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
«ІНФОРМАЦІЙНА БЕЗПЕКА»
(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 обов'язкова
(обов'язкова / за вибором)

2025–2026 навчальний рік

Робоча програма Інформаційна безпека
(назва навчальної дисципліни)

Укладачі: Ткачук Р.І. – д.т.н. професор кафедри інформаційних технологій
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 «27.08.2025року»
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	**7**	**7**
Кількість кредитів/годин	4/120	4/120
Усього годин аудиторної роботи	42	14
в т.ч.:		
– лекційні заняття, год.	14	6
– практичні заняття, год.	–	–
– лабораторні заняття, год.	28	8
– семінарські заняття, год.	–	–
Усього годин самостійної роботи	78	106
Форма контролю	іспит	іспит

Примітка.

Частка аудиторного навчального часу студента у відсотковому вимірі:

для денної форми здобуття освіти – 35%

для заочної форми здобуття освіти – 11.6%

1. МЕТА ТА ЗАВДАННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Метою вивчення освітньої компоненти «Інформаційна безпека» є всебічна теоретична та практична підготовка здобувачів вищої освіти. Ця підготовка спрямована на формування глибоких знань, умінь і навичок для ефективного захисту інформації в сучасних умовах.

Завдання навчальної дисципліни передбачають:

- Аналізувати та оцінювати ризики, пов'язані з інформаційною безпекою.
- Розробляти та впроваджувати комплексні стратегії та політики захисту даних.
- Використовувати сучасні технології та інструменти для запобігання кібератакам, виявлення вразливостей і реагування на інциденти.
- Забезпечувати конфіденційність, цілісність і доступність інформації.
- проєктувати та супроводжувати безпечні інформаційні системи.
- Визначати якість захисту інформації та керувати процесами її забезпечення.

Преквізити: для успішного опанування курсу «Інформаційна безпека» необхідно володіти знаннями з основ програмування, комп'ютерних мереж, операційних систем та адміністрування, а також мати навички роботи з алгоритмами і структурами даних, розуміти принципи 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 магістерських робіт, проходження практики, а також розроблення комплексних проєктів з кібербезпеки. 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 «Інформаційна безпека» є набуття студентами загальних компетентностей – здатність оцінювати та забезпечувати захист інформації в інформаційних системах, здатність оцінювати та забезпечувати якість виконуваних робіт, знання концепції інформаційної безпеки, принципів безпечного проєктування ІС а ІТ методології безпечного програмування, погроз і атак, безпеки комп'ютерних мереж. Фахових компетентностей – володіння навчально-методичними основами і стандартами в області ІТ, уміння їх застосовувати при розробці функціональних профілів ІТ, при побудові та інтеграції систем, продуктів і сервісів ІТ; здатність використовувати сучасні технології проєктування в розробці систем захисту інформації; здатність ефективно формувати комунікаційні стратегії у процесі формування концепції обміну інформацією, кодування та вибору каналу комунікації, передачі повідомлень і документів через канал, зберігання та добування документів, реалізації зворотного зв'язку.

Відповідно до освітньо-професійної програми «Комп'ютерні науки» вивчення дисципліни забезпечує 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.
Загальні компетентності	ЗК13. Здатність діяти на основі етичних міркувань
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. ПРН16. Виконувати паралельні та розподілені обчислення, застосовувати чисельні методи та алгоритми для паралельних структур, мови паралельного програмування при розробці та експлуатації паралельного та розподіленого програмного забезпечення

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 1 Семестр 2						Рік підготовки 1 Семестр 2					

Тема 1. Загальна характеристика управління проєктами, портфелями та програмами.	10	1	–	3	–	6	10	1	–	–	–	9
Тема 2. Ініціювання та планування змісту проєкту.	10	1	–	3	–	6	10	–	–	1	–	9
Тема 3. Структурування проєкту.	11	2	–	3	–	6	11	1	–	1	–	9
Тема 4. Планування змісту та часу проєктів.	11	2	–	3	–	6	11	1	–	1	–	9
Тема 5. Планування людських і матеріальних ресурсів проєкту.	11	2	–	3	–	6	11	–	–	2	–	9
Тема 6. Сутність бюджету проєкту, типові фор-ми, порядок складання.	11	2	–	3	–	6	11	1	–	–	–	10
Тема 7. Основні форми організаційної структури проєктів.	12	2	–	4	–	6	12	2	–	–	–	10
Тема 8. Управління проєктними ризиками.	14	2	–	6	–	6	14	–	–	3	–	11
Підготовка до навчальних занять та контрольних заходів.	30	–	–	–	–	30	30	–	–	–	–	30
Разом за семестр	120	14	–	28	0	78	120	6	–	8	0	106

3. ЛЕКЦІЙНІ ЗАНЯТТЯ

№ з/п	Назви тем та їх короткий зміст	Кількість годин	
		ДФЗО	ЗФЗО
1	Тема 1. Загальна характеристика управління проєктами, портфелями та програмами.	1	1
2	Тема 2. Ініціювання та планування змісту проєкту.	1	–
3	Тема 3. Структурування проєкту.	2	1
4	Тема 4. Планування змісту та часу проєктів.	2	1

5	Тема 5. Планування людських і матеріальних ресурсів проєкту.	2	–
6	Тема 6. Сутність бюджету проєкту, типові фор-ми, порядок складання.	2	1
7	Тема 7. Основні форми організаційної структури проєктів.	2	2
8	Тема 8. Управління проєктними ризиками.	2	–
Усього годин		14	6

