Міністерство освіти і науки України
Міжнародний гуманітарний університет
Кафедра комп'ютерної інженерії та інноваційних технологій

Йона Л.Г.

БЕЗПЕКА ПРОГРАМ ТА ДАНИХ

Методичні рекомендації для самостійної роботи здобувачів
першого (бакалаврського) рівня спеціальності
«Інженерія програмного забезпечення»

Одеса 2025

Затверджено Вченою Радою Міжнародного гуманітарного університету.
Протокол № 5 від 20 січня 2025 р.

Йона Л.Г. Безпека програм та даних. Методичні рекомендації для самостійної роботи здобувачів першого (бакалаврського) рівня спеціальності «Інженерія програмного забезпечення» [Електронне видання]. Кафедра комп'ютерних наук Міжнародного гуманітарного університету. Одеса, 2025. 20 с.

Методичні рекомендації для курсу «Безпека програм та даних» призначені для самостійної роботи здобувачів, що навчаються за першим (бакалаврським) рівнем за спеціальністю «Інженерія програмного забезпечення». Методичні рекомендації розроблені відповідно навчального плану. До складу методичних рекомендацій входять навчальна програма, теми практичних занять та самостійної роботи студентів. Матеріали призначено для студентів факультету кібербезпеки, програмної інженерії та комп'ютерних наук Міжнародного гуманітарного університету.

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 проєктування, розроблення та експлуатації. Курс охоплює основні принципи безпечного проєктування 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.

ЗМІСТ

1 ЗМІСТ ДИСЦИПЛІНИ 4
2 ПРОГРАМА ДИСЦИПЛІНИ 7
3 ПИТАННЯ ДО ПРАКТИЧНИХ ЗАНЯТЬ 9
4 САМОСТІЙНА РОБОТА 11
5 ВИДИ ТА МЕТОДИ КОНТРОЛЮ.....13
6 КРИТЕРІЇ ПІДСУМКОВОЇ ОЦІНКИ ЗНАНЬ СТУДЕНТІВ 14
7 ОЦІНЮВАННЯ ЗАГАЛЬНИХ РЕЗУЛЬТАТІВ ЗНАНЬ ЗДОБУВАЧІВ 16
8 ДОТРИМАННЯ ВИМОГ АКАДЕМІЧНОЇ ДОБРОЧЕСНОСТІ.....17
9 РЕКОМЕНДОВАНА ЛІТЕРАТУРА.....17

1 ЗМІСТ ДИСЦИПЛІНИ

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 проєктування, розроблення та експлуатації. Курс охоплює основні принципи безпечного проєктування 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.

ПРЕРЕКВІЗИТИ. 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.

Результати навчання та компетентності, заплановані освітньою програмою

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

К13. Здатність ідентифікувати, класифікувати та формулювати вимоги до програмного забезпечення.

К16. Здатність формулювати та забезпечувати вимоги щодо якості програмного забезпечення у відповідності з вимогами замовника, технічним завданням та стандартами.

К17. Здатність дотримуватися специфікацій, стандартів, правил і рекомендацій в професійній галузі при реалізації процесів життєвого циклу.

К18. Здатність аналізувати, вибирати і застосовувати методи і засоби для забезпечення інформаційної безпеки (в тому числі кібербезпеки).

К19. Володіння знаннями про інформаційні моделі даних, здатність створювати програмне забезпечення для зберігання, видобування та опрацювання даних.

К24. 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.

2 ПРОГРАМА ДИСЦИПЛІНИ

Назви змістових модулів і тем	Кількість годин									
	Денна форма					Заочна форма				
	Заг.	у тому числі				Заг.	у тому числі			
		Лек.	Прак.	Лаб.	Сам. роб.		Лек.	Прак.	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										

Тема 1. Архітектурні принципи безпеки програмних систем та операційних середовищ

Поняття безпеки програмного забезпечення та даних. Модель CIA (конфіденційність, цілісність, доступність) як основа побудови систем захисту. Поняття загроз, вразливостей і ризиків. Принципи безпечного проєктування: defense in depth, принцип найменших привілеїв, мінімальна поверхня атаки. Архітектурна роль операційної системи у забезпеченні захисту програм і даних. Урахування вимог безпеки під час проєктування програмних систем.

Принципи ізоляції процесів і ресурсів в операційних системах. Віртуалізація як інструмент забезпечення безпеки та моделювання атак і захисних механізмів. Типи віртуалізації та їх вплив на рівень захищеності. Контейнери як легковаговий механізм ізоляції. Використання віртуальних середовищ для аналізу вразливостей програмного забезпечення та тестування політик безпеки.

