МІНІСТРЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ
ВСП «РІВНЕНСЬКИЙ ФАХОВИЙ КОЛЕДЖ НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ»

Циклова комісія *програмування та інформаційних дисциплін*

ЗАТВЕРДЖУЮ
Заступник директора з навчальної роботи
29 серпня 2025 р.
_____ Людмила БАЛДИЧ

ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ОСНОВИ АРХІТЕКТУРИ І МОДЕЛІ БЕЗПЕКИ

(назва навчальної дисципліни)

освітньо-професійна програма *Кібербезпека*
(назва освітньо-професійної програми)

галузь знань *12 Інформаційні технології*
(шифр і назва напряму підготовки)

спеціальність *125 Кібербезпека*
(шифр і назва спеціальності)

відділення *Інформаційних технологій*
(назва відділення)

2025

Програма навчальної дисципліни з *основи архітектури і моделі безпеки* розроблена на основі освітньо-професійної програми «Кібербезпека» для здобувачів освіти освітньо-професійного ступеня «Фаховий молодший бакалавр» галузі знань *12 Інформаційні технології*, спеціальності *125 Кібербезпека*, затвердженої Вченою радою НУБіП України від 28.09.2022 р. № 2.

Розробники: *Масталярчук Євгеній Володимирович, спеціаліст вищої категорії, викладач програмування та інформаційних дисциплін*

(вказати авторів, їхні посади, наукові ступені та вчені звання)

Програма навчальної дисципліни затверджена на засіданні циклової комісії *програмування та інформаційних дисциплін*

Протокол від *29 серпня* 2025 року №1

Голова циклової комісії *програмування та інформаційних дисциплін*

29 серпня 2025 року _____ *Павло СТРИК*

Погоджено методичною радою ВСП «РФК НУБіП України»

Протокол від *29 серпня* 2025 року №1

29 серпня 2025 року Голова _____ *Людмила БАЛДИЧ*

1. Опис навчальної дисципліни

Галузь знань, напрям підготовки, спеціальність, освітньо-професійний ступінь	
Освітньо-професійний ступінь	фаховий молодший бакалавр
Галузь знань	12 Інформаційні технології
Спеціальність	125 Кібербезпека
Характеристика навчальної дисципліни	
Вид	**Обов'язкова**
Загальна кількість годин	**90**
Кількість кредитів ECTS	**3**
Кількість змістових модулів	2
Курсовий проект (робота) (якщо є в робочому навчальному плані)	
Мова викладання	Українська
Форма контролю	Залік
Показники навчальної дисципліни для денної форми навчання	
Форма навчання	денна форма навчання
Рік підготовки	2025-2026
Семестр	7
Аудиторні години:	44
Лекційні заняття	24
Практичні заняття	20
Самостійна робота	46
Кількість тижневих годин для денної форми навчання: аудиторних самостійної роботи студента –	4 год\тиждень 4 год\тиждень

2. Мета та завдання навчальної дисципліни

Метою навчальної дисципліни «Основи архітектури і моделі безпеки» є формування у здобувачів освіти системного розуміння принципів побудови архітектури інформаційних систем з урахуванням вимог безпеки, набуття знань про моделі, методи та засоби забезпечення інформаційної безпеки, а також розвиток умінь застосовувати теоретичні положення під час аналізу, проєктування та оцінювання захищеності комп'ютерних систем і мереж. Вивчення дисципліни спрямоване на усвідомлення ролі архітектурних рішень у формуванні комплексної системи захисту інформації, розуміння взаємозв'язку між елементами архітектури, принципами управління ризиками, політиками безпеки та технічними й організаційними засобами їх реалізації.

