичного захисту об'єктів. Літ.: [5] с.262-283.	2
7	**Забезпечення інформаційної безпеки у соціальних інтернет-сервісах** Поняття соціальних інтернет-сервісів (СІС). Вплив СІС на психіку користувачів. СІС як засіб проведення інформаційних операцій проти людини, суспільства, держави. Протидія впливу СІС. Літ.: [12] с.500-547.	2
8	**Підходи до автентифікації та авторизації користувачів в інформаційних системах** Поняття автентифікації та авторизації. Типи автентифікації. Переваги та недоліки різних методів. Літ.: [2] с.53-60; [12] с.272-278.	2
	Разом за 1-й семестр:	**16**
	Другий семестр	
	Тема 5. Призначення, функції та архітектури операційних систем	**14**
1	**Поняття операційної системи** Призначення та функції операційних систем. Класифікація сучасних операційних систем. Технології проектування. Архітектурні особливості будови сучасних операційних систем. Операційні системи Windows, Unix і Linux - архітектура та порівняльний аналіз. Літ.: [3] с.8-22.	2
2	**Ядро операційної системи** Складові частини ядра ОС. Підходи до проектування ядра. Багаторівневі системи. Змішані системи. Літ.: [14] с.86-105	2
3	**Процеси в операційних системах** Процеси в операційних системах. Основні відомості про процеси. Управління процесами. Взаємодія процесів. Планування. Синхронізація. Тупики. Літ.: [3] с.27-41; [5] с.187-196, [10] с.36-73.	2
4	**Потоки в операційних системах** Потоки в операційних системах. Основні операції з потоками. Способи реалізації. Стани потоків. Літ.: [3] с.41-53; [5] с.187-196, [10] с.73-84.	2
5	**Керування пам'яттю в операційних системах** Керування пам'яттю в операційних системах. Функції операційної системи по керуванню пам’яттю. Технології розподілу пам’яті. Віртуальна пам’ять. Організація пам’яті. Сегментація. Алгоритм запису. Літ.: [3] с.66-82; [5] с.196-202, [10] с.84-105.	2
6	**Файлові системи операційних систем** Файлова система NTFS. Архітектура файлової системи EFS. Файлові системи exFAT, Ext4, BtrFS, ReiserFS, XFS, JFS. RAID-масиви. Літ.: [3] с.82-94; [5] с.202-204, [10] с.105-123.	2
7	**Технології віртуалізації** Технології віртуалізації. Віртуалізація операційних систем. Віртуалізація програмного забезпечення. Віртуалізація інфраструктури. Віртуалізація віддалених робочих столів. Віртуалізація систем зберігання даних. Віртуалізація мережі. Літ.: [1] с.225-236; [3] с.116-125.	2
	Тема 6. Реалізація безпеки в операційній системі Windows	**10**
8	**Сутність проблеми захисту операційних систем** Вимоги, що висуваються до захищених операційних систем. Поняття та призначення політики інформаційної безпеки. Порушення політики інформаційної безпеки. Атаки на рівні операційної системи. Літ.: [12] с.11-39; [2] с.23-60; [6] с.593-602.	2
9	**Технології боротьби з вірусами в операційних системах** Найпоширеніші загрози безпеці операційних систем. Несанкціонований доступ. Незаконне використання привілеїв. Атаки типу: "салямі", "приховані канали", "маскарад", "збір сміття" та "злам системи". Шкідливе програмне забезпечення. Ознаки інфікованої операційної системи. Технології виявлення вірусів. Класифікація антивірусного програмного забезпечення. Літ.: [1] с.817-931.	2
10	**Організація безпеки операційної системи Windows** Компоненти системи захисту операційної системи Windows. Механізм захисту об’єктів операційної системи Windows. Ідентифікатор захисту. Маркери доступу. Дескриптори	2

