МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВЕТЕРИНАРНОЇ МЕДИЦИНИ ТА БІОТЕХНОЛОГІЙ ІМЕНІ С.З. ҐЖИЦЬКОГО

Факультет механіки, енергетики та інформаційних технологій
Кафедра інформаційних технологій

ПОГОДЖЕНО
Гарант ОПП «Комп'ютерні науки»
Вадим ПТАШНИК
(ім'я та прізвище, підпис)
«27» серпня 2025 року

ЗАТВЕРДЖЕНО
Декан факультету механіки, енергетики та інформаційних технологій
Степан КОВАЛИШИН
(ім'я та прізвище, підпис)
«28» серпня 2025 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«ТЕХНОЛОГІЇ І СТАНДАРТИ ЗАХИСТУ ДАНИХ»
(код і назва навчальної дисципліни)

рівень вищої освіти перший (бакалаврський)
(назва освітнього рівня)

галузь знань 12 Інформаційні технології
(назва галузі знань)

спеціальність 122 Комп'ютерні науки
(назва спеціальності)

освітня програма Комп'ютерні науки
(назва)

вид дисципліни вибіркова
(обов'язкова / за вибором)

2025-2026 навчальний рік

Робоча програма Технології і стандарти захисту даних
(назва навчальної дисципліни)

Укладачі: Станько В.Ю. – к.е.н., доцент кафедри інформаційних технологій
(вказати укладачів, їхні посади, наукові ступені та вчені звання)

Робочу програму схвалено на засіданні кафедри інформаційних технологій.

Протокол № 1 від 26.08.2025 року.

Завідувач кафедри _____ Тригуба А.М.
(підпис, ім'я та прізвище)

Погоджено навчально-методичною комісією спеціальності
«Комп'ютерні науки»
(назва спеціальності)

Протокол № 8/1 від «27.08.2025 року»
Голова НМКС _____ Пташник В.В.
(підпис, ім'я та прізвище)

Схвалено рішенням навчально-методичної ради факультету ФМЕІТ
(назва факультету)

Протокол № 1 від «28.08.2025 року»
Голова НМРФ _____ Ковалишин С.Й.
(підпис, ім'я та прізвище)

Ухвалено вченою радою ФМЕІТ протокол №1 від 28.08.2025 року.

ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Найменування показників	Всього годин	
	денна форма здобуття освіти	заочна форма здобуття освіти
Семестр	**8**	**8**
Кількість кредитів/годин	4/120	4/120
Усього годин аудиторної роботи	48	14
в т.ч.:		
– лекційні заняття, год.	24	6
– практичні заняття, год.	–	–
– лабораторні заняття, год.	24	8
– семінарські заняття, год.	–	–
Усього годин самостійної роботи	72	106
Форма контролю	іспит	іспит

Примітка.

Частка аудиторного навчального часу студента у відсотковому вимірі:

для денної форми здобуття освіти – 40%

для заочної форми здобуття освіти – 11,6%

1. МЕТА ТА ЗАВДАННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Метою вивчення освітньої компоненти «Технології і стандарти захисту даних» є формування у студентів системного розуміння принципів, технологій і стандартів захисту даних, а також розвиток практичних навичок виявлення вразливостей інформаційних систем, побудови політик безпеки, застосування сучасних засобів шифрування, автентифікації та контролю доступу, при побудові та інтеграції систем, продуктів і сервісів IT.

Завдання навчальної дисципліни передбачають:

- Аналізувати загрози та ризики для інформаційних систем
- Проєктувати та впроваджувати засоби захисту даних
- Використовувати апаратні та програмні рішення для забезпечення конфіденційності, цілісності та доступності інформації
- Застосовувати міжнародні стандарти, зокрема:
  - ISO/IEC 27001 – системи управління інформаційною безпекою
  - NIST – стандарти кібербезпеки США
  - GDPR – захист персональних даних у ЄС
  - PCI DSS – безпека платіжних систем

Преквізити: для успішного опанування курсу «Технології і стандарти захисту даних» необхідно володіти знаннями з вищої математики, основ програмування, комп'ютерних мереж, операційних систем, основ проектування інформаційних систем, розуміти принципи інформаційної безпеки та криптографії. Крім того, важливо володіти базовими soft-skills, такими як аналітичне мислення, вирішення проблем та командна взаємодія.

Постреквізити: отримані знання та компетентності є особливо важливими під час виконання курсових і кваліфікаційних робіт, проходження практики, а також розроблення комплексних проєктів з інформаційних систем. Це сприяє формуванню професійних умінь у сфері управління інноваційними процесами,

технологіями та системами захисту інформації в умовах сучасних викликів цифрового простору.