Основними завданнями дисципліни є формування у студентів знань щодо основних понять, принципів та структурних компонентів архітектури інформаційної безпеки, розкриття сутності та призначення моделей безпеки, які описують поведінку інформаційних систем у контексті конфіденційності, цілісності та доступності даних. Студенти повинні засвоїти класифікацію сучасних архітектур інформаційних систем, розуміти взаємодію між апаратним, програмним та організаційним рівнями забезпечення безпеки, а також оволодіти методами аналізу архітектурних ризиків і вразливостей. Важливим аспектом навчання є вивчення принципів побудови багаторівневих систем захисту, розроблення політик безпеки на рівні підприємства, застосування міжнародних стандартів і нормативних документів у сфері інформаційної безпеки, зокрема ISO/IEC 27001, ISO/IEC 15408 та NIST SP 800.

У межах дисципліни особлива увага приділяється вивченню архітектурних моделей безпеки, таких як модель Белла–ЛаПадули, Біби, Кларка–Вілсона, а також концепцій мандатного, дискреційного та рольового керування доступом. Студенти мають оволодіти методологією оцінювання ефективності архітектур безпеки, розуміти принципи побудови захищених систем з урахуванням життєвого циклу програмного забезпечення, уміти застосовувати сучасні інструменти і технології моніторингу та виявлення загроз. Вивчення дисципліни забезпечує підготовку фахівців, здатних здійснювати комплексний аналіз архітектури інформаційних систем, виявляти потенційні ризики, пропонувати обґрунтовані рішення для підвищення рівня безпеки та брати участь у проєктуванні і впровадженні систем захисту інформації на різних рівнях.

Таким чином, дисципліна «Основи архітектури і моделі безпеки» відіграє ключову роль у професійній підготовці майбутніх фахівців з комп'ютерної інженерії та інформаційної безпеки, сприяючи формуванню у них компетентностей, необхідних для розроблення, експлуатації та удосконалення надійних, стійких до зовнішніх і внутрішніх загроз інформаційних систем, що відповідають сучасним вимогам кібербезпеки.

3. Програма навчальної дисципліни

Змістовий модуль 1. Етапи становлення моделей інформаційної безпеки. основні види.

Тема 1. Поняття архітектури та історія розвитку.

Тема 2. Принципи побудови та організації системи захисту інформації.

Тема 3. Архітектурні моделі безпеки.

Змістовий модуль 2. Порівняльний аналіз моделей інформаційної безпеки та оцінка їхньої відповідності стандартам.

Тема 4. Концепції забезпечення конфіденційності, цілісності та доступності.

Тема 5. Багаторівневий захист та управління інцидентами.

Тема 6. Огляд стандартів у сфері інформаційної безпеки.

4. Структура навчальної дисципліни

№	*Назви змістових модулів і тем*	**Кількість годин**			
		денна форма			
		всього	лекційні	лабораторні	самостійне вивчення
1	*2*	*3*	*4*	*5*	*6*
ЗМІСТОВИЙ МОДУЛЬ 1. ЕТАПИ СТАНОВЛЕННЯ МОДЕЛЕЙ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ. ОСНОВНІ ВИДИ.					
Тема 1	Поняття архітектури та історія розвитку	8	2	0	6
Тема 2	Принципи побудови та організації системи захисту інформації	15	4	4	7
Тема 3	Архітектурні моделі безпеки.	15	4	4	7
	Разом за змістовим модулем 1	**38**	**10**	**8**	**20**
ЗМІСТОВИЙ МОДУЛЬ 2. ПОРІВНЯЛЬНИЙ АНАЛІЗ МОДЕЛЕЙ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА ОЦІНКА ЇХНЬОЇ ВІДПОВІДНОСТІ СТАНДАРТАМ.					
Тема 4	Концепції забезпечення конфіденційності, цілісності та доступності.	15	4	4	7
Тема 5	Багаторівневий захист та управління інцидентами.	15	4	4	7
Тема 6	Огляд стандартів у сфері інформаційної безпеки.	22	6	4	12
	Разом за змістовим модулем 2	**52**	**14**	**12**	**26**
	Всього	**90**	**24**	**20**	**46**