	захисту. Права та привілеї (суперпривілеї) облікових записів. Типові права користувачів ОС Windows. Аудит. Літ.: [6] с.966-975.	
11	**Конфігурація та моніторинг операційної системи Windows** Запуск від імені адміністратора, локальні користувачі та домени. CLI і PowerShell. Інструмент керування Windows, диспетчер завдань і монітор ресурсів. Літ.: [15]	2
12	**Політики безпеки операційної системи Windows** Політики облікових записів. Локальні політики. Монітор брандмауера для програми Windows Defender. Політика диспетчера списку мереж. Політика відкритого ключа. Політика управління додатками. Політика IP-безпеки на «Локальний комп'ютер». Конфігурація розширеної політики аудиту. Літ.: [16-18]	2
	Тема 7. Реалізація безпеки в операційній системі Linux	**4**
13	**Організація безпеки операційної системи Linux** Модель безпеки операційної системи Linux. Підсистема ідентифікації та аутентифікації. Підсистема розмежування доступу. Монітор безпеки. Літ.: [7] с.96-120, [8] с.75-84.	2
14	**Технології підвищення рівня захищеності операційної системи Linux** Linux з покращеним рівнем безпеки (SELinux). Система мандатного контролю доступу AppArmor. Система забезпечення мандатного контролю доступу TOMOYO Linux. Резервування в ОС Linux. Процеси та форки. Руткіт. Літ.: [7] с.146-163, [8] с.61-75.	2
	Тема 8. Реалізація безпеки в мобільних операційних системах	**4**
15	**Організація безпеки операційної системи Android** Модель безпеки операційної системи Android. Ідентифікації та аутентифікації. Розмежування доступу. Стандартні та спеціальні дозволи. Літ.: [10] с.30-36.	2
16	**Організація безпеки операційної системи iOS** Архітектура операційної системи iOS. Модель безпеки операційної системи iOS. Характеристика функціонування компонентів Secure Enclave та TouchID. Літ.: [11] с.54-58.	2
	Разом за 2-й семестр	**32**

5.2 Зміст практичних занять

№ з/п	Тема практичного заняття	Кількість годин
	Перший семестр	
	Тема 1. Основи інформаційної безпеки	**10**
1	Методика підготовки звітів і дотримання стандартів оформлення Літ.: [32]	2
2	Оформлення звітної документації згідно з нормативними вимогами Літ.: [32]	2
3	Кодування та шифрування даних як основа інформаційної безпеки Літ.: [21]	2
4	Кодування та шифрування даних як основа інформаційної безпеки (продовження) Літ.: [21]	2
5	Розробка політики інформаційної безпеки підприємства Літ.: [5] с.517-547.	2
	Тема 2. Архітектура комп'ютерів	**2**
6	Вивчення апаратної архітектури ПК та принципів взаємодії компонентів Літ.: [1] с.230-236.	2
	Тема 3. Безпека мереж	**4**
7	Монтаж локальної мережі з використанням SOHO-обладнання Літ.: [33] с.69-114, [34]	2
8	Налаштування локальної мережі з використанням SOHO-обладнання Літ.: [33] с.114-143	2
	Разом за 1-й семестр	**16**

5.2 Зміст лабораторних робіт

№ з/п	Тема лабораторної роботи	Кількість годин
	Перший семестр	
	Тема 1. Основи інформаційної безпеки	**4**
1	Використання корпоративних систем обміну повідомленнями. Літ.: [19-20]	4
	Тема 2. Архітектура комп'ютерів	**4**
2	Встановлення віртуальних машин та операційних систем Windows та Linux, інтеграція та оптимізація компонентів системи. Літ.: [23]	4
	Тема 3. Безпека мереж	**4**
3	Організація безпеки мереж на основі SOHO-маршрутизаторів Літ.: [31]	4
	Тема 4. Особливості застосування інформаційної безпеки	**20**
4	Протидія шкідливому програмному забезпеченню в операційній системі Windows. Літ.: [1] с.817-931	4
5	Розмежування прав доступу в операційній системі Windows. Права доступу до файлів і керування ними Літ.: [16-18]	4
6	Розмежування прав доступу в операційній системі Linux. Права доступу до файлів і керування ними Літ.: [26]	4
7	Відновлення та резервування даних. Літ.: [29]	4
8	Робота із соціальними інтернет-сервісами та інструменти виявлення неправдивих повідомлень. Літ.: [22]	4
9	Підсумкове заняття	**2**
	Разом за 1-й семестр	**34**
	Другий семестр	
	Тема 5. Призначення, функції та архітектури операційних систем	**12**
1	Системні функції роботи з процесами та віртуальною пам'яттю операційної системи Windows Літ.: [3] с.66-82; [5] с.196-202, [10] с.84-105.	4
2	Шифрування файлів в файловій системі NTFS. Літ.: [30]	4
3	Дослідження технології захисту цілісності даних Raid Літ.: [24]	4
	Тема 6. Реалізація безпеки в операційній системі Windows	**16**
4	Знайомство та базові операції з Power Shell Літ.: [11] с.17-30.	4
5	Політики безпеки Windows Літ.: [16-18]	4
6	Управління ресурсами та безпекою в середовищі Windows Server Літ.: [28] с.8-34.	4
7	Розгортання та управління службами Active Directory Літ.: [28] с.34-69	4
	Тема 7. Реалізація безпеки в операційній системі Linux	**4**
8	Налаштування аудиту в Linux Літ.: [27]	4
9	Підсумкове заняття	2
	Разом за 2-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, підготовці до практичних занять, тестування тощо. Керівництво самостійною роботою здійснюється викладачем згідно з розкладом консультацій у позаурочний час. Крім цього до послуг студентів сторінка навчальної дисципліни у Модульному середовищі для навчання, де розміщені Робоча програма дисципліни та необхідні документи з її навчально-методичного забезпечення.

