МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

МІЖНАРОДНИЙ ГУМАНІТАРНИЙ УНІВЕРСИТЕТ

Кафедра комп'ютерної інженерії та інноваційних технологій

«ЗАТВЕРДЖУЮ»

Ректор Міжнародного гуманітарного університету д.ю.н., професор

_____ Костянтин ГРОМОВЕНКО

«29» серпня 2025 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

БЕЗПЕКА ПРОГРАМ ТА ДАНИХ

Галузь знань	12 Інформаційні технології
Спеціальність	125 Кібербезпека та захист інформації
Назва освітньої програми	Кібербезпека
Рівень вищої освіти	перший (бакалаврський) рівень

Одеса - 2025 рік

Робоча програма затверджена на засіданні кафедри комп'ютерної інженерії та інноваційних технологій протокол № 1 від 28 серпня 2025 року.

Розробники і викладачі	Контактний тел.	E-mail
Професор кафедри комп'ютерної інженерії та інноваційних технологій **Радівілова Тамара Анатоліївна**	+380951609153	tamara.radivilova@gmail.com

Завідувач кафедри
комп'ютерної інженерії та
інноваційних технологій,
к.т.н., доцент _____ Лариса ЙОНА

Гарант освітньої програми,
к.т.н., доцент _____ Лариса ЙОНА

Узгоджено
Начальник навчального відділу _____ Лілія САЄНКО

1. ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

<table>
<tr><th rowspan="2">Найменування показників</th><th rowspan="2">Галузь знань, напрям підготовки, освітньо-кваліфікаційний рівень</th><th colspan="2">Характеристика навчальної дисципліни</th></tr>
<tr><th>денна форма навчання</th><th>заочна форма навчання</th></tr>
<tr><td rowspan="2">Кількість кредитів – 8

Загальна кількість годин – 240</td><td>Галузь –
12 Інформаційні технології</td><td colspan="2">обов’язкова</td></tr>
<tr><td rowspan="9">Спеціальність –
125 Кібербезпека та захист інформації</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td colspan="2">3, 4-й</td></tr>
<tr><td colspan="2">Семестр</td></tr>
<tr><td>6,7-й</td><td>6,7-й</td></tr>
<tr><td colspan="2">Лекції</td></tr>
<tr><td rowspan="8">Мова навчання – українська</td><td rowspan="8">Рівень вищої освіти – перший (бакалаврський) рівень</td><td>52 год.</td><td>8 год.</td></tr>
<tr><td colspan="2">Практичні, семінарські</td></tr>
<tr><td>40 год.</td><td>4 год.</td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>12 год.</td><td>8 год.</td></tr>
<tr><td colspan="2">Самостійна робота та індивідуальні завдання</td></tr>
<tr><td>136 год.</td><td>220 год.</td></tr>
<tr><td colspan="2">Вид контролю:</td></tr>
<tr><td>Залік, екзамен</td><td>Залік, екзамен</td></tr>
</table>

Дисципліна **«Безпека програм та даних»** є обов’язковою дисципліною професійного циклу підготовки бакалаврів за спеціальністю 125 «Кібербезпека та захист інформації» та спрямована на формування системного розуміння принципів, методів і засобів забезпечення безпеки програмного забезпечення та даних в інформаційних і інформаційно-комунікаційних системах.

Курс охоплює фундаментальні та прикладні аспекти захисту програмного середовища, зокрема архітектурні принципи безпеки, моделі контролю доступу, аудит і підвищення рівня захищеності операційних систем, захист від автоматизованих атак, мережеву фільтрацію та управління вразливостями.

Вивчення дисципліни забезпечує формування у студентів здатності проєктувати та впроваджувати комплексні системи захисту програм і даних, здійснювати моніторинг стану безпеки, виявляти та аналізувати вразливості, реагувати на інциденти інформаційної безпеки й забезпечувати відновлення штатного функціонування інформаційних систем.

Метою дисципліни є формування у здобувачів вищої освіти цілісного уявлення про безпеку програмного забезпечення та даних і розвиток практичних навичок застосування технічних, програмних і криптографічних засобів захисту. Зміст дисципліни узгоджено з освітньо-професійною програмою підготовки фахівців з кібербезпеки та забезпечує необхідну теоретичну й практичну базу для подальшого вивчення дисциплін з аналізу кіберзагроз, управління інформаційною безпекою та реагування на кіберінциденти.

ПРЕРЕКВІЗИТИ. Передумовами є знання з програмування («Основи програмування», ОК 8), операційних систем («Операційні системи», ОК 20), захисту інформації в мережах («Захист інформації в інфокомунікаційних системах та мережах», ОК 12), а також основ Web-безпеки («Основи Web-безпеки», ОК 22).

ПОСТРЕКВІЗИТИ. Знання та навички із захисту програм та даних є необхідними при вивченні «Комплексних систем захисту інформації» (ОК 24), «Управління інформаційною та кібербезпекою» (ОК 30), «Основ цифрової криміналістики» (ОК 26), «Етичного хакінгу та тестування на проникнення» (ОК 18), а також при проходженні переддипломної практики (ОК 35) та захисті кваліфікаційної роботи (ОК 36).

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

У процесі реалізації програми дисципліни «Безпека програм та даних» формуються наступні компетентності із передбачених освітньою програмою:

Інтегральна компетентність

ІК. Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі кібербезпеки та захисту інформації.

Загальні компетентності (ЗК)

ЗК1. Здатність застосовувати знання у практичних ситуаціях.

