



Міжнародний гуманітарний університет
Факультет кібербезпеки, програмної інженерії та комп'ютерних наук
Кафедра комп'ютерної інженерії та інноваційних технологій

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

БЕЗПЕКА ПРОГРАМ ТА ДАНИХ

Галузь знань	12 Інформаційні технології
Спеціальність	121 Інженерія програмного забезпечення
Назва освітньої програми	Інженерія програмного забезпечення
Рівень вищої освіти	перший (бакалаврський)

Розробники і викладачі	Контактний телефон	Електронна адреса
доцент кафедри комп'ютерної інженерії та інноваційних технологій, к.т.н., Йона Лариса Григорівна	+380677463777	yonalarysa66@gmail.com

1. АНОТАЦІЯ ДО КУРСУ

Дисципліна «Безпека програм та даних» є обов'язковою дисципліною професійного циклу підготовки бакалаврів за спеціальністю 121 Інженерія програмного забезпечення і спрямована на формування у здобувачів вищої освіти знань і навичок забезпечення безпеки програмних систем і даних під час їх проектування, розроблення та експлуатації. Курс охоплює основні принципи безпечного проектування програмного забезпечення, моделі контролю доступу, аудит і управління вразливостями, застосування криптографічних механізмів, використання захищених протоколів передачі даних та захист даних у розподілених і хмарних середовищах. Вивчення дисципліни сприяє

формуванню здатності аналізувати вимоги до безпеки програмного забезпечення, застосовувати сучасні засоби захисту даних та забезпечувати цілісність і надійність програмних систем.

МЕТА ДИСЦИПЛІНИ. Метою дисципліни є формування у здобувачів вищої освіти знань про принципи забезпечення безпеки програмного забезпечення та даних і розвиток практичних навичок застосування програмних, криптографічних і мережевих механізмів захисту під час розроблення та експлуатації програмних систем.

ПЕРЕКВІЗИТИ. Передумовами для вивчення дисципліни є знання і вміння, отримані здобувачем при вивченні попередніх навчальних дисциплін бакалаврської підготовки: «Вища математика», «Дискретна математика», «Теорія імовірностей та математична статистика», «Теорія інформації і кодування», «Комп'ютерні мережі».

ПОСТРЕКВІЗИТИ. Знання і вміння, отримані здобувачем при вивченні даної навчальної дисципліни, можуть бути використані при вивченні дисципліни «Програмування інфокомунікаційних сервісів та систем», а також при виконанні кваліфікаційної роботи.

2. ОЧІКУВАНІ КОМПЕТЕНТНОСТІ, ЯКІ ПЛАНУЄТЬСЯ СФОРМУВАТИ, ТА ДОСЯГНЕННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ

У процесі реалізації програми дисципліни формуються наступні компетентності із передбачених освітньою програмою:

Інтегральна компетентність

Здатність розв'язувати складні спеціалізовані завдання або практичні проблеми інженерії програмного забезпечення, що характеризуються комплексністю та невизначеністю умов, із застосуванням теорій та методів інформаційних технологій.

Спеціальні (фахові, предметні) компетентності

K13. Здатність ідентифікувати, класифікувати та формулювати вимоги до програмного забезпечення.

K16. Здатність формулювати та забезпечувати вимоги щодо якості програмного забезпечення у відповідності з вимогами замовника, технічним завданням та стандартами.

K17. Здатність дотримуватися специфікацій, стандартів, правил і рекомендацій в професійній галузі при реалізації процесів життєвого циклу.

K18. Здатність аналізувати, вибирати і застосовувати методи і засоби для забезпечення інформаційної безпеки (в тому числі кібербезпеки).

K19. Володіння знаннями про інформаційні моделі даних, здатність створювати програмне забезпечення для зберігання, видобування та опрацювання даних.

K24. Здатність здійснювати процес інтеграції системи, застосовувати стандарти і процедури управління змінами для підтримки цілісності, загальної функціональності і надійності програмного забезпечення.

Результати навчання

ПР04. Знати і застосовувати професійні стандарти і інші нормативно-правові документи в галузі інженерії програмного забезпечення.

ПР10. Проводити передпроектне обстеження предметної області, системний аналіз об'єкта проектування.