Результати навчання: у результаті навчання з дисципліни «Технології і стандарти захисту даних» є набуття студентами загальних компетентностей та знань щодо оцінювання та забезпечення захисту інформації в інформаційних системах. Вивчення сучасних технологій захисту даних, включаючи апаратні та програмні засоби. Опанування міжнародних стандартів у сфері інформаційної безпеки (ISO/IEC 27001, NIST, GDPR, PCI DSS). Аналіз вразливостей інформаційних систем та методів їх усунення. Використання засобів шифрування та криптографічного захисту інформації. Застосування політик контролю доступу та автентифікації..

Відповідно до освітньо-професійної програми «Комп'ютерні науки» вивчення дисципліни посилює набуття здобувачами таких компетентностей та програмних результатів навчання:

Інтегральна компетентність	Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі комп'ютерних наук або у процесі навчання, що передбачає застосування теорій та методів інформаційних технологій і характеризується комплексністю та невизначеністю умов.
Фахові (спеціальні) компетентності	ФК14. Здатність застосовувати методи та засоби забезпечення інформаційної безпеки, розробляти й експлуатувати спеціальне програмне забезпечення захисту інформаційних ресурсів об'єктів критичної інформаційної інфраструктури.
Програмні результати навчання	ПРН15. Розуміти концепцію інформаційної безпеки, принципи безпечного проектування програмного забезпечення, забезпечувати безпеку комп'ютерних мереж в умовах неповноти та невизначеності вихідних даних.

2. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Назви тем	Кількість годин											
	денна форма здобуття освіти (ДФЗО)						заочна форма здобуття освіти (ЗФЗО)					
	усього	у тому числі					усього	у тому числі				
		л	п	лаб.	інд.	с.р.		л	п	лаб.	інд.	с.р.
1	2	3	4	5	6	7	8	9	10	11	12	13
	Рік підготовки_4_ Семестр_7						Рік підготовки_4_ Семестр_7					
Тема 1.	10	2	2			6	10	0	0			10
Тема 2.	10	2	2			6	10	1	0			9
Тема 3.	10	2	2			6	10	0	1			9
Тема 4.	10	2	2			6	10	1	0			9
Тема 5.	10	2	2			6	10	0	1			9
Тема 6.	10	2	2			6	10	1	0			9
Тема 7.	10	2	2			6	10	0	1			9
Тема 8.	10	2	2			6	10	1	1			8
Тема 9.	10	2	2			6	10	0	1			9
Тема 10.	10	2	2			6	10	1	1			8
Тема 11.	10	2	2			6	10	0	1			9
Тема 12.	10	2	2			6	10	1	1			8
Разом	**120**	**24**	**24**			**72**	**120**	**6**	**8**			**106**

3. ЛЕКЦІЙНІ ЗАНЯТТЯ

№ з/п	Назви тем та їх короткий зміст	Кількість годин	
		ДФЗО	ЗФЗО
1	Вступ до інформаційної безпеки Ознайомлення з базовими поняттями: конфіденційність, цілісність, доступність. Роль захисту даних у цифровому суспільстві. Типи інформації та загрози її безпеці.	2	0
2	Законодавча та нормативна база Аналіз міжнародних і національних нормативів: GDPR, ISO/IEC 27001, Закон України «Про захист персональних даних». Права суб'єктів даних, обов'язки контролерів.	2	0
3	Класифікація загроз та вразливостей Типи загроз: внутрішні, зовнішні, технічні, соціальні. Моделі загроз, оцінка ризиків, приклади реальних атак.	2	1
4	Основи криптографії Симетричне та асиметричне шифрування, хеш-функції, цифрові підписи. Алгоритми AES, RSA, SHA-256. Застосування криптографії для захисту даних.	2	0
5	Аутентифікація та контроль доступу Механізми автентифікації (паролі, токени, біометрія), авторизації (ACL, RBAC), багатофакторна автентифікація. Побудова політик доступу.	2	1
6	Захист мережевих комунікацій Протоколи безпеки: SSL/TLS, HTTPS, VPN. Засоби виявлення та запобігання вторгненням (IDS/IPS). Захист передавання даних.	2	0
7	Захист даних у хмарних середовищах Особливості безпеки в хмарних платформах (AWS, Azure, GCP). Моделі відповідальності, шифрування в хмарі, Zero Trust.	2	1
8	Стандарти безпеки: ISO, NIST, PCI DSS Огляд ключових стандартів: ISO/IEC 27001 (управління безпекою), NIST SP 800-53 (контроль безпеки), PCI DSS (платіжні системи). Практики впровадження.	2	1
9	Аналіз вразливостей та тестування Методи виявлення вразливостей: сканування, пентестинг. OWASP Top 10, інструменти (ZAP, Burp Suite, SQLmap). Практичні кейси.	2	1
10	Політики безпеки та управління ризиками Розробка політик безпеки, аудит, оцінка ризиків, план реагування на інциденти. Побудова системи управління інформаційною безпекою.	2	1
11	Практичне моделювання систем захисту Інтеграція знань для побудови комплексної системи захисту. Проєктування архітектури безпеки для ІС. Командна робота над кейсом.	2	1
12	Підсумкове заняття. Вибір технологій та аргументування рішень.	2	1
Усього годин		24	8

