

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ЧОРТКІВСЬКИЙ НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
ПІДПРИЄМНИЦТВА І БІЗНЕСУ

ЗАТВЕРДЖУЮ
Директор ЧННПБ ЗУНУ

Надія КУДЬЧИЦЬКА

31.08.2026 р.

ЗАТВЕРДЖУЮ
Проректор з науково-педагогічної роботи
Віктор ОСТРОВЕРХОВ

31.08.2026 р.

РОБОЧА ПРОГРАМА

з дисципліни «Інформаційна безпека та захист даних у професійній освіті»
другого (магістерського) рівня вищої освіти
галузь знань - А Освіта
спеціальність - А5 Професійна освіта (за спеціалізаціями)
спеціалізація – А5.39 Цифрові технології
освітньо-професійна програма – Фінансова грамотність

кафедра фундаментальних та спеціальних дисциплін

Форма навчання	Курс	Семестр	Лекції (год.)	Практ. (год.)	ІРС (год.)	Самост. робота студ. (год.)	Разом (год.)	Екз. (сем.)
Денна	1	1	16	30	5	99	150	Екз.

Робоча програма складена на основі освітньо-професійної програми підготовки магістра галузі знань А Освіта, спеціальності А5 Професійна освіта (за спеціалізаціями), затвердженій Вченою радою ЗУНУ (протокол № 10 від 17.06.2026 р.).

Робочу програму склала
викладач фундаментальних та
спеціальних дисциплін

 Марія ЛОСЬ

Робоча програма затверджена на засіданні кафедри фундаментальних та спеціальних дисциплін (протокол № 1 від 27.08.2026 р.)

Завідувач кафедри



Людмила ДЕРМАНСЬКА

Гарант ОПП



Галина ЧЕКАЛОВСЬКА

СТРУКТУРА РОБОЧОЇ ПРОГРАМИ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «Інформаційна безпека та захист даних у професійній освіті»

1.Опис дисципліни

«Інформаційна безпека та захист даних у професійній освіті»

Дисципліна «Інформаційна безпека та захист даних у професійній освіті»	Галузь знань, Спеціальність спеціалізація, освітньо- професійна програма, ступінь вищої освіти	Характеристика навчальної дисципліни
Кількість кредитів - 5	галузь знань - А Освіта	Статус дисципліни нормативна дисципліна з циклу професійної підготовки Мова навчання українська
Кількість залікових модулів - 4	спеціальність - А5 Професійна освіта (за спеціалізаціями)	Рік підготовки: Денна – 1 Семестр: Денна – 1
Кількість змістових модулів - 2	освітньо-професійна програма – Фінансова грамотність	Лекції: Денна форма – 16 год. Практичні заняття: Денна форма – 30 год.
Загальна кількість годин – 150	Ступінь вищої освіти- рівень другий (магістерський)	Самостійна робота: Денна форма – 99 год. Індивідуальна робота : Денна – 5 год.
Тижневих годин – 10 год., з них аудиторних – 4 год.		Вид підсумкового контролю – екзамен

2.Мета й завдання дисципліни

«Інформаційна безпека та захист даних у професійній освіті»

2.1.Мета вивчення дисципліни

Метою навчальної дисципліни є формування у здобувачів вищої освіти теоретичних знань та практичних навичок щодо забезпечення інформаційної безпеки національних інтересів у будь-якій сфері життєдіяльності суспільства.

2.2. Завдання вивчення дисципліни

В результаті вивчення курсу «Інформаційна безпека» студенти повинні:
-опанувати знання з основ державної політики у сфері забезпечення інформаційної безпеки та зміст основних положень нормативно-правових актів у

сфері інформаційної безпеки;

-засвоєння знань щодо концептуальних засад, принципів, форм та методів забезпечення інформаційної безпеки;

-ознайомлення з ключовими загрозами інформаційної безпеки, основами управління інформаційною безпекою;

-формувати у студентів навички практичного використання знань теорії практики інформаційної безпеки у практичній діяльності.

2.3. Найменування та опис компетентностей, формування котрих забезпечує вивчення дисципліни:

СК 17. Здатність використовувати сучасні інформаційні технології та спеціалізоване програмне забезпечення та інтегрувати їх в освітнє середовище.

СК 19. Здатність аналізувати ефективність проектних рішень, пов'язаних з підбором, експлуатацією, удосконаленням, модернізацією технологічного обладнання та устаткування галузі/сфери відповідно до спеціалізації.