ЗК 5. Здатність вчитися і оволодівати сучасними знаннями

Спеціальні (фахові, предметні) компетентності

СК 2. Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації

СК 10. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.

СК 11. Здатність здійснювати проєктування, адміністрування та керування інформаційно-комунікаційними системами, забезпечуючи їхню надійність, безпеку та ефективність функціонування.

Навчальна дисципліна «Безпека програм та даних» забезпечує досягнення програмних результатів навчання (РН), передбачених освітньою програмою:

РН 4. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність

РН 5. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення

РН 6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.

РН 10. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.

РН 18. Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.

РН 21. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.

РН 22. Вміти застосовувати методи та інструменти проєктування й адміністрування мереж і систем, виконувати налаштування, моніторинг та підтримку їхньої працездатності з урахуванням вимог інформаційної безпеки.

Заплановані результати навчання за навчальною дисципліною

Знання:

1 На концептуальному рівні — фундаментальні принципи безпеки програмного забезпечення та даних, модель CIA (конфіденційність, цілісність, доступність), класифікацію загроз, вразливостей і ризиків, архітектурні підходи до побудови захищених систем (зокрема принципи defense in depth, найменших привілеїв, мінімальної поверхні атаки) та роль операційних систем у забезпеченні безпеки.

2 Структуру та механізми ключових компонентів захисту: моделі контролю доступу (DAC, MAC, RBAC), криптографічні алгоритми (симетричні, асиметричні, хеш-функції, цифрові підписи), захищені протоколи (TLS/SSL, SSH, IPsec), принципи роботи мережевих фаєрволів, систем аудиту

та моніторингу безпеки.

3 Сучасні підходи до управління безпекою в різних середовищах: методики управління вразливостями (CVE, CVSS), організацію віртуальних приватних мереж (VPN), захист даних «at rest» та «in transit» у хмарних і контейнерних середовищах, модель Zero Trust, а також вимоги нормативних стандартів (ISO/IEC 27001, ДСТУ, NIST).

Уміння:

4. Аналізувати архітектуру програмних систем та інформаційних середовищ з метою виявлення вразливостей, оцінювати рівень захищеності на основі аналізу конфігурацій, прав доступу, журналів подій та результатів аудиту за методиками CIS Benchmarks.

5. Обґрунтовано вибирати та інтегрувати технічні засоби захисту (криптографічні механізми, фаєрволи, системи запобігання вторгненням) залежно від специфіки завдання, середовища розгортання та вимог політики інформаційної безпеки.

6. Оцінювати ефективність захисних механізмів проти типових атак (грубої сили, credential stuffing, експлуатації вразливостей), прогнозувати наслідки помилкової конфігурації захищених протоколів або некоректного управління ключовою інформацією.

7. Розробляти комплексні заходи з підвищення рівня захищеності, враховуючи взаємозв'язок організаційних, технічних та програмних компонентів системи захисту інформації.

Навички:

8. Ефективно застосовувати сучасні інструменти захисту в віртуалізованих середовищах: налаштовувати мережеву фільтрацію та NAT, реалізовувати криптографічний захист файлів і передачі даних, організовувати захищені тунелі (IPsec, OpenVPN, WireGuard) та управління ключами.

9. Виконувати моніторинг безпеки, аналізувати системні та мережеві журнали для виявлення інцидентів, збирати цифрові докази з дотриманням процедур збереження цілісності, а також реалізовувати заходи з відновлення функціонування систем після реалізації кіберзагроз.

10. Працювати з автоматизованими засобами управління вразливостями, оновленнями та конфігураціями безпеки, забезпечуючи постійну підтримку захищеного стану інформаційних систем у відповідності до вимог сучасних стандартів кібербезпеки.

3. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Змістовий модуль 1. Безпека програмного середовища та операційних систем

Тема 1. Архітектурні основи безпеки програм та даних

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.

Тема 2. Ізоляція, віртуалізація та моделювання безпечного програмного середовища

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 і тестування політик безпеки.

Тема 3. Моделі контролю доступу та безпека облікових записів

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.

Тема 4. Аудит безпеки та оцінка стану захищеності операційних 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. Інтерпретація результатів перевірки та формування заходів з підвищення рівня захищеності.

Тема 5. Захист від атак грубої сили та автоматизованих вторгнень

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. Налаштування параметрів реагування та оцінка ефективності захисту.

Тема 6. Мережеві фаєрволи та фільтрація трафіку в операційних системах

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.

Тема 7. Управління оновленнями, вразливостями та конфігурацією безпеки

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

Змістовий модуль 2. Захист даних та безпечна комунікація

Тема 8. Криптографічні механізми захисту даних у програмних системах

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.

Тема 9. Управління криптографічними ключами та довірчою інфраструктурою

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 10. Захищені протоколи передачі даних та їх реалізація

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.

Тема 11. Віртуальні приватні мережі та організація захищених тунелів

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.

Тема 12. Захист даних у розподілених, хмарних та контейнерних середовищах

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.

Тема 13. Моніторинг безпеки, реагування на інциденти та цифрові докази

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 систем після інцидентів.

Тема 14. Стандарти та комплексний підхід до захисту програм і даних

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.

4. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Назви змістових модулів і тем	Кількість годин									
	денна форма					Заочна форма				
	усього	у тому числі				усього	у тому числі			
		лекц.	лаб.	практ.	сам. роб.		лекц.	лаб.	прак.	сам. роб.
Змістовий модуль 1. Безпека програмного середовища та операційних систем **Тема 1.** Архітектурні основи безпеки програм та даних	12	2		2	8	16	2			14
Тема 2. Ізоляція, віртуалізація та моделювання безпечного програмного середовища	18	4	2	2	10	18			2	16
Тема 3. Моделі контролю доступу та безпека облікових записів	18	4		4	10	18		2		16
Тема 4. Аудит безпеки та оцінка стану захищеності операційних систем	18	4	2	2	10	18	2			16
Тема 5. Захист від атак грубої сили та автоматизованих вторгнень	18	4	2	2	10	16				16
Тема 6. Мережеві фаєрволи та фільтрація трафіку в операційних системах	18	4		4	10	18		2		16
Тема 7. Управління оновленнями, вразливостями та конфігурацією безпеки	18	4		4	10	16				16
Змістовий модуль 2. Захист даних та безпечна комунікація **Тема 8.** Криптографічні механізми захисту даних у програмних системах	16	4		2	10	18	2			16
Тема 9. Управління криптографічними ключами та довірчою інфраструктурою	16	4	2	2	8	16		2		14
Тема 10. Захищені протоколи передачі даних та їх реалізація	18	4		4	10	18			2	16
Тема 11. Віртуальні приватні мережі та організація захищених тунелів	18	4	2	2	10	18		2		16
Тема 12. Захист даних у розподілених, хмарних та контейнерних середовищах	18	4		4	10	16				16
Тема 13. Моніторинг безпеки, реагування на інциденти та цифрові докази	16	2	2	2	10	18	2			16
Тема 14. Стандарти та комплексний підхід до захисту програм і даних	18	4		4	10	16				16
Усього годин	**240**	**52**	**12**	**40**	**136**	**240**	**8**	**8**	**4**	**220**
ПІДСУМКОВИЙ КОНТРОЛЬ – ЗАЛІК, ЕКЗАМЕН										

5. ПИТАННЯ ДО ПРАКТИЧНИХ ЗАНЯТЬ

№ з/п	. Назва теми	Кількість годин	
		денна форма	заочна форма
1	**Тема 1. Архітектурні основи безпеки програм та даних** 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 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. 6. Практичний аналіз сценаріїв порушення моделі CIA та розробка заходів щодо їх запобігання.	2	
2	**Тема 2. Ізоляція, віртуалізація та моделювання безпечного програмного середовища** 1. Механізми ізоляції процесів та ресурсів в операційних системах (namespaces, cgroups, chroot) та їх роль у запобіганні поширення загроз. 2. Типи віртуалізації (повна, паравіртуалізація, апаратно-прискорена) та їх вплив на рівень захищеності віртуальних середовищ. 3. Контейнеризація як легковаговий механізм ізоляції: порівняння безпеки контейнерів (Docker, Podman) та повної віртуалізації. 4. Практичне створення віртуального середовища для тестування вразливостей з дотриманням принципів безпеки та ізоляції. 5. Моделювання атак та захисних механізмів у віртуалізованих середовищах: методика безпечного проведення пентестів. 6. Управління ресурсами віртуальних середовищ для запобігання атакам типу «resource exhaustion».	2	2
3	**Тема 3. Моделі контролю доступу та безпека облікових записів** 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. Реалізація принципу найменших привілеїв для системних служб та демонів у багатокористувацьких середовищах. 5. Політики паролів та захист від атак на автентифікаційні механізми: практичне налаштування параметрів безпеки. 6. Аналіз журналів автентифікації для виявлення підозрілих спроб входу та автоматизованого підбору облікових даних.	4	
4	**Тема 4. Аудит безпеки та оцінка стану захищеності операційних 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.	2	

	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. 6. Перевірка відповідності конфігурацій вимогам нормативних стандартів (ДСТУ, ISO/IEC 27001) у практичному середовищі.		
5	**Тема 5. Захист від атак грубої сили та автоматизованих вторгнень** 1. Характеристика атак грубої сили («brute force»), словникових атак («dictionary attack») та «credential stuffing»: методи їх виявлення за журналами. 2. Налаштування механізмів автоматичного блокування зловмисних дій (fail2ban, PAM) у різних операційних системах. 3. Практичне застосування систем виявлення та запобігання вторгненням (IDS/IPS) для захисту від автоматизованих атак. 4. Аналіз системних логів для ідентифікації патернів атак грубої сили та формування сигнатур для систем моніторингу. 5. Налаштування параметрів реагування на підозрілі спроби автентифікації: балансування між безпекою та доступністю сервісів. 6. Оцінка ефективності реалізованих захисних механізмів шляхом симуляції атак у контрольованому середовищі.	2	
6	**Тема 6. Мережеві фаєрволи та фільтрація трафіку в операційних системах** 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. Тестування ефективності правил фаєрвола за допомогою інструментів мережевого сканування та аналізу трафіку.	4	
7	**Тема 7. Управління оновленнями, вразливостями та конфігурацією безпеки** 1. Процес управління вразливостями: практичне застосування бази даних CVE та оцінка ризиків за шкалою CVSS. 2. Методика перевірки цілісності програмних пакетів за допомогою криптографічних хешів та цифрових підписів. 3. Автоматизація оновлення безпеки в операційних системах: налаштування механізмів безпечного розгортання патчів. 4. Управління конфігураціями безпеки за допомогою інструментів типу Ansible або Puppet для підтримки узгодженого стану систем. 5. Створення та тестування плану відновлення після помилкового застосування оновлень, що призвели до порушення функціонування. 6. Практичний аналіз впливу затримки оновлень на рівень захищеності систем та розробка стратегії управління вразливостями.	4	
8	**Тема 8. Криптографічні механізми захисту даних у програмних системах** 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	2	