ПР13. Знати і застосовувати методи розробки алгоритмів, конструювання програмного забезпечення та структур даних і знань.

ПР18. Знати та вміти застосовувати інформаційні технології обробки, зберігання та передачі даних.

ПР21. Знати, аналізувати, вибирати, кваліфіковано застосовувати засоби забезпечення інформаційної безпеки (в тому числі кібербезпеки) і цілісності даних відповідно до розв'язуваних прикладних завдань та створюваних програмних систем.

Заплановані результати навчання за навчальною дисципліною

Знання:

- основні принципи забезпечення безпеки програмного забезпечення та даних, модель CIA (конфіденційність, цілісність, доступність);
- класифікацію загроз, вразливостей і ризиків у програмних системах;
- архітектурні принципи побудови захищених програмних систем (defense in depth, принцип найменших привілеїв, мінімальна поверхня атаки);
- моделі контролю доступу (DAC, MAC, RBAC) та механізми ідентифікації, автентифікації й авторизації користувачів;
- криптографічні механізми захисту даних: симетричні та асиметричні алгоритми шифрування, криптографічні хеш-функції та цифрові підписи;
- принципи роботи захищених протоколів передачі даних (TLS/SSL, SSH, IPsec) та їх застосування у програмних системах;
- сучасні підходи до захисту даних у розподілених, хмарних і контейнерних середовищах, а також основи управління вразливостями (CVE, CVSS) та вимоги міжнародних стандартів інформаційної безпеки.

Уміння:

- аналізувати архітектуру програмних систем і середовище їх розгортання з метою виявлення потенційних вразливостей;
- оцінювати рівень захищеності програмного середовища на основі аналізу конфігурацій, прав доступу та журналів подій;

- обґрунтовано вибирати та застосовувати засоби забезпечення інформаційної безпеки під час розроблення та експлуатації програмного забезпечення;
- аналізувати ефективність механізмів захисту програмних систем від типових атак і визначати можливі ризики;
- розробляти заходи з підвищення рівня безпеки програмних систем і захисту даних з урахуванням вимог стандартів і політик безпеки.

Навички:

- застосовувати сучасні інструменти та технології захисту програмних систем і даних;
- використовувати криптографічні механізми для забезпечення конфіденційності, цілісності та автентичності даних;
- виконувати моніторинг подій безпеки та аналізувати системні і мережеві журнали для виявлення інцидентів;
- застосовувати інструменти управління вразливостями, оновленнями та конфігураціями для підтримки безпечного стану програмних систем.

3. ОБСЯГ ТА ОЗНАКИ КУРСУ

Загалом		Вид заняття (денна форма/заочна форма)				Ознаки курсу		
Кредитів ЄКТС	Годин	Лекційні заняття	Практичні заняття	Лабораторні роботи	Самостійна робота	Курс, (рік навчання)	Семестр	Обов'язкова / вибіркова
5	150	38/12	26/8	0/0	86/130	3	6	Обов'язкова

4. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Назви змістових модулів і тем	Кількість годин									
	Денна форма					Заочна форма				
	Заг.	у тому числі				Заг.	у тому числі			
		Лекц.	Практ.	Лаб.	Сам. роб.		Лекц.	Практ.	Лаб.	Сам. роб.
Тема 1. Архітектурні принципи безпеки програмних систем та операційних середовищ	22	6	4	0	12	22	2	0	0	20
Тема 2. Управління доступом та автентифікацією у програмних системах	22	6	4	0	12	22	2	2	0	18

Тема 3. Аудит безпеки, управління конфігураціями та вразливостями програмних систем	24	6	4	0	14	24	2	2	0	20
Тема 4. Мережеві механізми захисту та безпечна передача даних	30	8	6	0	16	30	2	2	0	26
Тема 5. Криптографічний захист даних та управління ключами	28	6	4	0	18	28	2	2	0	24
Тема 6. Захист даних у сучасних інформаційних системах та управління інцидентами безпеки	24	6	4	0	14	24	2	0	0	22
Загалом	150	38	26	0	86	150	12	8	0	130
Підсумковий контроль – екзамен										

5. ТЕХНІЧНЕ Й ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ / ОБЛАДНАННЯ

Здобувачі отримують теми та питання курсу, основну і додаткову літературу, рекомендації, завдання та оцінки за їх виконання як традиційним шляхом, так і з використанням платформ онлайн навчання на основі інформаційних систем Moodle або Google Classroom. Практичні навички у пошуку та аналізу інформації за курсом, з оформлення індивідуальних завдань, тощо, здобувачі можуть отримувати як за допомогою власного обладнання, так і користуючись університетськими комп'ютерними класами та бібліотекою.