СК 20. Здатність використовувати відповідне програмне забезпечення для вирішення професійних завдань, відповідно до спеціалізації.

2.4. Передумови для вивчення дисципліни.

Вивчення курсу «Інформаційна безпека» передбачає наявність систематичних та ґрунтовних знань із суміжних курсів «Основи програмування», «Інженерна та комп'ютерна графіка», а також цілеспрямованої роботи на лекційних та лабораторних заняттях, самостійної роботи студентів.

2.5. Програмні результати:

ПР 02. Володіти інформацією чинних нормативно-правових документів, законодавства, галузевих стандартів професійної діяльності в установах, на виробництвах, організаціях галузі/сфери (відповідно до спеціалізації).

ПР 04. Розуміти особливості комунікації, взаємодії та співпраці в міжнародному культурному та професійному контекстах. ПР 05. Володіти культурою мовлення, обирати оптимальну комунікаційну стратегію у спілкуванні з групами та окремими особами.

ПР 07. Аналізувати та оцінювати ризики, проблеми у професійній діяльності й обирати ефективні шляхи їх вирішення.

3. Програма дисципліни

«Інформаційна безпека та захист даних у професійній освіті»

Змістовий модуль 1. Забезпечення захисту інформаційної безпеки

Тема 1. Поняття інформаційної безпеки держави, суспільства та особи.

Інформаційна безпека (поняття і визначення). Підходи до визначення поняття «інформаційна безпека». Інтереси особи, суспільства та держави в інформаційній сфері. Об'єкти, суб'єкти та види інформаційної безпеки.

Література: 1,2,3,4,5,6

Тема 2. Загрози інформаційної безпеки.

Характеристика інформаційної безпеки. Класифікація загроз. Сучасні загрози. Інформаційні ризики. Витік інформації.

Література: 1,2,3,4,5,6

Тема 3. Інформаційна система персональних даних.

Нормативні документи захисту даних. Конфіденційність персональних даних. Захист персональної інформації. Європейська система захисту персональних даних.

Література: 1,2,3,4,5,6

Тема 4. Забезпечення безпеки інформації та інформаційних ресурсів.

Основні напрями забезпечення безпеки інформації. Правовий захист. Організаційний захист. Інженерно-технічний захист.

Література: 1,2,3,4,5,6

Змістовий модуль 2. Управління інформаційною безпекою

Тема 5. Захист інформаційних систем.

Джерела конфіденційної інформації. Інформаційна система як об'єкт захисту інформації. Рівні захисту інформаційних систем. Аналіз вразливостей корпоративних інформаційних систем. Основні принципи захисту інформації.

Література: 1,2,3,4,5,6

Тема 6. Кіберзлочинність.

Характеристики кіберзлочинності. Засоби протидії кіберзлочинності. Класифікація кіберзлочинів. Протидія кіберзлочинності в Україні. Боротьба з кіберзлочинами. Національні інтереси України в інформаційній сфері та шляхи їх забезпечення. Сучасний стан кримінально-правового забезпечення боротьби з кіберзлочинністю.

Література: 1,2,3,4,5,6

Тема 7. Оцінка та управління ризиками інформаційної безпеки.

Оцінка ризиків. Стратегії управління ризиками. Стандарти безпеки, законодавство та регулювання в галузі кібербезпеки. Основні поняття та класифікація кіберзлочинів.

Література: 1,2,3,4,5,6

Тема 8. Відновлення даних.

Політика інформаційної безпеки організації. Основні правила інформаційної безпеки організації. Заходи управління інформаційною безпекою.

Література: 1,2,3,4,5,6

**4.Структура залікового кредиту дисципліни
«Інформаційна безпека та захист даних у професійній освіті»**

Тематика залікового кредиту	Кількість годин				
	Лекції	Практ. заняття	Самост. робота	Індив. робота	Контр. заходи
Змістовий модуль 1. Забезпечення захисту інформаційної безпеки					
Тема 1. Поняття інформаційної безпеки держави, суспільства та особи	2	4	14	2	Усне опитування, ситуаційні завдання, тестові завдання
Тема 2. Загрози інформаційної безпеки.	2	4	10		
Тема 3. Інформаційна система персональних даних.	2	2	13		
Тема4. Забезпечення безпеки інформації та інформаційних ресурсів.	2	4	10		Змістовий модуль по темах 1-4
Змістовий модуль 2. Управління інформаційною безпекою					
Тема 5. Захист інформаційних систем.	2	4	10	3	Усне опитування ситуаційні завдання, тестові завдання
Тема 6. Кіберзлочинність	2	4	12		
Тема 7.Оцінка та управління ризиками інформаційної безпеки.	2	4	14		
Тема 8. Відновлення даних.	2	4	16		Змістовий модуль по темах 5-8
ВСЬОГО: 150	16	30	99	5	екзамен