	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. 5. Типові помилки при впровадженні криптографічних механізмів (неправильний вибір режиму шифрування, слабкі вектори ініціалізації). 6. Оцінка криптографічної стійкості реалізованих рішень та відповідність сучасним вимогам безпеки.		
9	**Тема 9. Управління криптографічними ключами та довірчою інфраструктурою** 1. Життєвий цикл криптографічних ключів: практична реалізація процесів генерації, ротації, відклику та архівації. 2. Застосування апаратних модулів безпеки (HSM, TPM) та токенів для захисту ключової інформації від компрометації. 3. Побудова базової інфраструктури відкритих ключів (PKI): створення кореневого та проміжних центру сертифікації. 4. Генерація, підписання та перевірка сертифікатів X.509 для забезпечення безпечної комунікації. 5. Управління списками відкликаних сертифікатів (CRL) та реалізація протоколу OCSP для перевірки статусу сертифікатів. 6. Аналіз ризиків, пов'язаних з компрометацією ключів, та розробка плану реагування на інциденти.	2	
10	**Тема 10. Захищені протоколи передачі даних та їх реалізація** 1. Принципи роботи протоколу TLS/SSL: практичний аналіз рукостискання, узгодження шифрів та обміну ключами. 2. Налаштування захищених сервісів на основі протоколу SSH: методи затвердження ключів, налаштування автентифікації та захист від атак. 3. Реалізація захищеної передачі даних за допомогою протоколу IPsec: налаштування асоціацій безпеки (SA) та ключів. 4. Аналіз сертифікатів X.509 та ланцюгів довіри для верифікації автентичності віддалених сторін. 5. Типові помилки конфігурації захищених протоколів (використання слабких шифрів, відсутність валідації сертифікатів) та їх наслідки. 6. Тестування безпеки реалізованих протоколів за допомогою інструментів (SSL Labs, testssl.sh) та аналіз результатів.	4	2
11	**Тема 11. Віртуальні приватні мережі та організація захищених тунелів** 1. Порівняльний аналіз протоколів VPN (IPsec, OpenVPN, WireGuard): практичний вибір для різних сценаріїв застосування. 2. Налаштування site-to-site VPN для безпечного з'єднання віддалених мереж з використанням IPsec/IKEv2. 3. Реалізація remote access VPN для забезпечення безпечного віддаленого доступу до корпоративних ресурсів. 4. Практична конфігурація компонентів IPsec (AH, ESP) у режимах «transport» та «tunnel». 5. Налаштування маршрутизації та правил фільтрації для забезпечення безпеки всередині віртуальної приватної мережі. 6. Тестування стійкості VPN-з'єднань до атак та аналіз трафіку для верифікації конфіденційності переданих даних.	2	
12	**Тема 12. Захист даних у розподілених, хмарних та контейнерних середовищах** 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	4	

	спеціалізованих інструментів (HashiCorp Vault, AWS Secrets Manager). 3. Реалізація моделі «Zero Trust» у розподілених системах: практичне застосування принципів верифікації кожного запиту. 4. Ізоляція ресурсів та мінімізація привілеїв у контейнерних середовищах (securityContext, seccomp, AppArmor). 5. Захист конфігураційних файлів та змінних середовища від несанкціонованого доступу у хмарних розгортаннях. 6. Аудит та моніторинг доступу до даних у розподілених системах для виявлення підозрілих дій.		
13	**Тема 13. Моніторинг безпеки, реагування на інциденти та цифрові докази** 1. Налаштування централізованого збору системних та мережевих журналів (syslog, rsyslog) для моніторингу безпеки. 2. Створення правил виявлення інцидентів на основі аналізу патернів у журналах подій. 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. 6. Відновлення штатного функціонування систем після реалізації кіберзагрози з мінімізацією втрат даних.	2	
14	**Тема 14. Стандарти та комплексний підхід до захисту програм і даних** 1. Аналіз вимог міжнародних стандартів (ISO/IEC 27001, NIST) та національних ДСТУ до систем захисту інформації. 2. Інтеграція організаційних, технічних та програмних засобів у комплексну систему захисту програм і даних. 3. Розробка політики інформаційної безпеки з урахуванням специфіки навчального закладу та вимог законодавства України. 4. Проведення аудиту відповідності реалізованих заходів вимогам нормативних документів. 5. Оцінка ефективності комплексної системи захисту за кількісними та якісними показниками. 6. Планування подальшого розвитку системи захисту інформації з урахуванням еволюції загроз та технологічних змін.	4	
	Всього	**40**	**4**

6. САМОСТІЙНА РОБОТА

До самостійної роботи студентів щодо вивчення дисципліни «Безпека програм та даних» включаються:

1. Знайомство з науковою та навчальною літературою відповідно зазначених у програмі тем.
2. Опрацювання лекційного матеріалу.
3. Підготовка до практичних занять.
4. Консультації з викладачем протягом семестру.
5. Самостійне опрацювання окремих питань навчальної дисципліни.
6. Підготовка та виконання індивідуальних завдань у вигляді есе, рефератів тощо.
7. Підготовка до підсумкового контролю.