6. САМОСТІЙНА РОБОТА

До самостійної роботи здобувачів відносяться наступні види діяльності:

1. Опрацювання лекційного матеріалу.
2. Підготовка до практичних занять.
3. Консультації з викладачем впродовж семестру.
4. Ознайомлення з додатковою літературою відповідно до зазначених у програмі тем.
5. Самостійне опрацювання окремих питань навчальної дисципліни.
6. Підготовка індивідуальних завдань у вигляді презентацій або рефератів.
7. Підготовка до підсумкового контролю.

Назва теми	Кількість годин	
	Денна форма	Заочна форма
Тема 1. Архітектурні принципи безпеки програмних систем та операційних середовищ 1. Поняття безпеки програмного забезпечення та даних. Модель CIA (конфіденційність, цілісність, доступність) як основа побудови систем захисту. 2. Поняття загроз, вразливостей і ризиків у програмних системах. 3. Принципи безпечного проєктування: defense in depth, принцип найменших привілеїв, мінімальна поверхня атаки. 4. Архітектурна роль операційної системи у забезпеченні захисту програм і даних. 5. Принципи ізоляції процесів і ресурсів в операційних системах та їх значення для безпеки програмного середовища. 6. Віртуалізація і контейнеризація як засоби ізоляції та моделювання безпечного програмного середовища.	12	20
Тема 2. Управління доступом та автентифікацією у програмних системах 1. Моделі контролю доступу: дискреційна (DAC), обов'язкова (MAC), рольова (RBAC). 2. Ідентифікація, автентифікація та авторизація користувачів у програмних системах. 3. Управління обліковими записами користувачів і служб, політики паролів та багатофакторна автентифікація. 4. Принцип найменших привілеїв у багатокористувацьких операційних системах. 5. Характеристика атак типу brute force, dictionary attack, credential stuffing та методи їх виявлення. 6. Принципи роботи систем виявлення та запобігання вторгненням (IDS/IPS).	12	18
Тема 3. Аудит безпеки, управління конфігураціями та вразливостями програмних систем 1. Поняття аудиту безпеки та його місце в життєвому циклі системи захисту. 2. Етапи проведення аудиту: збір інформації, аналіз, оцінка ризиків, формування рекомендацій. 3. Стандарти та методики аудиту безпеки (CIS Benchmarks, NIST SP 800). 4. Автоматизовані інструменти аудиту безпеки та інтерпретація результатів перевірки. 5. Поняття CVE та CVSS, процес управління вразливостями програмного забезпечення. 6. Управління конфігураціями та оновленнями як складова підтримки безпечного стану системи.	14	20
Тема 4. Мережеві механізми захисту та безпечна передача даних 1. Поняття мережевого фаєрволу та архітектура фільтрації трафіку. 2. Типи фільтрації трафіку: за адресами, портами, протоколами та станом з'єднання. 3. Трансляція мережевих адрес (NAT) та логування мережевих подій у контексті забезпечення безпеки. 4. Принципи побудови захищених протоколів передачі даних. Протоколи SSH, TLS/SSL, IPsec. 5. Сертифікати X.509, ланцюги довіри та типові помилки конфігурації захищених протоколів. 6. Віртуальні приватні мережі (VPN), їх топології та практичні аспекти побудови захищених тунелів.	16	26
Тема 5. Криптографічний захист даних та управління ключами 1. Роль криптографії у забезпеченні конфіденційності, цілісності та автентичності даних. 2. Симетричні та асиметричні алгоритми шифрування, криптографічні хеш-функції та цифрові підписи. 3. Практичне застосування криптографії для захисту файлів, повідомлень і резервних копій. 4. Життєвий цикл криптографічних ключів: генерація, зберігання, розповсюдження, ротація та відклик. 5. Апаратні та програмні засоби захисту ключів (HSM, TPM, токени). 6. Основи інфраструктури відкритих ключів (PKI) та стандарти управління ключами.	18	24