5. Теми лекційних, практичних занять та самостійного вивчення

№ теми	№ заняття	Вид навчальної діяльності	Назва теми	Кількість годин
			Змістовий модуль 1. Етапи становлення моделей інформаційної безпеки, основні види	**38**
1			**Поняття архітектури та історія розвитку**	**8**
	1	лекція 1	Вступ до дисципліни. Поняття архітектури інформаційних систем та безпеки. Основні терміни та визначення.	2
		самостійне вивчення	Історія розвитку архітектури комп'ютерних систем. Етапи становлення концепції інформаційної безпеки.	3
		самостійне вивчення	Аналіз архітектури типової інформаційної системи. Визначення потенційних загроз.	3
2			**Принципи побудови та організації системи захисту інформації**	**15**
	2	лекція 2	Основні принципи побудови архітектури інформаційної безпеки. Класифікація архітектурних рішень.	2
		самостійне вивчення	Види архітектур інформаційних систем: клієнт-серверна, трирівнева, сервісно-орієнтована, хмарна.	4
	3	практична робота 1	Визначення потенційних загроз. Моделювання архітектури безпечної інформаційної системи. Визначення компонентів безпеки.	2
	4	лекція 3	Основи організації системи захисту інформації. Політика безпеки та її структура.	2
		самостійне вивчення	Методи управління ризиками та формування політики інформаційної безпеки.	3
	5	практична робота 2	Розробка політики безпеки підприємства. Визначення рівнів доступу користувачів.	2
3			**Архітектурні моделі безпеки**	**15**
	6	лекція 4	Архітектурні моделі безпеки: призначення, класифікація та сфери застосування.	2
		самостійне вивчення	Модель Белла–ЛаПадули. Модель Біби. Основні характеристики та обмеження.	3
	7	практична робота 3	Побудова моделі доступу на прикладі моделей Белла–ЛаПадули та Біби.	2
	8	лекція 5	Модель Кларка–Вілсона. Модель китайського стіни. Порівняльний аналіз моделей безпеки.	2
		самостійне вивчення	Формальні методи опису моделей безпеки. Переваги та недоліки різних підходів.	4
	9	практична робота 4	Впровадження моделі рольового керування доступом (RBAC) у системах управління.	2
			Змістовий модуль 2. Порівняльний аналіз моделей інформаційної безпеки та оцінка їхньої відповідності стандартам.	**52**
4			**Концепції забезпечення конфіденційності, цілісності та доступності**	**15**
	10	лекція 6	Концепції контролю доступу: дискреційний, мандатний, рольовий, атрибутний підходи.	2
		самостійне вивчення	Порівняння механізмів контролю доступу. Аналіз практичних прикладів.	4
	11	практична робота 5	Проєктування системи контролю доступу для умовного підприємства.	2
	12	лекція 7	Методи забезпечення конфіденційності, цілісності та доступності інформації.	2
		самостійне вивчення	Криптографічні методи захисту даних. Симетричні та асиметричні алгоритми шифрування.	3
	13	практична робота 6	Реалізація базових криптографічних алгоритмів на прикладі прикладного середовища.	2
5			**Багаторівневий захист та управління інцидентами**	**15**
	14	лекція 8	Захист інформації в комп`ютерних мережах. Концепція багаторівневого захисту.	2
		самостійне вивчення	Протоколи безпеки мережі: SSL/TLS, IPSec, VPN.	3
	15	практична робота 7	Аналіз типових мережевих атак та розроблення методів їх запобігання.	2