Номер тижня	Вид самостійної роботи	Кількість годин
	Перший семестр	
1	Опрацювання теоретичного матеріалу з Т №1. Підготовка до виконання ЛР №1.	8
2	Опрацювання теоретичного матеріалу з Т №1. Підготовка до ПЗ №1.	8
3	Опрацювання теоретичного матеріалу з Т №1. Підготовка до захисту ЛР №1. Підготовка до виконання ЛР №2.	8
4	Опрацювання теоретичного матеріалу з Т №1. Підготовка до ПЗ №2.	8
5	Опрацювання теоретичного матеріалу з Т №1. Підготовка до захисту ЛР №2. Підготовка до виконання ЛР №3.	9
6	Опрацювання теоретичного матеріалу з Т №1. Підготовка до ПЗ №3.	9
7	Опрацювання теоретичного матеріалу з Т №2. Підготовка до захисту ЛР №3. Підготовка до виконання ЛР №4.	9
8	Опрацювання теоретичного матеріалу з Т №2. Підготовка до ПЗ №4.	9
9	Опрацювання теоретичного матеріалу з Т №3. Підготовка до захисту ЛР №4. Підготовка до виконання ЛР №5.	9
10	Опрацювання теоретичного матеріалу з Т №3. Підготовка до ПЗ №5.	9
11	Опрацювання теоретичного матеріалу з Т №4. Підготовка до захисту ЛР №5. Підготовка до виконання ЛР №6.	9
12	Опрацювання теоретичного матеріалу з Т №4. Підготовка до ПЗ №6.	9
13	Опрацювання теоретичного матеріалу з Т №4. Підготовка до захисту ЛР №6. Підготовка до виконання ЛР №7.	9
14	Опрацювання теоретичного матеріалу з Т №4. Підготовка до ПЗ №7.	9
15	Опрацювання теоретичного матеріалу з Т №4. Підготовка до захисту ЛР №7. Підготовка до виконання ЛР №8.	9
16	Опрацювання теоретичного матеріалу з Т №4. Підготовка до ПЗ №8.	9
17	Опрацювання теоретичного матеріалу з Т №4, тестування. Підготовка до захисту ЛР №8.	4
	Разом 1-й семестр:	**144**
	Другий семестр	
1-2	Опрацювання теоретичного матеріалу з Т №5. Підготовка до виконання ЛР №1.	13
3-4	Опрацювання теоретичного матеріалу з Т №5. Підготовка до захисту ЛР №1. Підготовка до виконання ЛР №2.	13
5-6	Опрацювання теоретичного матеріалу з Т №5. Підготовка до захисту ЛР №2. Підготовка до виконання ЛР №3.	14
7-8	Опрацювання теоретичного матеріалу з Т №5. Підготовка до захисту ЛР №3. Підготовка до виконання ЛР №4.	14
9-10	Опрацювання теоретичного матеріалу з Т №6. Підготовка до захисту ЛР №4. Підготовка до виконання ЛР №5.	14
11-12	Опрацювання теоретичного матеріалу з Т №6. Підготовка до захисту ЛР №5. Підготовка до виконання ЛР №6.	14
13-14	Опрацювання теоретичного матеріалу з Т №7. Підготовка до захисту ЛР №6. Підготовка до виконання ЛР №7.	14
15-16	Опрацювання теоретичного матеріалу з Т №8. Підготовка до захисту ЛР №7. Підготовка до виконання ЛР №8.	14
17	Опрацювання теоретичного матеріалу з Т №8, тестування. Підготовка до захисту ЛР №8.	4
	Разом 2-й семестр:	**114**

***Примітки*:** Т – тема навчальної дисципліни, ПЗ – практичне заняття, ЛР – лабораторна робота.

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; практичні заняття – з використанням практичних методів; 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 аудиторних практичних та 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 роботи на практичних заняттях (опитування теоретичного матеріалу, участь у обговоренні ситуацій);

– оцінювання результатів захисту лабораторних робіт;

– тестовий контроль засвоєння теоретичного та практичного матеріалу.