Тема 6. Захист даних у сучасних інформаційних системах та управління інцидентами безпеки 1. Особливості зберігання та обробки даних у розподілених, хмарних та контейнерних середовищах. 2. Захист даних at rest та in transit, управління секретами та обліковими даними сервісів. 3. Модель Zero Trust та принципи мінімізації привілеїв у сучасних інформаційних системах. 4. Моніторинг безпеки та джерела подій: системні і прикладні журнали, мережеві логи. 5. Основи реагування на інциденти інформаційної безпеки та відновлення функціонування систем. 6. Нормативні та міжнародні стандарти у сфері захисту інформації та комплексний підхід до захисту програм і даних.	14	22
Загалом	86	130

7. ВИДИ ТА МЕТОДИ КОНТРОЛЮ

Види контролю	Складові оцінювання
Поточний контроль , який здійснюється під час проведення практичних (лабораторних) занять, виконання самостійної роботи, індивідуальних завдань, дослідної роботи здобувача тощо	50%
Підсумковий контроль , який здійснюється у ході проведення екзамену	50%

Методи діагностики знань (контролю)	Фронтальне опитування, розв'язання практичних завдань, тестування здобувачів, наукові доповіді, реферати, усні повідомлення, екзамен
--	--

8. ОЦІНЮВАННЯ ПОТОЧНОЇ, САМОСТІЙНОЇ ТА ІНДИВІДУАЛЬНОЇ РОБОТИ ЗДОБУВАЧІВ

Види роботи	Планові терміни виконання	Форми контролю та звітності	Максимальний відсоток оцінювання
Систематичність і активність роботи на практичних заняттях			
1.1. Підготовка до практичних занять	Відповідно до робочої програми та розкладу занять	Перевірка обсягу та якості засвоєного матеріалу під час практичних занять	30

Виконання завдань для самостійного опрацювання			
1.2. Індивідуальне тестування	Відповідно до робочої програми та розкладу занять	Перевірка результатів індивідуального тестування, перевірка конспектів лекцій, перевірка рефератів	10
Виконання індивідуальних завдань (дослідна робота здобувача)			
1.3. Інші види індивідуальних завдань, в т.ч. підготовка наукових публікацій, участь у роботі круглих столів, конференцій тощо.	Відповідно до робочої програми та розкладу занять	Обговорення результатів проведеної роботи під час аудиторних занять, наукових конференцій та круглих столів.	10
Разом балів за поточний контроль			50
Підсумковий контроль – екзамен			50
Загальний результат оцінювання			100

Поточний контроль знань здобувачів при підсумковому контролі у формі екзамену (максимум 50 балів) оцінюється за шкалою («2», «3», «4», «5»), з обов'язковим переведенням балів за кожний вид роботи таким чином:

– за підготовку до аудиторних занять (максимум 30 балів) здобувачу освіти необхідно мати не менше 1/2 оцінок від загальної кількості практичних (лабораторних) занять, для переведу балів за підготовку до аудиторних занять середньоарифметична оцінка множиться на коефіцієнт 6;

– за виконання завдань для самостійного опрацювання (тестування, завдання, підготовка реферату за заданою тематикою) (максимум 10 балів) здобувачу освіти необхідно мати не менше 1/2 оцінок від загальної кількості програмного матеріалу, що виноситься на самостійне вивчення, для переведу зазначених балів середньоарифметична оцінка множиться на коефіцієнт 2;

– за інші види індивідуальних завдань, в т.ч. підготовку наукових публікацій, участь у роботі круглих столів, конференцій тощо (максимум 10 балів) здобувачу освіти необхідно мати не менше 1/2 оцінок від загальної кількості інших видів індивідуальних завдань, для переведу балів за підготовку до аудиторних занять середньоарифметична оцінка множиться на коефіцієнт 2.

Критерії оцінювання поточного контролю

– «2» – виставляється за неправильну відповідь (письмову роботу), яка не відповідає змісту теми та свідчить про нерозуміння її основних положень;

– «3» – виставляється за відповідь (письмову роботу), яка відповідає змісту теми, але є неповною і неточною у визначенні понять, свідчить про неповне розуміння основних положень навчального матеріалу, свідчить про те, що знання здобувача мають фрагментарний, поверховий характер;

– «4» – оцінюється правильна і обґрунтована відповідь (письмова робота), з якої видно, що здобувач знає й розуміє теоретичний матеріал в обсязі навчальної теми, володіє необхідними навичками, не допускає суттєвих помилок.