4. ПРАКТИЧНІ ЗАНЯТТЯ

№ з/п	Назви тем та їх короткий зміст	Кількість, год.	
		ДФЗО	ЗФЗО
1	Аналіз термінів та інцидентів інформаційної безпеки Ознайомлення з базовими поняттями ІБ. Аналіз реальних кейсів порушень безпеки (витоки даних, атаки, збої).	2	0
2	Порівняльний аналіз GDPR та українського законодавства Вивчення вимог GDPR та Закону України «Про захист персональних даних». Порівняння прав, обов'язків, санкцій.	2	1
3	Моделювання загроз для інформаційної системи Побудова моделі загроз STRIDE або PASTA для заданої ІС. Визначення активів, загроз, векторів атак.	2	0
4	Криптографічні операції: шифрування та дешифрування Практика з використанням алгоритмів AES, RSA, SHA-256. Генерація ключів, підпис, перевірка.	2	1
5	Налаштування контролю доступу Реалізація ACL, RBAC, MFA у віртуальному середовищі або емуляторі.	2	1
6	Захист мережевих комунікацій Налаштування VPN (WireGuard/OpenVPN), аналіз HTTPS-трафіку через Wireshark.	2	1
7	Аналіз політик безпеки у хмарі Вивчення політик CSP (Azure/AWS IAM), реалізація Zero Trust-моделі.	2	1
8	Розробка політики безпеки за ISO/IEC 27001 Створення шаблону політики безпеки відповідно до вимог стандарту.	2	1
9	Аналіз вразливостей за OWASP Використання OWASP ZAP або аналогів для сканування веб-додатку. Аналіз результатів.	2	1
10	Розробка політики безпеки для навчальної симульованої ІС	2	0
11	Командне моделювання системи захисту Робота в групах над кейс-сценарієм: побудова архітектури захисту, вибір технологій, оцінка ризиків.	2	1
12	Захист проєкту та рецензування Презентація проєктів, обговорення рішень, взаємооцінювання.	2	0
	Усього годин	28	8

5. САМОСТІЙНА РОБОТА

№ з/п	Назви тем та їх короткий зміст	Кількість годин	
		ДФЗО	ЗФЗО
1	Основні терміни та поняття інформаційної безпеки та стандартів захисту даних Вивчення ключових термінів: конфіденційність, цілісність, доступність, загроза, ризик, актив. Формування глосарію.	6	10
2	Нормативно-правові акти у сфері захисту даних Ознайомлення з текстами GDPR, ISO/IEC 27001, Закону України «Про захист персональних даних». Підготовка порівняльної таблиці.	6	9
3	Моделі загроз та класифікація атак	6	9

	Аналіз моделей STRIDE, DREAD, PASTA. Класифікація атак: DoS, MITM, фішинг, SQL-ін’єкції.		
4	Криптографічні алгоритми та їх застосування Теоретичне обґрунтування алгоритмів AES, RSA, SHA. Сфери застосування, переваги та обмеження.	6	9
5	Механізми автентифікації та авторизації Вивчення принципів MFA, RBAC, ACL. Порівняння методів автентифікації: паролі, токени, біометрія.	6	9
6	Протоколи захисту мережевих комунікацій Теоретичний аналіз SSL/TLS, HTTPS, VPN. Розгляд механізмів шифрування трафіку та сертифікації.	6	9
7	Безпека хмарних обчислень Вивчення моделей розгортання (IaaS, PaaS, SaaS), політик доступу, концепції Zero Trust.	6	9
8	Стандарти інформаційної безпеки Порівняння ISO/IEC 27001, NIST SP 800-53, PCI DSS. Структура, цілі, сфери застосування.	6	8
9	OWASP Top 10 та аналіз вразливостей Вивчення найпоширеніших вразливостей веб-додатків. Методи виявлення та запобігання.	6	9
10	Розробка політик безпеки Структура політики ІБ, принципи формування, приклади політик для різних типів ІС.	6	8
11	Оцінка ризиків та план реагування на інциденти Методики оцінки ризиків (FAIR, OCTAVE), побудова плану реагування на кіберінциденти.	6	9
12	Аналіз та рецензування систем захисту Критичний аналіз існуючих систем безпеки. Підготовка рецензії на проєкт або кейс.	6	8
	Усього годин	72	106