	16	лекція 9	Управління інцидентами безпеки. Організація моніторингу та реагування на загрози.	2
		самостійне вивчення	Концепція SOC (Security Operations Center). Методи виявлення вторгнень.	4
	17	практична робота 8	Аналіз журналів подій безпеки. Виявлення аномалій у роботі системи.	2
6			**Огляд стандартів у сфері інформаційної безпеки**	**22**
	18	лекція 10	Стандарти та нормативні документи у сфері інформаційної безпеки. ISO/IEC 27001, 15408, NIST SP 800.	2
		самостійне вивчення	Національні нормативно-правові акти України у сфері захисту інформації.	3
	19	практична робота 9	Оцінювання відповідності системи вимогам стандартів інформаційної безпеки.	2
	20	лекція 11	Побудова архітектури захищених систем у контексті життєвого циклу програмного забезпечення.	2
		самостійне вивчення	Вимоги безпеки на етапах розроблення, тестування та експлуатації ПЗ.	3
	21	практична робота 10	Аналіз вразливостей у програмному забезпеченні та методи їх усунення.	2
	22	лекція 12	Тенденції розвитку архітектур безпеки та сучасні виклики кіберзахисту.	2
		самостійне вивчення	Сучасні підходи до кіберзахисту: Zero Trust, DevSecOps, Cloud Security.	3
		самостійне вивчення	Комплексний аналіз архітектури безпеки умовної інформаційної системи.	3
			Всього	**90**

6. Індивідуальні завдання студентам

№	Тема	Вид завдання (реферати, дослідно-розрахункові роботи тощо)	Календарні строки і форма контролю
1.	Поняття архітектури інформаційної системи та її роль у забезпеченні безпеки.	Реферат	Листопад
2.	Еволюція архітектур комп'ютерних систем і формування концепції інформаційної безпеки.	Реферат	Листопад
3.	Основні принципи побудови архітектури інформаційної безпеки.	Реферат	Листопад
4.	Політика безпеки як складова архітектури інформаційної системи.	Реферат	Листопад
5.	Модель безпеки Белла–ЛаПадули: принципи, обмеження, практичне застосування.	Реферат	Листопад
6.	Модель Біби: забезпечення цілісності інформації та аналіз практичних прикладів.	Реферат	Листопад
7.	Модель Кларка–Вілсона: контроль цілісності даних у корпоративних системах.	Реферат	Листопад
8.	Модель китайського стіни: захист від конфлікту інтересів у комерційних організаціях.	Реферат	Листопад
9.	Дискреційний контроль доступу: переваги та недоліки в сучасних системах.	Реферат	Листопад
10.	Мандатний контроль доступу: принципи реалізації та сфери використання.	Реферат	Листопад
11.	Рольовий контроль доступу (RBAC): особливості, структура та реалізація в IT-системах.	Реферат	Листопад
12.	Атрибутний контроль доступу (ABAC): сучасні тенденції розвитку систем авторизації.	Реферат	Листопад
13.	Методи управління ризиками в системах інформаційної безпеки.	Реферат	Листопад
14.	Архітектура багаторівневого захисту інформаційних систем.	Реферат	Листопад
15.	Криптографічні методи забезпечення конфіденційності	Реферат	Листопад