5. Тематика практичних занять з дисципліни «Інформаційна безпека та захист даних у професійній освіті»

Змістовий модуль 1. Забезпечення захисту інформаційної безпеки

Практичне заняття № 1-2

Тема: Основи інформаційної безпеки

Мета: *Засвоїти необхідність і сутність основних понять у сфері інформаційної безпеки.*

Питання для обговорення:

1. Поняття інформаційної безпеки.
2. Основні види безпеки.
3. Тріада (CIA): конфіденційність, цілісність, доступність.
4. Інформаційна безпека особи та суспільства.

Література: 1-12

Практичне заняття № 3-4

Тема: Загрози інформаційній безпеці.

Мета: *Вивчення та дослідження загроз безпеці інформації.*

Питання для обговорення:

1. Класифікація загроз.
2. Типи атак на інформаційні системи.
3. Шкідливе програмне забезпечення. Основні типи та загальний огляд комп'ютерних вірусів.
4. Поняття антивірусної програми. Огляд найпоширеніших антивірусних програм та їх класифікація.

Література: 1-12

Практичне заняття № 5

Тема: Безпека даних. Політика безпеки інформації.

Мета: *Вивчення та дослідження проблем інформаційної безпеки.*

Питання для обговорення:

1. Концепція захисту інформації.
2. Захист конфіденційності, цілісності та доступності даних.
3. Методи аутентифікації, авторизації та аудиту даних.
4. Види забезпечення безпеки інформації.
5. Критерії оцінки інформаційної безпеки та аспекти захисту інформації

Література: 1-12

Практичне заняття № 6-7

Тема: Основні напрями забезпечення безпеки інформації та інформаційних ресурсів.

Мета: *вивчення концептуальних положень захисту інформації та інформаційних ресурсів.*

Питання для обговорення:

1. Визначення базових загроз безпеці інформації та інформаційних ресурсів.
2. Класифікація уразливостей безпеці інформації та інформаційних ресурсів.
3. Вивчення основних напрямів забезпечення безпеки.

4. Вивчення загальних положень правового захисту.
 5. Вивчення загальних положень організаційного захисту.
 6. Вивчення загальних положень інженерно-технічного захисту.
 7. Вивчення архітектури захисту інформації в інформаційних системах та мережах.
- Література: 1-12

Змістовий модуль 2. Управління інформаційною безпекою

Практичне заняття № 8-9

Тема: Захист інформаційних систем. Криптографічний вид захисту інформації.

Мета: Розглянути базові поняття теорії чисел, отримання практичних навичок шифрування і дешифрування повідомлень за допомогою відкритого та закритого ключа криптосистеми RSA з використанням теорії чисел.

Питання для обговорення:

1. Основні поняття криптографії, способи шифрування файлів, папок, повідомлень.
2. Криптографічні методи захисту інформації, основні засоби здійснення криптографічного захисту інформації.
3. Використання теорії чисел для захисту інформації.
4. Криптосистема шифрування даних RSA.

Література: 1-12

Практичне заняття № 10-11

Тема: Кіберзлочинність.

Мета: Вивчення та дослідження засобів аутентифікації користувачів і аналіз безпеки системи. Навчитися налаштовувати елементи керувати безпекою під час управління обліковим записом.

Питання для обговорення:

1. Розмежування доступу до інформації.
2. Ідентифікація, аутентифікація, авторизація.
3. Системи аудиту та моніторингу.

Література: 1-12

Практичне заняття № 12-13

Тема: Оцінка та управління ризиками інформаційної безпеки.

Мета: Вивчення та дослідження принципів роботи системи аналізу та управління інформаційними ризиками.