Підсумкова семестрова оцінка виставляється за результатами поточного контролю. Здобувач вищої освіти, який набрав з будь-якого виду навчальної роботи, суму балів нижчу за 60 відсотків від максимального балу, 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 практичних занять та лабораторних робіт (вивчення теоретичного матеріалу з теми), активно працювати на занятті, розв'язувати задачі, брати участь у дискусіях щодо прийнятих рішень при виконанні здобувачами задач тощо.

Здобувачі вищої освіти мають дотримуватися встановлених термінів виконання всіх видів навчальної роботи відповідно до робочої програми навчальної дисципліни. Термін захисту лабораторної роботи вважається своєчасним, якщо студент захистив її на наступному після виконання роботи занятті. Пропущене практичне заняття чи лабораторну роботу 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 практичних занять, захисту лабораторних робіт та тестування.

Здобувач вищої освіти, виконуючи завдання практичних і 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 (наприклад https://www.netacad.com, https://prometheus.org.ua/, https://osvita.diia.gov.ua/), які сприяють формуванню 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 і володіння спеціальними 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 студентів

<table>
<tr><th colspan="16">Аудиторна робота</th><th>Самостійна робота</th><th>Семестровий контроль</th></tr>
<tr><td colspan="18">Перший семестр</td></tr>
<tr><td colspan="8">Захист лабораторних робіт</td><td colspan="8">Практичні заняття</td><td>Тестовий контроль</td><td>Залік</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><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>Т1-4</td><td rowspan="4">За рейтингом</td></tr>
<tr><td colspan="16">Кількість балів за вид навчальної роботи (мінімум-максимум)</td><td></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>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></tr>
<tr><td colspan="8">24-40</td><td colspan="8">24-40</td><td>12-20</td></tr>
<tr><td colspan="18">Другий семестр</td></tr>
<tr><td colspan="16">Захист лабораторних робіт</td><td>Тестовий контроль</td><td>Залік</td></tr>
<tr><td colspan="2">9</td><td colspan="2">10</td><td colspan="2">11</td><td colspan="2">12</td><td colspan="2">13</td><td colspan="2">14</td><td colspan="2">15</td><td colspan="2">16</td><td>Т5-8</td><td rowspan="4">За рейтингом</td></tr>
<tr><td colspan="16">Кількість балів за вид навчальної роботи (мінімум-максимум)</td><td></td></tr>
<tr><td colspan="2">6-10</td><td colspan="2">6-10</td><td colspan="2">6-10</td><td colspan="2">6-10</td><td colspan="2">6-10</td><td colspan="2">6-10</td><td colspan="2">6-10</td><td colspan="2">6-10</td><td>12-20</td></tr>
<tr><td colspan="16">48-80</td><td>12-20</td></tr>
</table>

Оцінювання на практичних заняттях

Оцінка, яка виставляється за практичне заняття, складається з таких елементів: усне опитування студентів на знання теоретичного матеріалу з теми; вільне володіння студентом термінологією і уміння професійно обґрунтувати прийняті рішення при розв'язуванні задач.

При оцінюванні практичного заняття викладач керується узагальненими критеріями, наведеними у таблиці «**Критерії оцінювання навчальних досягнень здобувача вищої освіти**» (мінімальний позитивний бал – 3 бали, максимальний – 5 балів).

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 Критеріїв оцінювання навчальних досягнень здобувача вищої освіти.

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.

При оцінюванні лабораторних робіт викладач керується узагальненими критеріями, наведеними у таблиці «**Критерії оцінювання навчальних досягнень здобувача вищої освіти**» (мінімальний позитивний бал – 3 бали, максимальний – 5 балів для 1 семестру та мінімальний позитивний бал – 6 балів, максимально – 10 балів для 2 семестру).

Оцінювання результатів тестового контролю

Кожний з тестів, передбачених Робочою програмою, складається із 50 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	0-29	30-31	32-33	34-36	37-38	39-41	42-43	44-46	47-48	49-50
Відсоток правильних відповідей	0-58	60-62	64-66	68-72	74-76	78-82	84-86	88-92	94-96	98-100
Кількість балів	0	12	13	14	15	16	17	18	19	20

На тестування відводиться 60 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.