	даних.		
16.	Цифровий підпис як інструмент забезпечення цілісності та автентичності інформації.	Реферат	Листопад
17.	Методи захисту інформації в комп'ютерних мережах.	Реферат	Листопад
18.	Протоколи безпеки SSL/TLS, IPSec і VPN: принципи роботи та застосування.	Реферат	Листопад
19.	Аналіз типових мережевих атак та методів їх запобігання.	Реферат	Листопад
20.	Захист операційних систем: архітектурні підходи та засоби забезпечення безпеки.	Реферат	Листопад
21.	Безпека баз даних: архітектурні принципи, моделі доступу та контролю.	Реферат	Листопад
22.	Побудова систем моніторингу та реагування на інциденти безпеки.	Реферат	Листопад
23.	Концепція SOC (Security Operations Center) та її роль у сучасній організації.	Реферат	Листопад
24.	Системи виявлення та запобігання вторгнень (IDS/IPS): архітектура та функціонування.	Реферат	Листопад
25.	Стандарти інформаційної безпеки: ISO/IEC 27001, ISO/IEC 15408, NIST SP 800.	Реферат	Листопад
26.	Нормативно-правова база України у сфері захисту інформації.	Реферат	Листопад
27.	Моделі управління безпекою підприємства. Організаційна структура служби безпеки.	Реферат	Листопад
28.	Архітектурні рішення у сфері кібербезпеки критичної інфраструктури.	Реферат	Листопад
29.	Особливості побудови захищених хмарних систем. Cloud Security Architecture.	Реферат	Листопад
30.	Концепція Zero Trust: нова парадигма безпеки інформаційних систем.	Реферат	Листопад
31.	Інтеграція безпеки у процес розроблення ПЗ (DevSecOps).	Реферат	Листопад
32.	Методи аналізу вразливостей та тестування на проникнення.	Реферат	Листопад
33.	Захист IoT-пристроїв: архітектура, загрози, підходи до безпеки.	Реферат	Листопад
34.	Тенденції розвитку архітектур безпеки в епоху штучного інтелекту.	Реферат	Листопад
35.	Перспективи розвитку моделей інформаційної безпеки в умовах кіберзагроз нового покоління.	Реферат	Листопад

7. Перелік питань на залік (екзамен)

1. Поняття архітектури інформаційної системи. Основні складові та рівні архітектури.
2. Визначення та основні принципи архітектури інформаційної безпеки.
3. Основні загрози, вразливості та ризики в інформаційних системах.
4. Сутність і структура політики інформаційної безпеки. Етапи її розроблення.
5. Класифікація та характеристика основних моделей безпеки інформаційних систем.
6. Модель Белла–ЛаПадули: мета, правила доступу, особливості застосування.
7. Модель Біби: забезпечення цілісності даних, принципи реалізації.
8. Модель Кларка–Вілсона та модель китайського стіни: порівняльний аналіз.
9. Методи контролю доступу: дискреційний, мандатний, рольовий, атрибутний.
10. Основні принципи побудови багаторівневої архітектури захисту інформації.
11. Криптографічні методи забезпечення конфіденційності, цілісності та автентичності даних.
12. Засоби та методи захисту інформації в комп'ютерних мережах.
13. Призначення, структура та функції Центру оперативного моніторингу безпеки (SOC).
14. Міжнародні стандарти та нормативні документи у сфері інформаційної безпеки (ISO/IEC 27001, ISO/IEC 15408, NIST SP 800).
15. Сучасні тенденції розвитку архітектур безпеки: концепції Zero Trust, DevSecOps, Cloud Security.

16. Методи навчання

Під час вивчення дисципліни «Основи архітектури і моделі безпеки» у навчальному процесі застосовуються такі методи навчання: розповідь, бесіда, лекція, пояснення, демонстрація, ілюстрація, навчальна дискусія, диспут, самостійне виконання практичних завдань, розв'язування задач, виконання вправ.

17. Контроль результатів навчання

У процесі вивчення дисципліни використовуються наступні методи оцінювання навчальної роботи студента:

- індивідуальне опитування, фронтальне опитування;
- поточне тестування;
- підсумкове тестування з кожного змістовного модуля;
- усний залік.

Підсумковий рейтинг (за 50-бальною шкалою) за семестр з дисципліни визначається як середнє арифметичне рейтингів залікових модулів.

9.1. Форми та засоби поточного і підсумкового контролю

Основними методами контролю знань, умінь та навичок студентів є:

— спостереження за навчальною діяльністю студентів,
— усне опитування,
— письмовий контроль,
— практичний контроль,
— тестовий контроль.

Щоб результати були вагомішими, студентам необхідно рекомендувати потрібну навчальну, наукову, методичну, довідкову літературу, навчити орієнтуватися у книжковому потоці, користуватися як традиційними, так і електронними каталогами.