Тема 2. Управління доступом та автентифікацією у програмних системах

Моделі контролю доступу: дискреційна (DAC), обов’язкова (MAC), рольова (RBAC). Ідентифікація, автентифікація та авторизація користувачів. Управління обліковими записами

користувачів і служб. Політики паролів, багатофакторна автентифікація. Принцип найменших привілеїв у багатокористувацьких операційних системах і програмних сервісах.

Характеристика атак типу brute force, dictionary attack, credential stuffing. Джерела даних для виявлення атак: журнали автентифікації, системні логи, мережеві події. Принципи роботи систем виявлення та запобігання вторгненням (IDS/IPS). Реалізація механізмів автоматичного блокування зловмисних дій. Захист механізмів автентифікації у програмних системах і вебсервісах.

Тема 3. Аудит безпеки, управління конфігураціями та вразливостями програмних систем

Поняття аудиту безпеки та його місце в життєвому циклі системи захисту. Етапи проведення аудиту: збір інформації, аналіз, оцінка ризиків, формування рекомендацій. Стандарти та методики аудиту (CIS Benchmarks, NIST SP 800). Автоматизовані інструменти аудиту безпеки. Аналіз конфігурацій операційних систем і програмних сервісів. Інтерпретація результатів перевірки та формування заходів з підвищення рівня захищеності.

Роль оновлень у запобіганні експлуатації відомих вразливостей. Поняття CVE та CVSS. Процес управління вразливостями програмного забезпечення. Перевірка цілісності програмних пакетів. Автоматизація оновлення безпеки. Управління конфігураціями як складова підтримки безпечного стану програмних систем.

Тема 4. Мережеві механізми захисту та безпечна передача даних

Поняття мережевого фаєрволу та його роль у захисті програмного середовища. Архітектура фільтрації трафіку. Типи фільтрації: за адресами, портами, протоколами, станом з'єднання. Таблиці та ланцюги правил. Трансляція мережевих адрес (NAT) як елемент безпеки. Логування мережевих подій і підготовка до аналізу інцидентів. Захист мережевих інтерфейсів програмних систем.

Принципи побудови захищених протоколів передачі даних. Протоколи SSH, TLS/SSL, IPsec та їх призначення. Процеси автентифікації, узгодження параметрів безпеки та обміну ключами. Сертифікати X.509 та ланцюги довіри. Типові помилки конфігурації захищених протоколів та їх наслідки для програмних сервісів.

Поняття віртуальної приватної мережі (VPN) та сфери її застосування. Топології VPN: site-to-site та remote access. Протокол IPsec: компоненти AH, ESP, IKE, режими transport і tunnel. Порівняння IPsec, OpenVPN та WireGuard. Практичні аспекти побудови захищених мережевих тунелів для доступу до програмних сервісів.

Тема 5. Криптографічний захист даних та управління ключами

Роль криптографії у забезпеченні конфіденційності, цілісності та автентичності даних. Симетричні та асиметричні алгоритми шифрування. Криптографічні хеш-функції та цифрові підписи. Практичне застосування криптографії для захисту файлів, повідомлень і резервних копій. Типові помилки при самостійному впровадженні криптографічних механізмів у програмному забезпеченні.

Життєвий цикл криптографічних ключів: генерація, зберігання, розповсюдження, ротація, відклик та архівація. Ризики компрометації ключової інформації. Апаратні та програмні засоби захисту ключів (HSM, TPM, токени). Основи інфраструктури відкритих ключів (PKI). Нормативні вимоги та стандарти управління ключами.

Тема 6. Захист даних у сучасних інформаційних системах та управління інцидентами безпеки

Особливості зберігання та обробки даних у розподілених системах. Захист даних at rest та in transit. Управління секретами та обліковими даними сервісів. Модель Zero Trust як сучасний підхід до безпеки. Ізоляція ресурсів та мінімізація привілеїв у хмарних і контейнерних середовищах.

Роль моніторингу у забезпеченні безпеки програм і даних. Джерела подій безпеки: системні та прикладні журнали, мережеві логи. Основи реагування на інциденти інформаційної безпеки. Збір, збереження та первинний аналіз цифрових доказів. Забезпечення відновлення штатного функціонування програмних систем після інцидентів.

Нормативні та міжнародні стандарти у сфері захисту інформації (ISO/IEC 27001, ДСТУ, вимоги регуляторів). Вимоги до криптографічного захисту. Аудит відповідності політикам безпеки. Інтеграція організаційних, програмних і технічних засобів у комплексну систему захисту програм і даних.