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 залік виставляється на останньому занятті за умови якщо загальна сума балів, яку накопичив здобувач з дисципліни (іншого освітнього компонента) за результатами ***поточного*** контролю, знаходиться у межах від 60 до 100 балів. При цьому за інституційною шкалою ставиться оцінка «***зараховано***», а за шкалою ЄКТС – буквене позначення оцінки, що відповідає набраній студентом сумі балів відповідно до таблиці Співвідношення. Присутність здобувача у цьому випадку не є обов'язковою.

Таблиця – Співвідношення інституційної шкали оцінювання і шкали оцінювання ЄКТС

<table>
<tr><th rowspan="2">Оцінка ЄКТС</th><th rowspan="2">Рейтингова шкала балів</th><th colspan="2">Інституційна оцінка (рівень досягнення здобувачем вищої освіти запланованих результатів навчання з навчальної дисципліни)</th></tr>
<tr><th>Залік</th><th>Іспит/диференційований залік</th></tr>
<tr><td>A</td><td>90-100</td><td rowspan="5">Зараховано</td><td>Відмінно/Excellent – високий рівень досягнення запланованих результатів навчання з навчальної дисципліни, що свідчить про безумовну готовність здобувача до подальшого навчання та/або професійної діяльності за фахом</td></tr>
<tr><td>B</td><td>83-89</td><td rowspan="3">Добре/Good – середній (максимально достатній) рівень досягнення запланованих результатів навчання з навчальної дисципліни та готовності до подальшого навчання та/або професійної діяльності за фахом

Задовільно/Satisfactory – Наявні мінімально достатні для подальшого навчання та/або професійної діяльності за фахом результати навчання з навчальної дисципліни</td></tr>
<tr><td>C</td><td>73-82</td></tr>
<tr><td>D</td><td>66-72</td></tr>
<tr><td>E</td><td>60-65</td></tr>
<tr><td>FX</td><td>40-59</td><td rowspan="2">Незараховано</td><td>Незадовільно/Fail – Низка запланованих результатів навчання з навчальної дисципліни відсутня. Рівень набутих результатів навчання є недостатнім для подальшого навчання та/або професійної діяльності за фахом</td></tr>
<tr><td>F</td><td>0-39</td><td>Незадовільно/Fail – Результати навчання відсутні</td></tr>
</table>

10. Питання для самоконтролю результатів навчання

Перший семестр

1. Способи подання інформації.
2. Основні характеристики інформації.
3. Основні принципи кібербезпеки.
4. Правила кібергігієни.
5. Корпоративні системи обміну повідомленнями (чати та інші) і відповідне програмне забезпечення.
6. Адміністрування корпоративних систем обміну повідомленнями
7. Системи числення.
8. Архітектура комп’ютерів.
9. Типи комп’ютерних архітектур.
10. Комп'ютерні мережі.
11. Мережева модель OSI
12. Основні протоколи стеку TCP/IP
13. Зміст і основні поняття комп'ютерної безпеки
14. Основні поняття та стандарти інформаційної безпеки.
15. Класифікація загроз інформаційної безпеки.
16. Основні характеристики інформації.
17. Інформація як об’єкт посягань і захисту
18. Основні поняття щодо захисту інформації в автоматизованих системах.
19. Загрози безпеки даних та їх особливості.
20. Захист даних від комп'ютерних вірусів.
21. Шкідливі програми на ЕОМ.
22. Засоби захисту від комп'ютерних вірусів та їх особливості.
23. Вбудовані засоби операційних систем для захисту даних
24. Відновлення та резервування даних
25. Поняття соціальних інтернет-сервісів (СІС).
26. Вплив СІС на психіку користувачів.
27. СІС як засіб проведення інформаційних операцій проти людини, суспільства, держави.
28. Протидія впливу СІС.

Другий семестр

1. Призначення та функції.
2. Класифікація сучасних операційних систем.
3. Тенденції в розвитку ОС.
4. Технології проектування.
5. Основні поняття концепції операційної системи.
6. Архітектурні особливості будови сучасних операційних систем.
7. Операційні системи Windows, Unix і Linux - архітектура та порівняльний аналіз.
8. Складові частини ядра.
9. Підходи до проектування ядра.
10. Багаторівневі системи.
11. Змішані системи.
12. Файлова система FAT.
13. Файлова система NTFS.
14. Архітектура файлової системи EFS.
15. Файлові системи exFAT, Ext4, BtrFS, ReiserFS, XFS, JFS.
16. Технології віртуалізації
17. Процеси
18. Потоки
19. Керування пам’яттю
20. RAID-масиви
21. Вимоги, що висуваються до захищених операційних систем.
22. Поняття та призначення політики інформаційної безпеки.
23. Порушення політики інформаційної безпеки.
24. Атаки на рівні операційної системи.
25. Несанкціонований доступ.
26. Незаконне використання привілеїв.
27. Атаки типу: "салямі", "приховані канали", "маскарад", "збір сміття" та "злам системи".
28. Шкідливе програмне забезпечення.
29. Ознаки інфікованої операційної системи.
30. Технології виявлення вірусів.
31. Класифікація антивірусного програмного забезпечення.
32. Парольна технологія ідентифікації.
33. Апаратна технологія ідентифікації.
34. Біометрична технологія ідентифікації.