Тематика та питання до самостійної підготовки та індивідуальних завдань

№ з/п	Назва теми	Кількість годин	
		денна форма	заочна форма
1	**Змістовий модуль 1. Безпека програмного середовища та операційних систем** **Тема 1. Архітектурні основи безпеки програм та даних** 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.	8	14
2	**Тема 2. Ізоляція, віртуалізація та моделювання безпечного програмного середовища** 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 і тестування політик безпеки.	10	16
3	**Тема 3. Моделі контролю доступу та безпека облікових записів** 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.	10	16
4	**Тема 4. Аудит безпеки та оцінка стану захищеності операційних 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. Інтерпретація результатів перевірки та формування заходів з підвищення рівня захищеності.	10	16
5	**Тема 5. Захист від атак грубої сили та автоматизованих вторгнень** 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. Налаштування параметрів реагування та оцінка ефективності захисту.	10	16
6	**Тема 6. Мережеві фаєрволи та фільтрація трафіку в операційних системах** 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.	10	16
7	**Тема 7. Управління оновленнями, вразливостями та конфігурацією безпеки** Роль оновлень у запобіганні експлуатації відомих вразливостей. Поняття CVE та CVSS. Процес управління вразливостями. Перевірка цілісності програмних пакетів. Автоматизація оновлення безпеки. Управління	10	16

	конфігураціями як складова підтримки безпечного стану системи.		
	Змістовий модуль 2. Захист даних та безпечна комунікація **Тема 8. Криптографічні механізми захисту даних у програмних системах** 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.	10	16
	Тема 9. Управління криптографічними ключами та довірчою інфраструктурою 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.	8	14
	Тема 10. Захищені протоколи передачі даних та їх реалізація 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.	10	16
	Тема 11. Віртуальні приватні мережі та організація захищених тунелів 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.	10	16
	Тема 12. Захист даних у розподілених, хмарних та контейнерних середовищах 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.	10	16
	Тема 13. Моніторинг безпеки, реагування на інциденти та цифрові докази 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 систем після інцидентів.	10	16
	Тема 14. Стандарти та комплексний підхід до захисту програм і даних 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.	10	16
	Всього	**136**	**220**

7. ВИДИ ТА МЕТОДИ КОНТРОЛЮ

Види контролю	**Складові оцінювання**	
	Для екзамену	**Для заліку**
поточний контроль, який здійснюється у ході: проведення практичних (лабораторних) занять, виконання самостійної роботи, індивідуальних завдань, дослідна робота здобувача	**50%**	**100%**

тощо.		
підсумковий контроль	**50%**	

Методи діагностики знань (контролю)	**фронтальне опитування; наукова доповідь, реферати, усне повідомлення, індивідуальне опитування; робота у групах; ділова гра, розв`язання ситуаційних завдань, кейсів, практичних завдань, залік, екзамен**

Питання до заліку та екзамену

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 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.
6. Практичний аналіз сценаріїв порушення моделі CIA та розробка заходів щодо їх запобігання.
7. Механізми ізоляції процесів та ресурсів в операційних системах (namespaces, cgroups, chroot) та їх роль у запобіганні поширення загроз.
8. Типи віртуалізації (повна, паравіртуалізація, апаратно-прискорена) та їх вплив на рівень захищеності віртуальних середовищ.
9. Контейнеризація як легковаговий механізм ізоляції: порівняння безпеки контейнерів (Docker, Podman) та повної віртуалізації.
10. Практичне створення віртуального середовища для тестування вразливостей з дотриманням принципів безпеки та ізоляції.
11. Моделювання атак та захисних механізмів у віртуалізованих середовищах: методика безпечного проведення пентестів.
12. Управління ресурсами віртуальних середовищ для запобігання атакам типу resource exhaustion.
13. Порівняльний аналіз моделей контролю доступу (DAC, MAC, RBAC): практична реалізація кожної моделі в Linux та Windows.
14. Механізми ідентифікації, автентифікації та авторизації користувачів: налаштування багатофакторної автентифікації в операційних системах.
15. Управління обліковими записами користувачів та служб: принципи ротації паролів, обмеження терміну дії та відкликання доступу.
16. Реалізація принципу найменших привілеїв для системних служб та демонів у багатокористувацьких середовищах.
17. Політики паролів та захист від атак на автентифікаційні механізми: практичне налаштування параметрів безпеки.
18. Аналіз журналів автентифікації для виявлення підозрілих спроб входу та автоматизованого підбору облікових даних.
19. Етапи проведення аудиту безпеки: практична методика збору інформації, аналізу конфігурацій та оцінки ризиків.
20. Застосування стандартів CIS Benchmarks для оцінки стану захищеності Linux та Windows систем.
21. Автоматизовані інструменти аудиту безпеки (Lynis, OpenSCAP): практичне використання для перевірки відповідності політикам.
22. Інтерпретація результатів аудиту: методика пріоритезації виявлених вразливостей за