Питання для обговорення:

1. Оцінка ризиків.
2. Стратегії управління ризиками.
3. Стандарти безпеки, законодавство та регулювання в галузі кібербезпеки.
4. Основні поняття та класифікація кіберзлочинів.
5. Сучасний стан кримінально-правового забезпечення боротьби з кіберзлочинністю.

Література: 1-12

Практичне заняття № 14-15

Тема: Відновлення даних з різних носіїв інформації.

Мета: Вивчення та дослідження засобів відновлення даних з різних носіїв інформації.

Питання для обговорення:

1. Поняття захисту інформації та інформаційної безпеки.
2. Критерії оцінки інформаційної безпеки. Аспекти захисту інформації.
Електронний підпис: види та використання.
3. Онлайн інструменти для електронного підпису.
4. Засоби резервного копіювання та відновлення даних. Пристрої відновлення даних.

Література: 1-12

6.Самостійна робота студентів

Самостійна робота студентів має на меті формування пізнавальної активності студентів, засвоєння ними основних умінь та навичок роботи з навчальними матеріалами, поглиблення та розширення вже набутих знань, підвищення рівня організованості студентів тощо.

Для набуття умінь самостійного мислення і самоконтролю у студентів особливе значення має виконання індивідуального завдання з дисципліни «Інформаційна безпека», яке виконується самостійно кожним студентом згідно методичних рекомендацій та інструкцій. Воно охоплює основні теми дисципліни та має на меті засвоєння теоретичного матеріалу, оволодіння навиками застосування набутих теоретичних знань щодо захисту інформаційної безпеки, і є одним із обов'язкових складових модулів залікового кредиту з дисципліни. Написання реферату на тему оцінюється (max 100 балів). Перелік тем:

- 1.Державна таємниця
- 2.Матеріальні носії секретної інформації
- 3.Система захисту державної таємниці
- 4.Допуск до державної таємниці
- 5.Гриф секретності
- 6.Ступінь секретності
- 7.Інформаційна безпека держав.
- 8.Поняття інформаційної безпеки держави, суспільства та особи
- 9.Загрози інформаційної безпеки
10. Система забезпечення інформаційної безпеки України.
11. Державна політика в інформаційній сфері та забезпечення інформаційної безпеки
12. Державна політика інформаційної безпеки як інструмент забезпечення інформаційної безпеки держави
13. Безпека інформації, інформаційних ресурсів та інформаційної інфраструктури
14. Національні інформаційні ресурси.
15. Система національних інформаційних ресурсів
16. Поняття та основні задачі інформаційної безпеки
17. Загрози інформаційної безпеки
18. Системи забезпечення інформаційної безпеки
19. Основні сервіси безпеки

20. Особливості сучасних інформаційних систем з погляду безпеки
21. Фізичні засоби захисту
22. Інформаційна безпека в електронному урядуванні
23. Інформаційні виборчі технології
24. Огляд міжнародних стандартів у галузі інформаційна безпека
25. Основні положення теорії захисту інформації
26. Сутність та види атак на комп'ютерну мережу
27. Реалізація системи захисту інформації в комп'ютерних системах і мережах
28. Інформаційне та правове забезпечення електронних видань і цифрової передачі даних в Україні
29. Міжнародна інформаційна безпека
30. Технологія реалізації атак на комп'ютерну систему та мережу
31. Законодавча база в галузі захисту інформації
32. Основні поняття і аналіз загроз інформаційної безпеки
33. Проблеми інформаційної безпеки мереж
34. Політики безпеки
35. Стандарти інформаційної безпеки
36. Принципи криптографічного захисту інформації
37. Криптографічні алгоритми
38. Технології аутентифікації
39. Забезпечення безпеки операційних систем
40. Технології міжмережевих екранів
41. Основи технології віртуальних захищених мереж VPN
42. Захист на каналному і сеансовому рівнях
43. Захист на мережевому рівні – протокол IPSEC
44. Інфраструктура захисту на прикладному рівні
45. Аналіз захищеності і виявлення атак
46. Захист від вірусів
47. Методи управління засобами мережевої безпеки

7.Засоби оцінювання та методи демонстрування результатів навчання

У процесі вивчення дисципліни «Інформаційна безпека та захист даних у професійній освіті» використовуються наступні засоби оцінювання та методи демонстрування результатів навчання:

- поточне опитування, тестування;
- презентації результатів виконаних завдань;
- оцінювання результатів модульної контрольної роботи;
- оцінювання результатів самостійної роботи;
- студентські презентації та виступи на наукових заходах;
- екзамен

8.Політика щодо оцінювання

Політика щодо дедлайнів і перескладання. Для виконання усіх видів завдань студентами і проведення контрольних заходів встановлюються конкретні терміни. Перескладання модулів відбувається з дозволу дирекції факультету за наявності поважних причин (наприклад, лікарняний).