9.2. Критерії оцінювання результатів навчання

Оцінка «відмінно» виставляється студенту, який має стійкі системні, глибокі і різнобічні знання, відмінно володіє матеріалом, знає нормативну і законодавчу базу та її застосування за певних умов, дає обґрунтовані, правильні відповіді на питання, доцільно використовує термінологію дисципліни (предмета), усвідомлює взаємозв'язок окремих розділів дисципліни, їхнє значення для майбутньої професії, виявляє творчі здібності у розумінні та використанні навчально-програмного матеріалу, проявляє здатність до самостійного оновлення і поповнення знань. Практичні завдання і задачі вирішує правильно, розрахунки проводить без помилок, отримує достовірні результати, правильно заповнює і складає документи, робить відповідні узагальнення і висновки та охайно оформляє виконані завдання та звіти.

- глибоке, теоретично обґрунтоване розкриття питання; розрахунки, зроблені без помилок, проведено повний аналіз, відображена власна позиція – оцінюються в **48-50 балів**;
- обґрунтоване розкриття питання чи/та розрахунки, зроблені з незначними неточностями, які істотно не впливають на правильність відповіді – **45-47 балів**;

Оцінка «добре» виставляється студенту, який знає викладений матеріал і добре ним володіє але допускає незначні помилки у формулюванні термінів, категорій, понять, використанні нормативно-правової бази, показує стійкий рівень знань з дисципліни і та професійної діяльності. Під час виконання практичних завдань, вирішення задач, проведення розрахунків допускає незначні помилки, але за допомогою викладача швидко орієнтується і знаходить правильні відповіді, правильно або з незначними помилками заповнює і складає документи, робить відповідні узагальнення і висновки та охайно оформляє виконані завдання та звіти.

- відповідь не дає повного розкриття питання, не проведено повний аналіз результатів розрахунків, немає власної позиції – **42-44 балів**;

- неповне розкриття питання, доведені до завершення розрахунки але не зроблено їх аналіз; загалом наявні достатні знання – **38-41 балів**;

Оцінка «задовільно» виставляється студенту, який посередньо володіє матеріалом, виявив знання основного навчально-програмного матеріалу в обсязі, необхідному для подальшого навчання та наступної роботи за професією, справляється з виконанням завдань, передбачених програмою, дає неправильну відповідь на окремі питання або на всі питання дає малообґрунтовані, невичерпні відповіді, знання має обмежені, несистемні, слабо орієнтується у нормативно-правових документах. Під час виконання практичних завдань, вирішення задач, проведення розрахунків припускається грубих помилок і тільки за допомогою викладача може виправити допущені помилки, із значними помилками заповнює і складає документи, поверхово робить узагальнення і висновки та не зовсім охайно оформляє виконані завдання та звіти.

- питання розкрите фрагментарно, наявні фактологічні помилки під час викладу чи/та помилки під час проведення розрахунків – **34-37 балів**;
- відповідь неповна, наявні суттєві помилки при викладі та проведенні розрахунків – **30-33 балів**;

Оцінка «незадовільно» виставляється студенту, який не виявив достатніх знань основного навчально-програмного матеріалу, дає відповіді лише на деякі питання або дає неправильні відповіді на питання, може відтворити кілька термінів, не знає термінології дисципліни і основних нормативно-правових документів, не може без допомоги викладача використати знання у подальшому навчанні, не спромігся оволодіти навичками самостійної роботи. Допускає принципові помилки у виконанні передбачених програмою завдань, вирішенні задач, проведенні розрахунків припускається грубих помилок і не може їх виправити, не виконує практичне завдання у визначений термін, із значними помилками заповнює і складає документи, не робить узагальнення і висновки та не охайно оформляє виконані завдання та звіти.

- відповідь має значні помилки елементарного рівня – **1-30 бали**;
- відсутність відповіді на питання – **0 балів**.