критеріями ризику.
23. Розробка плану заходів з підвищення рівня захищеності на основі результатів аудиту.
24. Перевірка відповідності конфігурацій вимогам нормативних стандартів (ДСТУ, ISO/IEC 27001) у практичному середовищі.
25. Характеристика атак грубої сили (brute force), словникових атак (dictionary attack) та credential stuffing: методи їх виявлення за журналами.
26. Налаштування механізмів автоматичного блокування зловмисних дій (fail2ban, PAM) у різних операційних системах.
27. Практичне застосування систем виявлення та запобігання вторгненням (IDS/IPS) для захисту від автоматизованих атак.
28. Аналіз системних логів для ідентифікації патернів атак грубої сили та формування сигнатур для систем моніторингу.
29. Налаштування параметрів реагування на підозрілі спроби автентифікації: балансування між безпекою та доступністю сервісів.
30. Оцінка ефективності реалізованих захисних механізмів шляхом симуляції атак у контрольованому середовищі.
31. Архітектура фільтрації трафіку в Linux (iptables/nftables) та Windows Firewall: практичне порівняння можливостей.
32. Створення правил фільтрації за адресами, портами, протоколами та станом з'єднання для захисту від мережевих загроз.
33. Реалізація трансляції мережевих адрес (NAT) як елемента безпеки: практичні сценарії застосування.
34. Налаштування логування мережевих подій для подальшого аналізу інцидентів та виявлення аномалій.
35. Побудова багаторівневої схеми фільтрації трафіку з урахуванням принципу defense in depth.
36. Тестування ефективності правил фаєрвола за допомогою інструментів мережевого сканування та аналізу трафіку.
37. Процес управління вразливостями: практичне застосування бази даних CVE та оцінка ризиків за шкалою CVSS.
38. Методика перевірки цілісності програмних пакетів за допомогою криптографічних хешів та цифрових підписів.
39. Автоматизація оновлення безпеки в операційних системах: налаштування механізмів безпечного розгортання патчів.
40. Управління конфігураціями безпеки за допомогою інструментів типу Ansible або Puppet для підтримки узгодженого стану систем.
41. Створення та тестування плану відновлення після помилкового застосування оновлень, що призвели до порушення функціонування.
42. Практичний аналіз впливу затримки оновлень на рівень захищеності систем та розробка стратегії управління вразливостями.
43. Порівняльний аналіз симетричних (AES, ChaCha20) та асиметричних (RSA, ECC) алгоритмів шифрування: практичний вибір для різних сценаріїв.
44. Застосування криптографічних хеш-функцій (SHA-256, BLAKE2) для забезпечення цілісності даних та верифікації файлів.
45. Реалізація цифрових підписів для забезпечення автентичності та недовірності даних у програмних системах.
46. Практичне шифрування файлів, повідомлень та резервних копій за допомогою інструментів GnuPG та OpenSSL.
47. Типові помилки при впровадженні криптографічних механізмів (неправильний вибір режиму шифрування, слабкі вектори ініціалізації).
48. Оцінка криптографічної стійкості реалізованих рішень та відповідність сучасним вимогам безпеки.
49. Життєвий цикл криптографічних ключів: практична реалізація процесів генерації, ротації, відклику та архівації.
50. Застосування апаратних модулів безпеки (HSM, TPM) та токенів для захисту ключової

інформації від компрометації.
51. Побудова базової інфраструктури відкритих ключів (PKI): створення кореневого та проміжних центру сертифікації.
52. Генерація, підписання та перевірка сертифікатів X.509 для забезпечення безпечної комунікації.
53. Управління списками відкликаних сертифікатів (CRL) та реалізація протоколу OCSP для перевірки статусу сертифікатів.
54. Аналіз ризиків, пов'язаних з компрометацією ключів, та розробка плану реагування на інциденти.
55. Принципи роботи протоколу TLS/SSL: практичний аналіз рукостискання, узгодження шифрів та обміну ключами.
56. Налаштування захищених сервісів на основі протоколу SSH: методи затвердження ключів, налаштування автентифікації та захист від атак.
57. Реалізація захищеної передачі даних за допомогою протоколу IPsec: налаштування асоціацій безпеки (SA) та ключів.
58. Аналіз сертифікатів X.509 та ланцюгів довіри для верифікації автентичності віддалених сторін.
59. Типові помилки конфігурації захищених протоколів (використання слабких шифрів, відсутність валідації сертифікатів) та їх наслідки.
60. Тестування безпеки реалізованих протоколів за допомогою інструментів (SSL Labs, testssl.sh) та аналіз результатів.
61. Порівняльний аналіз протоколів VPN (IPsec, OpenVPN, WireGuard): практичний вибір для різних сценаріїв застосування.
62. Налаштування site-to-site VPN для безпечного з'єднання віддалених мереж з використанням IPsec/IKEv2.
63. Реалізація remote access VPN для забезпечення безпечного віддаленого доступу до корпоративних ресурсів.
64. Практична конфігурація компонентів IPsec (AH, ESP) у режимах transport та tunnel.
65. Налаштування маршрутизації та правил фільтрації для забезпечення безпеки всередині віртуальної приватної мережі.
66. Тестування стійкості VPN-з'єднань до атак та аналіз трафіку для верифікації конфіденційності переданих даних.
67. Методи захисту даних «at rest» (шифрування дискового простору, менеджери секретів) та «in transit» (TLS, mTLS) у хмарних середовищах.
68. Управління секретами та обліковими даними сервісів за допомогою спеціалізованих інструментів (HashiCorp Vault, AWS Secrets Manager).
69. Реалізація моделі Zero Trust у розподілених системах: практичне застосування принципів верифікації кожного запиту.
70. Ізоляція ресурсів та мінімізація привілеїв у контейнерних середовищах (securityContext, seccomp, AppArmor).
71. Захист конфігураційних файлів та змінних середовища від несанкціонованого доступу у хмарних розгортаннях.
72. Аудит та моніторинг доступу до даних у розподілених системах для виявлення підозрілих дій.
73. Налаштування централізованого збору системних та мережевих журналів (syslog, rsyslog) для моніторингу безпеки.
74. Створення правил виявлення інцидентів на основі аналізу патернів у журналах подій.
75. Практичні кроки реагування на інцидент інформаційної безпеки: ізоляція, аналіз, усунення, відновлення.
76. Методика збору цифрових доказів з дотриманням процедур збереження цілісності (ланцюг зберігання, хешування).
77. Аналіз журналів для встановлення хронології подій та визначення вектору атаки під час розслідування інциденту.
78. Відновлення штатного функціонування систем після реалізації кіберзагрози з мінімізацією

втрат даних.