– «5» – оцінюється повна, правильна, ґрунтовна відповідь (письмова робота) на запитання теми, що передбачає логічність і послідовність викладу матеріалу, володіння термінологією, показує вміння повно й глибоко використовувати теоретичні знання в практичній площині.

Критерії оцінювання підсумкового контролю у формі екзамену

Максимальна оцінка підсумкового контролю у формі екзамену не може перевищувати 50 балів. При цьому рівень знань оцінюється:

– **від 40 до 50 балів** – здобувач виявляє особливі творчі здібності, вміє самостійно знаходити та опрацьовувати необхідну інформацію, демонструє знання матеріалу, проводить узагальнення і висновки;

– **від 30 до 40 балів** – здобувач володіє знаннями матеріалу, але допускає незначні помилки у формуванні термінів, категорій, проте за допомогою викладача швидко орієнтується і знаходить правильні відповіді;

– **від 20 до 30 балів** – здобувач відтворює значну частину теоретичного матеріалу, виявляє знання і розуміння основних положень, з допомогою викладача може аналізувати навчальний матеріал, але дає недостатньо обґрунтовані, невичерпні відповіді, допускає помилки.

– **від 10 до 20 балів** – здобувач володіє навчальним матеріалом на середньому рівні, допускає помилки, серед яких є значна кількість суттєвих;

– **від 0 до 10 балів** – здобувач володіє навчальним матеріалом на рівні, вищому за початковий, значну частину його відтворює на репродуктивному рівні, на всі запитання дає необґрунтовані, невичерпні відповіді, допускає помилки.

9. ОЦІНЮВАННЯ ЗАГАЛЬНИХ РЕЗУЛЬТАТІВ ЗНАНЬ ЗДОБУВАЧІВ

Загальні результати знань здобувачів по даній дисципліні оцінюються наступним чином:

– **«Відмінно»/«зараховано» (А)** – від 90 до 100 балів. Здобувач виявляє особливі творчі здібності, вміє самостійно знаходити та опрацьовувати необхідну інформацію, демонструє знання матеріалу, проводить узагальнення і висновки. Був присутній на лекціях та практичних заняттях, під час яких давав вичерпні, обґрунтовані, теоретично і практично правильні відповіді, має конспект з виконаними завданнями до самостійної роботи, презентував реферат за заданою тематикою, проявляє активність і творчість у науково-дослідній роботі;

– **«Добре»/«зараховано» (В)** – від 82 до 89 балів. Здобувач володіє знаннями матеріалу, але допускає незначні помилки у формуванні термінів, категорій, проте за допомогою викладача швидко орієнтується і знаходить правильні відповіді. Був присутній на лекціях та практичних заняттях, має конспект з виконаними завданнями до самостійної роботи, презентував реферат за заданою тематикою, проявляє активність і творчість у науково-дослідній роботі;

– **«Добре»/«зараховано» (С)** – від 74 до 81 балів. Здобувач відтворює значну частину теоретичного матеріалу, виявляє знання і розуміння основних положень, з допомогою викладача може аналізувати навчальний матеріал, але дає недостатньо обґрунтовані, невичерпні відповіді, допускає помилки. При цьому враховується наявність конспекту з виконаними завданнями до самостійної роботи, реферату та активність у науково-дослідній роботі;

– **«Задовільно»/«зараховано» (D)** – від 64 до 73 балів. здобувач був присутній не на всіх лекціях та практичних заняттях, володіє навчальним матеріалом на середньому рівні, допускає помилки, серед яких є значна кількість суттєвих. При цьому враховується наявність конспекту з виконаними завданнями до самостійної роботи та рефератів;

– **«Задовільно»/«зараховано» (E)** – від 60 до 63 балів. Здобувач був присутній не на всіх лекціях та практичних заняттях, володіє навчальним матеріалом на рівні, вищому за початковий, значну частину його відтворює на репродуктивному рівні, на всі запитання дає необґрунтовані, невичерпні відповіді, допускає помилки, має неповний конспект з завданнями до самостійної роботи.