4. ЛАБОРАТОРНІ ЗАНЯТТЯ

№ з/п	Назви тем та їх короткий зміст	Кількість годин	
		ДФЗО	ЗФЗО
1	Аналіз інформаційної безпеки в Україні.	3	–
2	Програмна реалізація і криптоаналіз шифрів з симетричними ключами.	3	1
3	Основи сучасної криптології. Шифр зсуву; шифр частоколу; шифр одноразового блокноту.	3	1
4	Класичні методи шифрування.	3	1
5	Шифрування за допомогою аналітичних перетворень.	3	2
6	Засоби забезпечення безпеки в операційних системах	3	–
7	Ідентифікація і аутентифікація користувача	4	–
8	Захист об'єктів системі	6	3
	Усього годин	28	8

5. САМОСТІЙНА РОБОТА

№ з/п	Назви тем та їх короткий зміст	Кількість годин	
		ДФЗО	ЗФЗО
1	Основні характеристики проєктів. Переваги та виклики під час управління портфелями проєктів.	6	9
2	Формування основних документів планування змісту.	6	9
3	Інструменти для структурування проєкту.	6	9
4	Оцінка тривалості завдань та загальної тривалості проєкту.	6	9
5	Використання матриць відповідальності у проєкті.	6	9
6	Контроль виконання бюджету проєкту.	6	10
7	Ідентифікація і аутентифікація користувача	6	10
8	Захист об'єктів системі	6	11
Іспит		30	30
	Усього годин	78	106

6. ІНДИВІДУАЛЬНІ ЗАВДАННЯ

–

7. МЕТОДИ НАВЧАННЯ

Навчання з дисципліни «Інформаційна безпека» 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 підсумкового контролю.

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.

Підсумковий контроль проводиться з метою оцінювання результатів навчання на завершальному етапі вивчення дисципліни. Підсумковий контроль здійснюється у формі екзамену.

9. КРИТЕРІЇ ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Успішність студента оцінюється шляхом проведення поточного та підсумкового контролю.

Максимальна кількість балів з дисципліни «Інформаційна безпека», яку може отримати студент протягом семестру за всі види роботи, становить 100, при цьому 50 балів за результатами поточного оцінювання, та 50 – за результатами екзаменаційного контролю.

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:

$$\mathbf{ПК = 10 \cdot САЗ}$$

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.Правове забезпечення інформаційної безпеки : курс лекцій / В. Фурашев, О. Радзієвська ; ДНУ «Ін-т інформ., безпеки і права Нац. акад. прав. наук України». – Київ; Одеса : Фенікс, 2022. 158 с. URL: https://ippi.org.ua/pravove-zabezpechennya-informatsiinoi-bezpeki

2. Правові засади забезпечення кібербезпеки в умовах цифрової трансформації: навчальний посібник / О. Довгань , Н. Ткачук , Т. Ткачук , В. Петров. – К., Артек. 2022. 171 с. URL: https://ippi.org.ua/pravovi-zasadi-zabezpechennya-kiberbezpeki-v-umovakh-tsifrovoi-transformatsii

3. Захист прав, приватності та безпеки людини в інформаційну епоху / Пилипчук В.Г., Брижко В.М., Доронін І.М. та ін. : монографія; за заг. ред. акад. НАПрН України В.Г. Пилипчука. – Київ-Одеса : Фенікс, 2020. 260 с. URL: https://ippi.org.ua/zakhist-prav-privatnosti-ta-bezpeki-lyudini-v-informatsiinu-epokhu

4. Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О. Довгань; упоряд. О. Довгань, Л. Литвинова, С. Дорогих; Державна наукова установа «Інститут інформації, безпеки і права НАПрН України»; Національна бібліотека України ім. В.І. Вернадського. URL: https://ippi.org.ua/kiberbezpeka-v-informatsiinomu-suspilstvi

Допоміжна

1. Русин Б.П. Біометрична аутентифікація та криптографічний захист / Б.П. Русин, Я.Ю. Варецький. – Львів: «Коло», 2007. – 287 с.

2. 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.

3. ДСанПіН 3.3.6.096-2002 Державні санітарні норми і правила при роботі з джерелами електромагнітних полів

4. ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення.

5. ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Проведення робіт.

12. ІНФОРМАЦІЙНІ РЕСУРСИ

1. Бібліотечно-інформаційні ресурси

– Бібліотека ЛНУВМБ: м. Дубляни, вул. В.Великого, 1; тел. 22-45-915

– Львівська наукова бібліотека ім. Стефаника НАН України: вул. Стефаника, 2; тел. 74-43-72

– Львівська обласна наукова бібліотека: просп. Шевченка, 13; тел.74-02-26

– Наукова бібліотека ЛНУ ім. Франка, метод. відділ: вул. Драгоманова, 17; тел. 296-42-41

– Центральна міська бібліотека ім Лесі Українки: вул. Мулярська, 2а; тел.72-05-81

2. Інформаційні ресурси в Інтернеті

1. http://dstszi.gov.ua.

2. Історія розвитку інформаційних технологій в Україні. – http://www.icfcst.kiev.ua/MUSEUM/IT_u.html

3. Нормативні акті Україн // https://www.nau.kiev.ua

4. https://www.rootshell.com.

5. https://www.securityfocus.com.

6. https://www.sysinternals.com.