3 ПИТАННЯ ДО ПРАКТИЧНИХ ЗАНЯТЬ

Тема 1. Архітектурні принципи безпеки програмних систем та операційних середовищ

1. Модель CIA (конфіденційність, цілісність, доступність) як основа проектування систем захисту: практичні приклади реалізації кожного компонента у програмних системах.
2. Практичний аналіз сценаріїв порушення моделі CIA та розробка заходів щодо їх запобігання.
3. Принцип «defense in depth» (захист у глибину): практична реалізація багаторівневої архітектури захисту у сучасних операційних системах.
4. Принцип найменших привілеїв та мінімальної поверхні атаки: методи їх застосування при налаштуванні прав доступу та конфігурації сервісів.
5. Архітектурна роль операційної системи як посередника між програмним забезпеченням та апаратними ресурсами у контексті забезпечення безпеки.

Тема 2. Управління доступом та автентифікацією у програмних системах

1. Порівняльний аналіз моделей контролю доступу (DAC, MAC, RBAC): практична реалізація кожної моделі в Linux та Windows.
2. Механізми ідентифікації, автентифікації та авторизації користувачів: налаштування багатофакторної автентифікації в операційних системах.
3. Управління обліковими записами користувачів та служб: принципи ротації паролів, обмеження терміну дії та відкликання доступу.
4. Політики паролів та захист від атак на автентифікаційні механізми: практичне налаштування параметрів безпеки.
5. Аналіз журналів автентифікації для виявлення підозрілих спроб входу та автоматизованого підбору облікових даних.

Тема 3. Аудит безпеки, управління конфігураціями та вразливостями програмних систем

1. Етапи проведення аудиту безпеки: практична методика збору інформації, аналізу конфігурацій та оцінки ризиків.

2. Застосування стандартів CIS Benchmarks для оцінки стану захищеності Linux та Windows систем.

3. Автоматизовані інструменти аудиту безпеки (Lynis, OpenSCAP): практичне використання для перевірки відповідності політикам.

4. Інтерпретація результатів аудиту: методика пріоритезації виявлених вразливостей за критеріями ризику.

5. Розробка плану заходів з підвищення рівня захищеності на основі результатів аудиту.

Тема 4. Мережеві механізми захисту та безпечна передача даних

1. Архітектура фільтрації трафіку в Linux (iptables/nftables) та Windows Firewall: практичне порівняння можливостей.

2. Створення правил фільтрації за адресами, портами, протоколами та станом з'єднання для захисту від мережевих загроз.

3. Реалізація трансляції мережевих адрес (NAT) як елемента безпеки: практичні сценарії застосування.

4. Налаштування логування мережевих подій для подальшого аналізу інцидентів та виявлення аномалій.

5. Побудова багаторівневої схеми фільтрації трафіку з урахуванням принципу «defense in depth».

6. Принципи роботи протоколу TLS/SSL: практичний аналіз рукостискання, узгодження шифрів та обміну ключами.

7. Налаштування захищених сервісів на основі протоколу SSH: методи затвердження ключів, налаштування автентифікації та захист від атак.

Тема 5. Криптографічний захист даних та управління ключами

1. Порівняльний аналіз симетричних (AES, ChaCha20) та асиметричних (RSA, ECC) алгоритмів шифрування: практичний вибір для різних сценаріїв.

2. Застосування криптографічних хеш-функцій (SHA-256, BLAKE2) для забезпечення цілісності даних та верифікації файлів.

3. Реалізація цифрових підписів для забезпечення автентичності та недовірності даних у програмних системах.

4. Практичне шифрування файлів, повідомлень та резервних копій за допомогою інструментів GnuPG та OpenSSL.

Тема 6. Захист даних у сучасних інформаційних системах та управління інцидентами безпеки

1. Методи захисту даних «at rest» (шифрування дискового простору, менеджери секретів) та «in transit» (TLS, mTLS) у хмарних середовищах.

2. Управління секретами та обліковими даними сервісів за допомогою спеціалізованих інструментів (HashiCorp Vault, AWS Secrets Manager).

3. Практичні кроки реагування на інцидент інформаційної безпеки: ізоляція, аналіз, усунення, відновлення.

4. Методика збору цифрових доказів з дотриманням процедур збереження цілісності (ланцюг зберігання, хешування).

5. Аналіз журналів для встановлення хронології подій та визначення вектору атаки під час розслідування інциденту.

4 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.

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.

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).

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.

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.

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.

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.