Політика щодо академічної доброчесності. Списування під час проведення контрольних заходів заборонені. Під час контрольного заходу студент може користуватися лише дозволеними допоміжними матеріалами або засобами, йому забороняється в будь-якій

формі обмінюватися інформацією з іншими студентами, використовувати, розповсюджувати, збирати варіанти контрольних завдань.

Політика щодо відвідування. За об'єктивних причин (наприклад, карантин, воєнний стан, хвороба, закордонне стажування тощо) навчання може відбуватись в дистанційній формі за погодженням із керівником курсу з дозволу дирекції факультету.

9. Політика щодо визнання результатів навчання

Відповідно до «Положення про визнання в Західноукраїнському національному університеті результатів попереднього навчання» (https://www.wunu.edu.ua/pdf/pologenya/Polozhennya_ruzult_poper_navch.pdf) здобувачам вищої освіти може бути зараховано результати навчання неформальної/інформальної освіти, академічної мобільності тощо) на підставі підтвердних документів (сертифікати, довідки, документи про підвищення кваліфікації тощо).

Рішення про зарахування здобувачу результатів (певного освітнього компонента в цілому, або ж окремого виду навчальної роботи за таким освітнім компонентом) приймається уповноваженою Комісією з визнання результатів навчання за процедурою, визначеною вищезазначеним положенням.

10. Критерії, форми поточного та підсумкового контролю

Підсумковий бал (за 100-бальною шкалою) з дисципліни «Інформаційна безпека та захист даних у професійній освіті» визначається як середньозважена величина, залежно від питомої ваги кожної складової залікового кредиту:

Модуль 1		Модуль 2		Модуль 3	Модуль 4
10 %	10 %	10 %	10 %	20%	40%
Поточне оцінювання	Модульний контроль 1	Поточне оцінювання	Модульний контроль 2	Самост. робота	Екзамен
Оцінюється як середнє арифметичне з оцінок, отриманих по 1-4 темах	Підсумкова модульна контрольна робота по 1-4 темах Теоретичні питання (2 питання по макс 25 балів) Задача 1 – макс. 25 балів Тестові завдання 5 тестів по (5 б. за тест) – макс. 25 балів	Оцінюється як середнє арифметичне з оцінок, отриманих по 5-8 темах	Підсумкова модульна контрольна робота по 5-8 темах Теоретичні питання (2 питання по макс 25 балів) Задача 1 – макс. 25 балів Тестові завдання 5 тестів по (5 б. за тест) – макс. 25 балів	Сукупність питомої ваги кожної складової: 80% підготовка реферату; 20% - захист реферату.	Завдання 1 – макс. 25 балів Завдання 2 – макс. 25 балів Задача -25 балів Тестові завдання (5 тестів по 5 б. за тест) – макс. 25 балів

Поточне опитування під час заняття:

90–100 балів – у повному обсязі володіє навчальним матеріалом, вільно самостійно та аргументовано його викладає під час відповідей, глибоко та всебічно розкриває зміст теоретичних питань;

75–89 балів – достатньо повно володіє навчальним матеріалом, але при викладанні деяких питань не вистачає достатньої глибини та аргументації, допускаються при цьому окремі несуттєві неточності та незначні помилки;

65–74 бали – в цілому володіє навчальним матеріалом та викладає його основний зміст, але без глибокого всебічного аналізу, обґрунтування та аргументації, допускаючи при цьому окремі суттєві неточності та помилки;

60–64 бали – не в повному обсязі володіє навчальним матеріалом, фрагментарно (без аргументації та обґрунтування) його викладає, недостатньо розкриває зміст теоретичних питань, допускаючи при цьому суттєві неточності;

1–59 балів – не володіє навчальним матеріалом, не розкриває зміст теоретичних питань.

Підсумкова оцінка за поточне опитування кожного модуля визначається як середнє арифметичне оцінок, отриманих під час занять в межах кожного модуля.