35. Багатофакторна ідентифікація.
36. Компоненти системи захисту ОС Windows.
37. Механізм захисту об’єктів ОС Windows.
38. Ідентифікатор захисту.
39. Маркери доступу.
40. Дескриптори захисту.
41. Права та привілеї (суперпривілеї) облікових записів.
42. Типові права користувачів ОС Windows.
43. Категорії аудиту безпеки.
44. Процес входу користувача в операційну систему.
45. Політика обмеженого використання програм.
46. Резервування в ОС Windows
47. Запуск від імені адміністратора, локальні користувачі та домени.
48. CLI і PowerShell.
49. Інструмент керування Windows, диспетчер завдань і монітор ресурсів.
50. Доступ до мережевих ресурсів.
51. Windows Server.
52. Політики облікових записів.
53. Локальні політики.
54. Монітор брандмауера для програми Windows Defender.
55. Політика диспетчера списку мереж.
56. Політика відкритого ключа.
57. Політика управління додатками.
58. Політика IP-безпеки на «Локальний комп'ютер».
59. Конфігурація розширеної політики аудиту.
60. Модель безпеки операційної системи Linux.
61. Підсистема ідентифікації та аутентифікації.
62. Підсистема розмежування доступу.
63. Монітор безпеки.
64. Linux з покращеним рівнем безпеки (SELinux).
65. Система мандатного контролю доступу AppArmor.
66. Система забезпечення мандатного контролю доступу TOMOYO Linux.
67. Резервування в ОС Linux.
68. Процеси та форки.
69. Зловмисне програмне забезпечення на хості Linux.
70. Перевірка руткіта.
71. Модель безпеки ОС Android.
72. Ідентифікації та аутентифікації.
73. Розмежування доступу.
74. Стандартні та спеціальні дозволи.
75. Архітектура операційної системи iOS.
76. Модель безпеки операційної системи iOS.
77. Характеристика функціонування компонентів Secure Enclave та TouchID.

11. Навчально-методичне забезпечення

Освітній процес з дисципліни «Основи інформаційної безпеки» забезпечений необхідними навчально-методичними матеріалами, що розміщені в Модульному середовищі для навчання MOODLE:

1. Курс «Технології виявлення вразливостей та вторгнень»: https://msn.khmnu.edu.ua/course/view.php?id=6845

Зокрема, викладачами кафедри підготовлені і видані такі роботи:

1. Операційні системи та технології їх захисту : лабораторний практикум з дисципліни для здобувачів першого (бакалаврського) рівня вищої освіти спеціальності «Кібербезпека та захист інформації» / Ю. П. Кльоц, Н. С. Петляк, С. В. Мостовий, О. В. Пирч. Хмельницький : ХНУ, 2025. 82 с.

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

Інформаційна та комп’ютерна підтримка: ПК або ноутбук, проєктор, доступ до мережі Інтернет, робота з презентаціями. Програмне забезпечення: ОС Windows, ОС Windows Server, ОС Linux Ubuntu, програми Microsoft Office або аналогічні, VirtualBox, Cisco Packet Tracer, Windows Defender, Avira Free Security, AVG AntiVirus Free, Panda Dome Free Antivirus, 7-Zip, Advanced ZIP Password Recovery, R-Studio, Recuva, Vera Crypt.

13. Рекомендована література

Основна

1. Безпека інформаційно-комунікаційних систем : підручник / Ю.В. Костюк та ін. Київ : Київський столичний університет імені Бориса Грінченка, 2025. 1016 с.
2. Вишня В. Б., Гавриш О. С., Рижков Е. В. Основи інформаційної безпеки: навч. посіб. Дніпро : Дніпроп. держ. ун-т внутріш. справ, 2020. 128 с.

3. Головня О.С. Основи операційних систем: навч. посіб. Житомир : Житомирська політехніка, 2023. 126 с.
4. Кравчук С.О. Протидія хакерським атакам в мобільних інфокомунікаціях: навч. посіб. Київ: КПІ ім. Ігоря Сікорського, 2025. 814 с.
5. Вступ до кібербезпеки: навч. посіб. / Смірнов О.А.та ін. Кропивницький: ЦНТУ, 2022. 967 с.