5 ВИДИ ТА МЕТОДИ КОНТРОЛЮ

Види контролю		Складові оцінювання
Поточний контроль, який здійснюється під час проведення практичних (лабораторних) занять, виконання самостійної роботи, індивідуальних завдань, дослідної робота 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	

Питання для підсумкового контролю

1. Модель CIA (конфіденційність, цілісність, доступність) як основа проектування систем захисту: практичні приклади реалізації кожного компонента у програмних системах.
2. Класифікація загроз, вразливостей та ризиків: методика ідентифікації та оцінки їх впливу на безпеку програмного середовища.
3. Принцип defense in depth (захист у глибину): практична реалізація багаторівневої архітектури захисту у програмних системах.
4. Принцип найменших привілеїв та мінімальної поверхні атаки: методи їх застосування при проєктуванні програмних систем.
5. Архітектурна роль операційної системи як середовища виконання програм у контексті забезпечення безпеки.
6. Механізми ізоляції процесів та ресурсів в операційних системах та їх роль у запобіганні поширенню загроз.
7. Типи віртуалізації та їх вплив на рівень захищеності віртуальних середовищ.
8. Контейнеризація як механізм ізоляції програмних сервісів.
9. Моделі контролю доступу (DAC, MAC, RBAC) та їх застосування у програмних системах.
10. Механізми ідентифікації, автентифікації та авторизації користувачів у програмних системах.
11. Управління обліковими записами користувачів та служб.
12. Політики паролів та захист від атак на автентифікаційні механізми.
13. Аналіз журналів автентифікації для виявлення підозрілих спроб входу.
14. Етапи проведення аудиту безпеки програмних та системних середовищ.
15. Стандарти та методики аудиту безпеки (CIS Benchmarks, NIST SP 800).
16. Автоматизовані інструменти аудиту безпеки програмних середовищ.
17. Інтерпретація результатів аудиту та пріоритезація виявлених вразливостей.
18. Процес управління вразливостями: застосування бази CVE та оцінка ризиків за шкалою CVSS.
19. Управління конфігураціями безпеки програмних систем.
20. Архітектура фільтрації мережевого трафіку та роль фаєрволів у захисті програмних сервісів.
21. Створення правил фільтрації за адресами, портами, протоколами та станом з’єднання.
22. Налаштування логування мережевих подій для аналізу інцидентів безпеки.
23. Принципи побудови захищених протоколів передачі даних.
24. Протоколи SSH, TLS/SSL, IPsec та їх роль у забезпеченні безпечної комунікації.

25. Сертифікати X.509 та ланцюги довіри у системах захищеної комунікації.

26. Типові помилки конфігурації захищених протоколів та їх наслідки.

27. Порівняльний аналіз симетричних (AES, ChaCha20) та асиметричних (RSA, ECC) алгоритмів шифрування.

28. Криптографічні хеш-функції та їх використання для забезпечення цілісності даних.

29. Реалізація цифрових підписів для забезпечення автентичності даних.

30. Типові помилки при впровадженні криптографічних механізмів у програмних системах.

31. Життєвий цикл криптографічних ключів: генерація, зберігання, ротація та відклик.

32. Основи інфраструктури відкритих ключів (PKI).

33. Порівняльний аналіз протоколів VPN (IPsec, OpenVPN, WireGuard).

34. Захист даних at rest та in transit у програмних системах.

35. Управління секретами та обліковими даними сервісів у сучасних інформаційних системах.

36. Модель Zero Trust та її застосування у програмних системах.

37. Моніторинг безпеки програмних систем та джерела подій безпеки.

38. Реагування на інциденти інформаційної безпеки та основні етапи їх обробки.

39. Збір і аналіз цифрових доказів під час розслідування інцидентів безпеки.

40. Відновлення функціонування програмних систем після інцидентів безпеки.

6 КРИТЕРІЇ ПІДСУМКОВОЇ ОЦІНКИ ЗНАНЬ СТУДЕНТІВ

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**
Загалом балів			**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 переводу 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 переводу 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 переводу 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 добувач 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.

7 ОЦІНЮВАННЯ ЗАГАЛЬНИХ РЕЗУЛЬТАТІВ ЗНАНЬ ЗДОБУВАЧІВ

Загальні результати знань здобувачів по даній дисципліні оцінюються наступним чином:

– **«Відмінно»/«зараховано» (A)** – 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» (B)** – 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» (C)** – 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. добувач 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 за 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		

8 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)», затвердженої 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);

– посилання 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, використані методики досліджень і джерела інформації.

9 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. Євсеєв С. П. Лабораторний практикум з основ криптографічного захисту [Електронний ресурс] : навчальний посібник / С. П. Євсеєв, 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 КПІ ім. Ігоря Сікорського. — Київ : Вид-во «Політехніка» КПІ 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. Євсеєв, 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 : МЕГУ, 2011. — 97 с.

11. Кузнецов О. О. Захист інформації в інформаційних системах. Методи традиційної криптографії / О. О. Кузнецов, С. П. Євсеєв, 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/

Навчальне видання

Йона Лариса Григорівна

БЕЗПЕКА ПРОГРАМ ТА ДАНИХ

Методичні рекомендації для самостійної роботи здобувачів, першого (бакалаврського) рівня спеціальності «Інженерія програмного забезпечення»

Українською мовою