Самостійна робота:

90–100 балів – зміст самостійної роботи повністю відповідає встановленим вимогам, містить елементи самостійного дослідження, свідчить про високий рівень опанування навчального матеріалу, студент на високому рівні виявляє творчий підхід до виконання завдань;

75–89 балів – зміст самостійної роботи в основному відповідає встановленим вимогам, можуть бути несуттєві недопрацювання за окремими завданнями, свідчить про належний рівень опанування навчального матеріалу, студент належно виявляє творчий підхід до виконання завдань;

60–74 балів – поставлені завдання виконані на недостатньому рівні; наведені авторські напрацювання є загальними і слабо обґрунтованими, свідчать про недостатній рівень опанування навчального матеріалу; студент припускається значних помилок у виконанні завдань, в окремих моментах виявляє творчий підхід до виконання завдань;

1–59 балів – завдання практично не виконані; відсутні авторські напрацювання; грубі помилки у вирішенні завдань роботи, що свідчать про низький рівень опанування навчального матеріалу; студент не виявляє творчого підходу до виконання завдань.

Модульна робота – види контролю, при яких засвоєння студентом теоретичного та практичного матеріалу оцінюється від 0 до 100 балів як сума балів за виконані завдання.

Екзаменаційний білет складається із:

тестів: 5 тестів, за правильну відповідь на кожен із яких студент може отримати 5 балів, що в підсумку дає максимально 25 балів;

5 балів – за тест надано правильну відповідь.

практичних завдань: 1 завдання, за розв'язання студент може отримати від 0 до 25 балів;

15–25 балів – у повному обсязі володіє навчальним матеріалом, правильно розв'язує практичне завдання і інтерпретує отримані результати, демонструє самостійність виконання.

5–14 балів – у достатньому обсязі володіє навчальним матеріалом, правильно розв'язує практичне завдання, але на додаткові контрольні запитання відсутня повна відповідь, допускає несуттєві неточності та фрагментарно (без аргументації) інтерпретує отримані результати, демонструє самостійність виконання.

1–4 балів – не в повному обсязі володіє матеріалом, фрагментарно розв'язує практичне завдання, допускає суттєві неточності, поверхнево його викладає, недостатньо розкриває зміст поставлених питань.

теоретичного питання: 2 теоретичних питання, за відповідь на кожне питання, студент може отримати від 0 до 25 балів, що в підсумку дає максимально 50 балів

15–25 балів – у повному обсязі володіє навчальним матеріалом, всебічно, самостійно та аргументовано його викладає під час відповіді, глибоко та всебічно розкриває зміст завдання.

1–14 балів – в цілому володіє навчальним матеріалом, але не в повному обсязі, фрагментарно (без аргументації та обґрунтування) його викладає, недостатньо розкриває зміст завдання, допускаючи при цьому суттєві неточності, відповіді на запитання нечіткі.

Екзамен – види контролю, при яких засвоєння студентом теоретичного та практичного матеріалу оцінюється від 0 до 100 балів як сума балів за виконані завдання.

Екзаменаційний білет складається із:

теоретичні питання: 2 теоретичних питань, за відповідь на яке студент може отримати від 0 до 25 балів.

10–25 балів – у повному обсязі володіє навчальним матеріалом, всебічно, самостійно та аргументовано його викладає під час відповіді, глибоко та всебічно розкриває зміст завдання.

1–9 балів – в цілому володіє навчальним матеріалом, але не в повному обсязі, фрагментарно (без аргументації та обґрунтування) його викладає, недостатньо розкриває зміст завдання,

допускаючи при цьому суттєві неточності, відповіді на запитання нечіткі.

практичних завдань: 1 задача, за розв'язання якої студент може отримати від 0 до 25 балів;

15–25 балів – у повному обсязі володіє навчальним матеріалом, правильно розв'язує практичне завдання і інтерпретує отримані результати, демонструє самостійність виконання.

5–14 балів – у достатньому обсязі володіє навчальним матеріалом, правильно розв'язує практичне завдання, але на додаткові контрольні запитання відсутня повна відповідь, допускає несуттєві неточності та фрагментарно (без аргументації) інтерпретує отримані результати, демонструє самостійність виконання.

1–4 балів – не в повному обсязі володіє матеріалом, фрагментарно розв'язує практичне завдання, допускає суттєві неточності, поверхнево його викладає, недостатньо розкриває зміст поставлених питань.