Додаткова

6. Tanenbaum A., Bos H.. Modern operating systems. Fourth edition. Amsterdam: Vrije Universiteit, The Netherlands, 2016. 1137 pages
7. Горбань Г. В. Кандиба І. О. Операційна система Linux : навч. посіб. Миколаїв : Вид-во ЧНУ ім. Петра Могили, 2019. 276 с.
8. Операційна ситема Linux: принципи роботи з файловою системою: навч.посіб. / Черевик В.М. та ін. Київ: ДУТ, 2021. 147 с.
9. Операційні системи та технології їх захисту : лабораторний практикум / Ю. П. Кльоц та ін. Хмельницький : ХНУ, 2025. 82 с.
10. Операційні системи: навч. посіб. / Федотова-Півень І. М. та ін. Харків: ТОВ «ДІСА ПЛЮС», 2019. 216 с.
11. Гаркуша І.М. Операційні системи: конспект лекцій. Дніпро: НТУ «ДП», 2020. 73 с.
12. Інформаційна безпека: навч. посіб. / Бобало Ю.Я. та ін. Львів: Видавництво Львівської політехніки, 2019. 580 с.
13. Мосіюк О. О., Федорчук А. Л. Операційні системи та системне програмування: навч.-метод. посібник. Житомир: Вид-во ЖДУ ім. Івана Франка, 2022. 76 с.
14. Авраменко В.С., Авраменко А.С. Основи операційних систем: навч. посіб. Черкаси: ЧНУ ім. Богдана Хмельницького, 2018. 524 с.
15. Security configuration guidance support. URL: https://support.microsoft.com/en-us/topic/security-configuration-guidance-support-ea9aef24-347f-15fa-b94f-36f967907f2f (дата звернення 22.08.2025)
16. Configure security policy settings. URL: https://docs.microsoft.com/uk-ua/windows/security/threat-protection/security-policy-settings/how-to-configure-security-policy-settings (дата звернення: 22.08.2025)
17. NTFS overview. URL: https://docs.microsoft.com/en-us/windows-server/storage/file-server/ntfs-overview (дата звернення 20.08.2025)
18. Advanced security audit policies. URL: https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/advanced-security-audit-policy-settings (дата звернення 20.08.2025)
19. Threat analysis of an enterprise messaging system. URL: https://www.sciencedirect.com/science/article/abs/pii/S1353485814701217#preview-section-abstract (дата звернення 20.08.2025)
20. Gerardus Blokdyk. Secure Messaging: A Complete Guide. 2019. Inc. ISBN: 0655820469. 480 p.
21. Олександр Мізюк. Системи числення. URL: https://nrs.rozh2sch.org.ua/ (дата звернення 22.08.2025)
22. Social Engineering. URL: https://www.imperva.com/learn/application-security/social-engineering-attack/ (дата звернення 18.08.2025)
23. Oracle VirtualBox. User Guide. URL: https://www.virtualbox.org/manual/ (дата звернення 28.07.2025)
24. Ubuntu. Installation RAID. URL: https://help.ubuntu.com/community/Installation/SoftwareRAID?_gl=1*24tbam*_gcl_au*MjYwOTkxMDY2LjE3NTU3OTEwMjk (дата звернення 23.07.2025)
25. Install Ubuntu Desktop. URL: https://ubuntu.com/tutorials/install-ubuntu-desktop#1-overview (дата звернення 23.07.2025)
26. Облікові записи користувачів. URL: https://help.ubuntu.com/stable/ubuntu-help/user-accounts.html.uk (дата звернення 25.07.2025)
27. Audit Oracle Linux with Auditd. URL: https://docs.oracle.com/en/learn/ol-auditd/#introduction (дата звернення 26.07.2025)
28. Сагун А.В., Бобков В.Б.. Операційні системи та комп'ютерні мережі : навч. посіб. Київ : КПІ ім. Ігоря Сікорського», 2022. 164 с.
29. Резервне копіювання та відновлення за допомогою служба Windows для резервного копіювання. URL: https://surl.li/zlcpge (дата звернення 18.07.2025)
30. Безпека Cipher.exe. exe для шифрування файлової системи. URL: https://surl.li/wtatag (дата звернення 16.07.2025)
31. Початок роботи з Cisco Packet Tracer. URL: https://www.netacad.com/courses/getting-started-cisco-packet-tracer?courseLang=en-US (дата звернення 13.08.2025)
32. Текстові документи. Загальні вимоги СОУ 207.01:2017 / Бойко Ю. М. та ін. Хмельницький : ХНУ, 2018. 45 с.
33. Жураковський Б.Ю., Зенів І.О.. Комп'ютерні мережі. Частина 1 : навч. посіб. Київ : КПІ ім. Ігоря Сікорського, 2020. 336 с.
34. Схеми з'єднань та способи обтиску витої пари. URL: https://shop-gsm.ua/blog/shemy-soedinenij-i-sposoby-obzhima-vitoj-pary/?srsltid=AfmBOorftdf3eUhHJOHAt7SlAnYoKQ7oCjtImhJ5O8pnF9GxMGUKnfYh (дата звернення 21.08.2025)