79. Аналіз вимог міжнародних стандартів (ISO/IEC 27001, NIST) та національних ДСТУ до систем захисту інформації.
80. Інтеграція організаційних, технічних та програмних засобів у комплексну систему захисту програм і даних.
81. Розробка політики інформаційної безпеки з урахуванням специфіки навчального закладу та вимог законодавства України.
82. Проведення аудиту відповідності реалізованих заходів вимогам нормативних документів.
83. Оцінка ефективності комплексної системи захисту за кількісними та якісними показниками.
84. Планування подальшого розвитку системи захисту інформації з урахуванням еволюції загроз та технологічних змін.

8. ОЦІНЮВАННЯ ЗДОБУВАЧІВ ВИЩОЇ ТА ФАХОВОЇ ПЕРДВИЩОЇ ОСВІТИ ЗА НАВЧАЛЬНУ ДИСЦИПЛІНУ У МІЖНАРОДНОМУ ГУМАНІТАРНОМУ УНІВЕРСИТЕТІ

(*поточний контроль, підсумковий контроль, загальний результат оцінювання)*

ЕКЗАМЕН

Поточний контроль			
Види роботи	**Планові терміни виконання**	**Форми контролю та звітності**	**Максимальний відсоток оцінювання**
Систематичність і активність роботи на практичних (лабораторних) заняттях			
1.1. Підготовка до практичних (лабораторних) занять	Відповідно до робочої програми та розкладу занять	Перевірка обсягу та якості засвоєного матеріалу під час практичних (лабораторних) занять	**30**
Виконання завдань для самостійного опрацювання			
1.2. Індивідуальне тестування, завдання, підготовка реферату (есе) за заданою тематикою	Відповідно до робочої програми та розкладу занять	Розгляд відповідного матеріалу під час аудиторних занять або ІКР, перевірка конспектів навчальних текстів тощо	**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 освіти при формі контролю **екзамен** (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 (есе) 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 пдготовку до аудиторних занять середньоарифметична оцінка множиться на коефіцієнт 2.

КРИТЕРІЇ ОЦІНЮВАННЯ ЗА ПОТОЧНИЙ КОНТРОЛЬ

- «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 студента мають фрагментарний, поверховий характер;
- «4» - оцінюється правильна і обґрунтована відповідь (письмова робота), з якої видно, що студент 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 ЗНАНЬ ЗДОБУВАЧІВ ЗА ЕКЗАМЕН
(максимум 50 балів)

Рівень знань оцінюється:

- від 40 до 50 балів - студент виявляє особливі творчі здібності, вміє самостійно знаходити та опрацьовувати необхідну інформацію, демонструє знання матеріалу, проводить узагальнення і висновки;
- 30 до 40 балів - студент володіє знаннями матеріалу, але допускає незначні помилки у формуванні термінів, категорій, проте за допомогою викладача швидко орієнтується і знаходить правильні відповіді;
- 20 - 30 балів - студент 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.
- 10 - 20 балів - володіє навчальним матеріалом на середньому рівні, допускає помилки, серед яких є значна кількість суттєвих;
- 0 10 балів - володіє навчальним матеріалом на рівні, вищому за початковий, значну частину його відтворює на репродуктивному рівні, на всі запитання дає необґрунтовані, невичерпні відповіді, допускає помилки.

ЗАЛІК

Поточний контроль			
Види роботи	**Планові терміни виконання**	**Форми контролю та звітності**	**Максимальний відсоток оцінювання**
Систематичність і активність роботи на практичних (лабораторних) заняттях			

1.1. Підготовка до практичних (лабораторних) занять	Відповідно до робочої програми та розкладу занять	Перевірка обсягу та якості засвоєного матеріалу під час практичних (лабораторних) занять	**60**
Виконання завдань для самостійного опрацювання			
1.2. Індивідуальне тестування, завдання, підготовка реферату (есе) за заданою тематикою	Відповідно до робочої програми та розкладу занять	Розгляд відповідного матеріалу під час аудиторних занять або ІКР, перевірка конспектів навчальних текстів тощо	**20**
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.	**20**
Разом балів за поточний контроль			**100**
Загальний результат оцінювання			**100**

Поточний контроль знань здобувачів освіти при формі контролю **залік** (максимум 100 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 60 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 12;
- за виконання завдань для самостійного опрацювання (тестування, завдання, підготовка реферату (есе) за заданою тематикою) (максимум 20 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 4;
- за інші види індивідуальних завдань, в т.ч. підготовку наукових публікацій, участь у роботі круглих столів, конференцій тощо (максимум 20- 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 4.

КРИТЕРІЇ ОЦІНЮВАННЯ ЗА ПОТОЧНИЙ КОНТРОЛЬ

- «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 студента мають фрагментарний, поверховий характер;
- «4» - оцінюється правильна і обґрунтована відповідь (письмова робота), з якої видно, що студент 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.