тестів: 5 тестів, за правильну відповідь на кожен із яких студент може отримати 5 балів, що в підсумку дає максимально 25 балів;

5 балів – на тест надано правильну відповідь.

Шкала оцінювання:

За шкалою університету	За національною Шкалою	За шкалою ECTS
90-100	Відмінно	A (відмінно)
85-89	Добре	B (дуже добре)
75-84		C (добре)
65-74	Задовільно	D (задовільно)
60-64		E (достатньо)
35-59	Незадовільно	FX (незадовільно з можливістю повторного складання)
1-34		F (незадовільно з обов'язковим повторним курсом)

11.Інструменти, обладнання та програмне забезпечення, використання яких передбачає навчальна дисципліна

№	Найменування	Номер теми
1.	Мультимедійний проектор	1-8
2.	Проекційний екран	1-8
3.	Комунікаційне програмне забезпечення (Internet Explorer, Google Chrome, Firefox)	1-8
4.	Комунікаційне програмне забезпечення (Zoom) для проведення занять у режимі он-лайн (за необхідності)	1-8
5.	Комунікаційна навчальна платформа (Moodle) для організації дистанційного навчання (за необхідності)	1-8
6.	Програмне забезпечення: ОС Windows	1-8
7.	Інструменти Microsoft Office (Word; Excel; Power Point)	1-8

РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

1. Закон України «Про основні засади забезпечення кібербезпеки України» зі змінами. Відомості Верховної Ради (ВВР), 2017, № 45, ст.403, зі змінами від 28.07.2022 року. Режим доступу: URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>
2. Вишня В. Б. Основи інформаційної безпеки : навч. посібник В. Б. Вишня, О. С. Гавриш, Е. В. Рижков. Дніпро : Дніпроп. держ. ун-т внутріш. справ, 2020. 128 с.
3. Вишняков В.М. Захист інформації в комп'ютерних системах: навч. посіб. Київ: КНУБА, 2022. 120 с.
4. Інформаційна безпека. Яковенко Є., Журавель І., Горбатий І., Бондарєв А. Видавництво Львівська політехніка, 2019. 580 с.
5. Інформаційна безпека держави: навч. посіб. В.І.Гур'єв, Д.Б. Мехед, Ю.М.Ткач, І.В.Фірсова. Ніжин: ФОП Лук'яненко В.В.ТПК «Орхідея», 2018. 166с.
6. Інформаційна безпека держави : навч. посіб. В. М. Рудницький [та ін.] ; Черкас. держ. технол. ун-т. Харків : ДІСА ПЛЮС, 2018. 358 с.
7. Інформаційна безпека. Підручник В.В.Остроухов, М.М.Присяжнюк, О.І.Фармагей, М.М.Чеховська та ін.; під ред. В. В. Остроухова. К.: Видавництво Ліра-К, 2021. 412 с.
8. Лизанчук В. В. Інформаційна безпека України: теорія і практика : підручник Львів. нац. ун-т ім. Івана Франка, Львів. шк. журналістики. Львів : ЛНУ ім. Івана Франка, 2017. 725 с.
9. Костюченко А.О., Горошко Ю.В. Віртуалізація операційних систем: навчально-методичний посібник. Ч.: ФОП Баликіна С.М., 2021. 56 с.
10. Методичні вказівки до виконання лабораторних робіт з курсу “Основи кібербезпеки” для студентів спеціальностей “Кібербезпека” Укл.: Яцків В. В. Тернопіль: Економічна думка, 2018. 44 с.
11. Управління інформаційною безпекою: конспект лекцій: навч. посіб. для студ. спец. 125 «Кібербезпека» КПІ ім. Ігоря Сікорського; уклад.: С. О. Носок, О. М. Фаль, В. М. Ткач. – Електронні текстові дані (1 файл: 1114 Кбайт). Київ : КПІ ім. Ігоря Сікорського, 2021. 258 с.
12. AlFardan, N. (2023). Cyber threat hunting. Manning, 2023. 442 p.
13. Adedoyin, F. F., & Christiansen, B. (2023). Effective cybersecurity operations for Enterprise-Wide systems. Information Science Reference. 2023. 344 p.
14. Alexandrou, A. (2021). Cybercrime and internet technology: Theory and Practice. CRC Press, 2022. 455p.
15. Dr. Hidaia Mahmood Alassouli. (2021). Common Windows, Linux and Web Server Systems Hacking Techniques, 2021. 171 p.