.

14. Інформаційні ресурси

1. Модульне середовище для навчання. URL : https://msn.khmnu.edu.ua/course/view.php?id=6845
2. Електронна бібліотека ХНУ. URL: https://library.khmnu.edu.ua/
3. Інституційний репозитарій ХНУ. URL : https://elar.khmnu.edu.ua/

ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Тип дисципліни	Обов'язкова
Рівень вищої освіти	Перший (бакалаврський*)*
Мова викладання	Українська
Семестр	Перший – другий
Кількість призначених кредитів ЄКТС	13,0
Форми здобуття освіти, для яких викладається дисципліна	Очна (денна)

Результати навчання. Після вивчення дисципліни студент повинен: *виявляти* загальні знання та розуміння предметної області та розуміння професійної діяльності; *застосовувати* й адаптувати принципи, методи, поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності; *мати* базові знання та практичні навички з використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах; *використовувати* інформаційно-комунікаційних технології, базові знання сучасних методів і моделей інформаційної безпеки та/або кібербезпеки, теорії та методів захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем; *обирати* і *використовувати* методи та способи розв'язання спеціалізованих задач і практичних проблем у професійній діяльності; вирішувати базові задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження; *застосовувати* принципи, методи, поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності; *адаптуватися* до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.

Зміст навчальної дисципліни. Основи інформаційної безпеки. Архітектура комп'ютерів. Безпека мереж. Особливості застосування інформаційної безпеки. Призначення, функції та архітектури операційних систем. Реалізація безпеки в операційній системі Windows. Реалізація безпеки в операційній системі Linux. Реалізація безпеки в мобільних операційних системах.

Пререквізити: вихідна.

Постреквізити: математичні основи захисту інформації; захист інформації в інформаційно-комунікаційних системах; захист інформації в інформаційно-комунікаційних системах (курсовий проєкт); нормативно-правове забезпечення кібербезпеки.

Запланована навчальна діяльність: Мінімальний обсяг навчальних занять в одному кредиті ЄКТС навчальної дисципліни для ***першого*** (бакалаврського) рівня вищої освіти за денною формою здобуття освіти становить 10 годин на 1 кредит ЄКТС.

Форми (методи) навчання: лекції (з використанням словесних, наочних, інтерактивних та проблемних методів); практичні заняття (з використанням практичних 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 на практичних заняттях; оцінювання результатів захисту лабораторних робіт; тестування.

Вид семестрового контролю: залік – 1, 2 семестр.

Навчальні ресурси:

1. Безпека інформаційно-комунікаційних систем : підручник / Ю.В. Костюк та ін. Київ : Київський столичний університет імені Бориса Грінченка, 2025. 1016 с.
2. Вишня В. Б., Гавриш О. С., Рижков Е. В. Основи інформаційної безпеки: навч. посіб. Дніпро : Дніпроп. держ. ун-т внутріш. справ, 2020. 128 с.
3. Головня О.С. Основи операційних систем: навч. посіб. Житомир : Житомирська політехніка, 2023. 126 с.
4. Кравчук С.О. Протидія хакерським атакам в мобільних інфокомунікаціях: навч. посіб. Київ: КПІ ім. Ігоря Сікорського, 2025. 814 с.
5. Вступ до кібербезпеки: навч. посіб. / Смірнов О.А.та ін. Кропивницький: ЦНТУ, 2022. 967 с.
6. Модульне середовище для навчання. Доступ до ресурсу: https://msn.khmnu.edu.ua/course/view.php?id=6845
7. Електронна бібліотека ХНУ. Доступ до ресурсу: https://library.khmnu.edu.ua/

Викладач: д-р філософії, ст. викл. Наталія Петляк.