– **«Незадовільно з можливістю повторного складання»/«не зараховано» (FX)** – від 35 до 59 балів. Здобувач володіє матеріалом на рівні окремих фрагментів, що становлять незначну частину навчального матеріалу.

– **«Незадовільно з обов'язковим повторним вивченням дисципліни»/«не зараховано» (F)** – від 0 до 34 балів. Здобувач не володіє навчальним матеріалом.

Таблиця відповідності результатів контролю знань за різними шкалами

100-бальна шкала	Шкала ECTS	Національна шкала	
		екзамен	залік
90-100	A	Відмінно	Зараховано
82-89	B	Добре	Зараховано
74-81	C		
64-73	D	Задовільно	Зараховано
60-63	E		
35-59	FX	Незадовільно	Не зараховано
0-34	F		

10. ДОТРИМАННЯ ВИМОГ АКАДЕМІЧНОЇ ДОБРОЧЕСНОСТІ

Викладання та засвоєння навчальної дисципліни передбачає неухильне дотримання вимог академічної доброчесності, яка регулюється Законом України «Про освіту» (Відомості Верховної Ради (ВВР), 2014, № 37-38, ст. 2004), «Методичними рекомендаціями для закладів вищої освіти з підтримки принципів академічної доброчесності» (Лист МОН № 1/9-650 від 23.10.2018), іншими нормативними документами. Зокрема, основні засади дотримання академічної доброчесності визначено у «Положенні про академічну доброчесність у Міжнародному гуманітарному університеті», «Кодексі академічної доброчесності Міжнародного гуманітарного університету» та «Інструкції щодо процедури технічної перевірки на наявність текстових запозичень (академічного плагіату)», затверджені наказом Міжнародного гуманітарного університету № 708а від 03.05.2024.

Відповідно до ст. 42 Закону України «Про освіту» академічна доброчесність – це сукупність етичних принципів та визначених законом правил, якими мають керуватися учасники освітнього процесу під час навчання, викладання та провадження наукової (творчої) діяльності з метою забезпечення довіри до результатів навчання та/або наукових (творчих) досягнень.

Дотримання академічної доброчесності передбачає:

- самостійне виконання навчальних завдань, завдань поточного та підсумкового контролю результатів навчання (для осіб з особливими освітніми потребами ця вимога застосовується з урахуванням їхніх індивідуальних потреб і можливостей);
- посилення на джерела інформації у разі використання ідей, розробок, тверджень, відомостей;
- дотримання норм законодавства про авторське право і суміжні права;
- надання достовірної інформації про результати власної навчальної (наукової, творчої) діяльності, використанні методики досліджень і джерела інформації.

11. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

1. Горбенко В. І., Лісняк А. О. Безпека програм та даних : навчальний посібник для здобувачів ступеня вищої освіти бакалавра спеціальності 121 «Інженерія програмного забезпечення» освітньо-професійної програми «Програмна інженерія». Запоріжжя : ЗНУ, 2022. — 72 с.
2. Сенів М. М. Безпека програм та даних : навч. посібник / М. М. Сенів, В. С. Яковина. — Львів : Львівська політехніка, 2015. — 256 с.
3. Дем'яненко В. А. Безпека програм та даних [Електронний ресурс] : навч. посіб. до лаб. практикуму / В. А. Дем'яненко, Ю. А. Кузнецова. — Харків : Нац. аерокосм. ун-т ім. М. Є. Жуковського «Харків. авіац. ін-т», 2021. — 95 с.
4. Євсєєв С. П. Лабораторний практикум з основ криптографічного захисту [Електронний ресурс] : навчальний посібник / С. П. Євсєєв, О. В. Мілов, О. Г. Король. — Харків : ХНЕУ ім. С. Кузнеця, 2020. — 222 с.
5. Технології захисту інформації в інформаційно-телекомунікаційних системах : навч. посібник / А. В. Жилін, О. М. Шаповал, О. А. Успенський ; ІСЗЗІ КПП ім. Ігоря Сікорського. — Київ : Вид-во «Політехніка» КПП ім. Ігоря Сікорського, 2021. — 213 с.
6. Кузнецов О. О. Захист інформації в інформаційних системах : навч. посіб. — Х. : ХНЕУ, 2018. — 510 с.
7. Мамченко С. М. Комплексні системи захисту інформації: навч. посіб. / С. М. Мамченко, В. Д. Козюра, В. Д. Бровко. — Київ: Нац. Акад. СБУ, 2018. — 372 с.