6. ІНДИВІДУАЛЬНІ ЗАВДАННЯ

–

7. МЕТОДИ НАВЧАННЯ

Навчання з дисципліни «Технології і стандарти захисту даних» здійснюється із застосуванням сучасних інтерактивних та практикоорієнтованих методів, що поєднують словесні (лекція, пояснення, дискусія), наочні (демонстрація, робота з мультимедійними матеріалами) та активні форми (групові проєкти, семінари-дискусії, моделювання ситуацій, аналіз кейсів). Використання методів мозкового штурму, проблемно-орієнтованих і дослідницьких підходів сприяє розвитку критичного та креативного мислення, уміння працювати в команді й приймати ефективні управлінські рішення. Ефективність забезпечується залученням сучасних цифрових інструментів, програмних засобів для планування й контролю, а також роботи з професійною літературою та науковими публікаціями.

8. МЕТОДИ КОНТРОЛЮ

Оцінювання результатів навчання студентів здійснюється проведенням поточного та захистом власних проектів.

Поточний контроль здійснюється під час практичних занять і має на меті перевірку рівня підготовленості студента до виконання відповідних завдань. Форми проведення поточного контролю – усне та письмове опитування, тестовий контроль.

Захист і презентація проектів проводиться з метою оцінювання результатів навчання на завершальному етапі вивчення дисципліни.

9. КРИТЕРІЇ ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Успішність студента оцінюється шляхом проведення поточного контролю та захистом виконаних проектів.

Максимальна кількість балів з дисципліни «Технології і стандарти захист даних», яку може отримати студент протягом семестру за всі види роботи, становить 100, при цьому 50 балів за результатами поточного оцінювання, та 50 – за результатами захисту виконаних робіт.

Результати поточного контролю оцінюються за чотирибальною («2», «3», «4», «5») шкалою. В кінці семестру обчислюється середнє арифметичне значення (САЗ) усіх отриманих студентом оцінок з наступним переведенням його у 50-ти бальну шкалу за формулою:

ПК = 10•САЗ

Критерії поточного оцінювання знань студентів

Оцінка	Критерії оцінювання
5 («відмінно»)	У повному обсязі володіє навчальним матеріалом, вільно, самостійно та аргументовано його викладає, глибоко і всебічно розкриває зміст, використовуючи обов’язкову та додаткову літературу. Правильно вирішив 90% тестових завдань.
4 («добре»)	Достатньо повно володіє навчальним матеріалом, обґрунтовано його викладає, в основному розкриває зміст завдань, використовуючи обов’язкову літературу. При викладанні окремих питань не вистачає достатньої глибини та аргументації, допускаються несуттєві неточності й незначні помилки. Правильно вирішив більшість тестових завдань.
3 («задовільно»)	У цілому володіє навчальним матеріалом, викладає його основний зміст, але без глибокого всебічного аналізу, обґрунтування та аргументації, допускаючи окремі суттєві неточності та помилки. Правильно вирішив близько половини тестових завдань.
2 («незадовільно»)	Не в повному обсязі володіє навчальним матеріалом. Викладає матеріал фрагментарно та поверхово, без аргументації й обґрунтування, недостатньо розкриває зміст теоретичних і практичних завдань, допускає суттєві неточності. Правильно вирішив меншість тестових завдань.

Переведення підсумкових рейтингових оцінок з дисципліни, виражених у балах за 100-бальною шкалою, у оцінки за національною шкалою та шкалою ECTS

Таблиця 1 – **Шкала оцінювання: національна та ECTS**

Сума балів за всі види навчальної діяльності	Оцінка ECTS	Оцінка за національною шкалою	
		для екзамену, диференційованого заліку, курсового проєкту (роботи), практики	для заліку
90–100	**A**	відмінно	зараховано
82–89	**B**	добре	
74–81	**C**		
64–73	**D**	задовільно	
60–63	**E**		
35–59	**FX**	незадовільно з можливістю повторного складання	не зараховано з можливістю повторного складання
0–34	**F**	незадовільно з обов'язковим повторним вивченням дисципліни	не зараховано з обов'язковим повторним вивченням дисципліни

10. МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ

Підручники і навчальні посібники; інструктивно-методичні матеріали до практичних занять; індивідуальні навчально-дослідні завдання; контрольні роботи; текстові та електронні варіанти тестів для поточного контролю, методичні матеріали для організації самостійної роботи студентів, виконання індивідуальних завдань.

11. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Базова

1. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" від 05.07.1994 // Відомості Верховної Ради України, 1994, № 31. – Ст. 286, із змінами 2005 р.
2. Закон України "Про інформацію" // Відомості Верховної Ради, 1992, № 48. – Ст. 650 – 651.
3. Баранов, О. А. Інформаційна безпека: навч. посіб. / О. А. Баранов. – Київ: КНТ, 2020. – 312 с.
4. Єфіменко В. В. Технології захисту інформації: навч. посіб. / В. В. Єфіменко. – Київ: НАУ, 2021. – 198 с.
5. Загребельний А. В. Захист інформації в комп'ютерних системах: навч. посіб. / А. В. Загребельний, І. В. Козлов. – Львів: ЛНУ ім. І. Франка, 2019. – 280 с.
6. Коженевський С.Р. Термінологічний довідник з питань захисту інформації / С.Р. Коженевський, Г.В. Кузнецов, В.О. Хорошко, Д.В. Чирков. – К.: ДУІКТ, 2007. – 382 с.
7. Нестеров А. В. Криптографія та захист інформації: навч. посіб. / А. В. Нестеров. – Харків: Фоліо, 2021. – 256 с.

8. Хомич В. С. Основи інформаційної безпеки: навч. посіб. / В. С. Хомич. – Житомир: ЖДУ ім. І. Франка, 2020. – 224 с.

Допоміжна

1. ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення.
2. ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Проведення робіт.
3. Русин Б.П. Біометрична аутентифікація та криптографічний захист / Б.П. Русин, Я.Ю. Варецький. – Львів: «Коло», 2007. – 287 с.
4. Термінологічний довідник з питань технічного захисту інформації / Коженевський С.Р., Кузнецов Г.В., Хорошко В.О., Чирков Д.В. / За ред. проф. В.О. Хорошка. – К.: ДУІКТ, 2007. – 365 с.
5. General Data Protection Regulation (GDPR). Regulation (EU) 2016/679 of the European Parliament and of the Council. – Brussels: European Union, 2016. – [Електронний ресурс]. – Режим доступу: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679
6. PCI Security Standards Council. Payment Card Industry Data Security Standard: Requirements and Security Assessment Procedures. – Version 4.0. – Wakefield, MA: PCI SSC, 2022. – 139 p.
7. Ross Anderson. Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley, 2020.
8. William Stallings. "Cryptography and Network Security: Principles and Practice." Pearson, 2016. (784 p.) – https://www.pearson.com/us/highereducation/program/Stallings-Cryptography-and-Network-Security-Principles-and-Practice-7th-Edition/PGM335896.html
9. Ross Anderson. "Security Engineering: A Guide to Building Dependable Distributed Systems." Wiley, 2020. (1024 p.) – https://www.wiley.com/enus/Security+Engineering%3A+A+Guide+to+Building+Dependable+Distributed+Systems%2C+3rd+Edition-p-9781119642787
10. Brian Krebs. "Krebs on Security" – Online blog focusing on cybersecurity. – https://krebsonsecurity.com/

12. ІНФОРМАЦІЙНІ РЕСУРСИ

Бібліотечно-інформаційні ресурси

1. ISO/IEC 27001:2022. Information technology – Security techniques – Information security management systems – Requirements. – Geneva: International Organization for Standardization, 2022. – 33 p.
2. National Cyber Security Centre (NCSC) – Various publications and recommendations. – https://www.ncsc.gov.uk/
3. NIST SP 800-53 Rev. 5. Security and Privacy Controls for Information Systems and Organizations. – Gaithersburg, MD: National Institute of Standards and Technology, 2020. – 487 p. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

4. OWASP Foundation. OWASP Top Ten Web Application Security Risks – 2023. – [Електронний ресурс]. – Режим доступу: https://owasp.org/www-project-top-ten/

Інформаційні ресурси в Інтернеті

5. Coursera: Cybersecurity Specialization – Various courses from leading universities. – https://www.coursera.org/specializations/intro-cyber-security
6. http://dstszi.gov.ua.
7. ISO/IEC 27001:2013 – Information Security Management Systems – Requirements. https://www.iso.org/standard/54534.html
8. Virtual Hacking Labs – Practical labs for ethical hacking and penetration testing. – https://www.virtualhackinglabs.com/
9. www.rootshell.com.
10. www.securityfocus.com.
11. www.sysinternals.com.