9.3. Оцінювання за формами контролю

	Заліковий модуль 1	**Заліковий модуль 2**	**Заліковий модуль 3**	**Заліковий модуль 4**	**Заліковий модуль 5**	**Разом**
%	**20**	**20**	**20**	**20**	**20**	**100**
Мінімум	**0**	**0**	**0**	**0**	**0**	**0**
Максимум	**50**	**50**	**50**	**50**	**50**	**50**

9.4 Шкала оцінювання

Відсоток правильних відповідей	Рейтинг за п'ятидеся-тибальною шкалою	Оцінка за п'ятибальною шкалою	Запис у заліковій книжці студента та відомості	Оцінка за дванадцяти-бальною шкалою
97-100	49-50	5	відмінно	12
93-96	47-48	5	відмінно	11
90-92	45-46	5	відмінно	10
85-89	43-44	4	добре	9
80-84	40,41,42	4	добре	8
75-79	38,39	4	добре	7
69-74	35,36,37	3	задовільно	6
65-68	33-34	3	задовільно	5
60-64	30,31,32	3	задовільно	4
менше 60	0-29	2	незадовільно	2

10. Методичне забезпечення

1. Витяг з навчального плану
2. Програма навчальної дисципліни
3. Плани занять
4. Конспект лекцій з дисципліни
5. Завдання для обов'язкової контрольної роботи
6. Інструкційно-методичні матеріали до практичних занять
7. Інструкційно-методичні матеріали до самостійної роботи
8. Питання до заліків з модулів
9. Контрольні тестові завдання до заліків з модулів
10. Питання до заліку
11. Залікові білети
12. Презентації до тем

11.Рекомендовані джерела інформації

Базова

1. Бондаренко М. Ф., Баранов О. В. *Інформаційна безпека: теоретичні основи та організаційно-технічні аспекти.* — Київ: КНЕУ, 2020.
2. Гнатюк С. О. *Основи кібербезпеки: навчальний посібник.* — Київ: НАУ, 2021.
3. Іванченко А. В. *Архітектура інформаційних систем.* — Харків: ХНУРЕ, 2019.
4. Stallings W. *Computer Security: Principles and Practice.* — 5th ed. — Pearson, 2023.
5. Bishop M. *Computer Security: Art and Science.* — 2nd ed. — Addison-Wesley, 2019.
6. Ross A., NIST. *Security and Privacy Controls for Information Systems and Organizations (SP 800-53 Rev. 5).* — NIST, 2020.
7. Anderson R. *Security Engineering: A Guide to Building Dependable Distributed Systems.* — 3rd ed. — Wiley, 2020.
8. ISO/IEC 27001:2022 — *Information Security Management Systems — Requirements.* — Geneva: ISO, 2022.
9. Schneier B. *Applied Cryptography: Protocols, Algorithms, and Source Code in C.* — 20th Anniversary Edition. — Wiley, 2015.
10. Tanenbaum A. S., Van Steen M. *Distributed Systems: Principles and Paradigms.* — 2nd ed. — Pearson, 2017.

Допоміжна

1. Коваленко В. О. *Інформаційна безпека в комп'ютерних системах і мережах.* — Київ: Видавництво «Слово», 2022.
2. Гребенюк В. М. *Захист інформації в інформаційних системах: навчальний посібник.* — Львів: ЛНУ, 2021.
3. Whitman M. E., Mattord H. J. *Principles of Information Security.* — 7th ed. — Cengage Learning, 2022.
4. Pfleeger C., Pfleeger S. *Security in Computing.* — 6th ed. — Pearson, 2018.
5. ISO/IEC 15408:2022 — *Common Criteria for Information Technology Security Evaluation.* — Geneva: ISO, 2022.
6. Shostack A. *Threat Modeling: Designing for Security.* — Wiley, 2014.
7. NIST SP 800-160 Vol. 1 — *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems.* — NIST, 2018.