Допоміжна

8. Остапов С. Є. Технології захисту інформації / С. Є. Остапов, С. П. Євсєєв, О. Г. Король. — Чернівці : Видавничий дім «Родовід», 2014. — 428 с.
9. Захист інформації в автоматизованих системах управління : навч. посібник / уклад.: І. А. Пількевич, Н. М. Лобанчикова, К. В. Молодецька. — Житомир : Вид-во ЖДУ ім. І. Франка, 2015. — 226 с.
10. Літнарович Р. М. Сучасні технології інформаційної безпеки : навч. посібник. — Рівне : МЕНУ, 2011. — 97 с.
11. Кузнецов О. О. Захист інформації в інформаційних системах. Методи традиційної криптографії / О. О. Кузнецов, С. П. Євсєєв, О. Г. Король. — Харків : Вид-во ХНЕУ, 2010. — 316 с.
12. Згуровський М. Проблеми інформаційної безпеки в Україні, шляхи їх вирішення // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. — Київ, 2018. — С. 10–14.

13. Дудатьєв А. В. Захист програмного забезпечення. Ч. 1 : навч. посібник / А. В. Дудатьєв, В. А. Каплун, В. П. Семеренко. — Вінниця : ВНТУ, 2005. — 140 с.
14. Мельник І. В. Інформаційні комп'ютерні мережі : навч. посібник для дист. навчання. — К. : Вид-во Універ. «Україна», 2006. — 250 с.
15. Столлінгс В. Криптографія та захист мереж: принципи й практика / В. Столлінгс ; пер. з англ. — 2-е вид. — К. : Видавничий дім «Вільямс», 2001. — 672 с.
16. Богуш В. М., Давидьков О. А. Теоретичні основи захищених інформаційних технологій. — К. : ДУІКТ, 2010. — 414 с.
17. Довгань О. Д. Методологія захисту інформації: навч.-метод. посіб. / О. Д. Довгань, Г. М. Гулак, А. К. Гринь, С. В. Мельник. — К. : Наук.-вид. центр НА СБ України, 2012. — 184 с.
18. Ленков С. В. Методи і засоби захисту інформації / С. В. Ленков, Д. А. Перегудов, В. А. Хорошко; за ред. В. А. Хорошко. — К. : Арий, 2008. — Т. II. Інформаційна безпека. — 344 с.
19. Грайворонський М. В., Новіков О. М. Безпека інформаційно-комунікаційних систем. — К. : Видавнича група BHV, 2009. — 608 с.
20. Юдін О. К., Корченко О. Г., Конахович В. Г. Захист інформації в мережах передачі даних. — К. : Вид-во ТОВ НВП «ІНТЕРСЕРВІС», 2009. — 716 с.

Інформаційні ресурси

21. Онлайн бібліотека «Лібком» : URL: <http://www.lib.com.ua>
22. MIT OpenCourseWare (OCW) : URL: <https://ocw.mit.edu/>
23. Dive into Systems : URL: <https://diveintosystems.org/>
24. Open Textbook Library : URL: <https://open.umn.edu/opentextbooks>
25. Directory of Open Access Books (DOAB) : URL: <https://www.doabooks.org/> .
26. Internet Engineering Task Force (IETF) : URL: <https://www.ietf.org/>
27. RFC Editor : URL: <https://www.rfc-editor.org/>
28. National Institute of Standards and Technology (NIST) – Computer Security Resource Center : URL: <https://csrc.nist.gov/>
29. OWASP (Open Web Application Security Project) : URL: <https://owasp.org/>
30. IEEE Standards Association : URL: <https://standards.ieee.org/>
31. Wireshark Documentation : URL: <https://www.wireshark.org/docs/>
32. SANS Institute Reading Room : URL: <https://www.sans.org/white-papers/>
33. ENISA (European Union Agency for Cybersecurity) : URL: <https://www.enisa.europa.eu/>