9. КРИТЕРІЇ ЗАГАЛЬНИХ РЕЗУЛЬТАТІВ ОЦІНЮВАННЯ ЗНАНЬ ЗДОБУВАЧІВ

(для іспиту / заліку)

Рівень знань оцінюється:

- «відмінно» / «зараховано» A - від 90 до 100 балів. Студент виявляє особливі творчі здібності, вміє самостійно знаходити та опрацьовувати необхідну інформацію, демонструє знання матеріалу, проводить узагальнення і висновки. Був присутній на лекціях та семінарських заняттях, під час яких давав вичерпні, обґрунтовані, теоретично і практично правильні відповіді, має конспект з виконаними завданнями до самостійної роботи, презентував реферат (есе) за заданою тематикою, проявляє активність і творчість у науково-дослідній роботі;
- «добре» / «зараховано» B - від 82 до 89 балів. Студент 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 семінарських заняттях, має конспект з виконаними завданнями до самостійної роботи, презентував реферат (есе) за заданою тематикою, проявляє активність і творчість у науково-дослідній роботі;
- «добре» / «зараховано» C - від 74 до 81 балів. Студент 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. Студент був присутній не на всіх лекціях та семінарських 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, рефератів (есе);
- «задовільно» / «зараховано» E - від 60 до 63 балів. Студент був присутній не на всіх лекціях та семінарських 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. Студент 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. Студент не володіє навчальним матеріалом.

ТАБЛИЦЯ ВІДПОВІДНОСТІ ЗАГАЛЬНИХ РЕЗУЛЬТАТІВ ОЦІНЮВАННЯ ЗНАНЬ ЗА РІЗНИМИ ШКАЛАМИ

100-бальною шкалою	Шкала за ECTS	За національною шкалою	
		екзамен	залік
90-100	A	Відмінно	Зараховано
82-89	B	Добре	
74-81	C		
64-73	D	Задовільно	
60-63	E		
35-59	Fx	Незадовільно	Не зараховано
1-34	F		

10. 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. Радівілова Т.А., Йона Л.Г. Методичні рекомендації до практичних занять та самостійної роботи з навчальної дисципліни «Захист інформації в інформаційно-комунікаційних системах» для здобувачів вищої освіти першого (бакалаврського) рівня спеціальностей 121 «Інженерія програмного забезпечення», 122 «Комп'ютерні науки», 123 «Комп'ютерна інженерія», 125 «Кібербезпека та захист інформації», 172 «Електронні комунікації та радіотехніка», 014 «Середня освіта. Інформатика» денної та заочної форми навчання [Електронне видання] / Радівілова Т.А., Йона Л.Г. Кафедра комп'ютерної інженерії та інноваційних технологій Міжнародного гуманітарного університету. Одеса. 2025.

5. Йона Л. Г., Педяш, В. В. Мазур Г. Д. Безпека програм та даних : метод. реком. для практичних та лабораторних занять [Електронне видання] / Кафедра комп'ютерної інженерії та інноваційних технологій Міжнародного гуманітарного університету. — Одеса, 2025. — 136 с. — Режим доступу: https://hdl.handle.net/11300/32279

6. 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.

7. 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.

8. Кузнецов О. О. Захист інформації в інформаційних системах : навч. посіб. — Х. : ХНЕУ, 2018. — 510 с.

9. 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

10. Остапов С. Є. Технології захисту інформації / С. Є. Остапов, С. П. Євсеєв, О. Г. Король. — Чернівці : Видавничий дім «Родовід», 2014. — 428 с.

11. 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.

12. Літнарович Р. М. Сучасні технології інформаційної безпеки : навч. посібник. — Рівне : МЕГУ, 2011. — 97 с.

13. 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.

14. 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.

15. Дудатьєв А. В. Захист програмного забезпечення. Ч. 1 : навч. посібник / А. В. Дудатьєв, В. А. Каплун, В. П. Семеренко. — Вінниця : ВНТУ, 2005. — 140 с.
16. Мельник І. В. Інформаційні комп'ютерні мережі : навч. посібник для дист. навчання. — К. : Вид-во Універ. «Україна», 2006. — 250 с.
17. Столлінгс В. Криптографія та захист мереж: принципи й практика / В. Столлінгс ; пер. з англ. — 2-е вид. — К. : Видавничий дім «Вільямс», 2001. — 672 с.
18. Богуш В. М., Давидьков О. А. Теоретичні основи захищених інформаційних технологій. — К. : ДУІКТ, 2010. — 414 с.
19. 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.
20. 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. ІІ. Інформаційна безпека. — 344 с.
21. Грайворонський М. В., Новіков О. М. Безпека інформаційно-комунікаційних систем. — К. : Видавнича група BHV, 2009. — 608 с.
22. 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

1. Національна бібліотека України ім. В. І. Вернадського : URL: http://www.nbuv.gov.ua.
2. Он-лайн бібліотека «Лібком» : URL: http://www.lib.com.ua.
3. MIT OpenCourseWare (OCW) : URL: https://ocw.mit.edu/.
4. Dive into Systems : URL: https://diveintosystems.org/.
5. Open Textbook Library : URL: https://open.umn.edu/opentextbooks.
6. Directory of Open Access Books (DOAB) : URL: https://www.doabooks.org/.
7. Internet Engineering Task Force (IETF) : URL: https://www.ietf.org/.
8. RFC Editor : URL: https://www.rfc-editor.org/.
9. National Institute of Standards and Technology (NIST) – Computer Security Resource Center : URL: https://csrc.nist.gov/.
10. OWASP (Open Web Application Security Project) : URL: https://owasp.org/.
11. IEEE Standards Association : URL: https://standards.ieee.org/.
12. Wireshark Documentation : URL: https://www.wireshark.org/docs/.
13. SANS Institute Reading Room : URL: https://www.sans.org/white-papers/.
14. ENISA (European Union Agency for Cybersecurity) : URL: https://www.enisa.europa.eu/.