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

ЗАХИСТ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ

Галузь знань	12 Інформаційні технології
Спеціальність	122 Комп'ютерні науки
Назва освітньої програми	Комп'ютерні науки
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, доктор технічних наук, професор **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 _____ Ірина СОЛОВСЬКА

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="6">Кількість кредитів – 5

Загальна кількість годин – 150</td><td rowspan="6">Галузь –
12 – Інформаційні технології
Спеціальність –
122 – Комп’ютерні науки</td><td colspan="2">обов’язкова</td></tr>
<tr><td colspan="2">Рік підготовки:</td></tr>
<tr><td colspan="2">7-й</td></tr>
<tr><td colspan="2">Семестр</td></tr>
<tr><td>7-й</td><td>7-й</td></tr>
<tr><td colspan="2">Лекції</td></tr>
<tr><td rowspan="10">Мова навчання – українська</td><td rowspan="10">Рівень вищої освіти – перший (бакалаврський) рівень</td><td>26 год.</td><td>12 год.</td></tr>
<tr><td colspan="2">Практичні, семінарські</td></tr>
<tr><td>40 год.</td><td>8 год.</td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td></td><td></td></tr>
<tr><td colspan="2">Самостійна робота та індивідуальні завдання</td></tr>
<tr><td>84 год.</td><td>130 год.</td></tr>
<tr><td colspan="2">Вид контролю:</td></tr>
<tr><td>екзамен</td><td>екзамен</td></tr>
</table>

Дисципліна «Захист інформації в інформаційно-комунікаційних системах» є обов’язковим компонентом освітньої програми «Комп’ютерні науки» для здобуття освітнього рівня «бакалавр» й спрямована на формування знань і навичок із захисту інформації в інформаційно-комунікаційних системах, включаючи криптографічні методи, мережеву безпеку, організаційні заходи та сучасні технології кіберзахисту.

МЕТА ДИСЦИПЛІНИ. Метою дисципліни є забезпечення здобувачів знаннями з питань захисту інформації у інформаційно-комунікаційних системах від порушення її конфіденційності, цілісності та доступності з урахуванням сучасного стану та перспективних напрямів розвитку криптографії та стеганографії, а також набуття практичних навичок застосування криптографічних, технічних, організаційних та мережевих методів захисту інформації під час її передавання, оброблення та зберігання.

ПРЕРЕКВІЗИТИ. Передумовами вивчення дисципліни є знання і вміння, отримані здобуачем при вивченні навчальних дисциплін бакалаврської підготовки. Дисципліна базується на основних положеннях дисциплін*:* «Вища математика», «Дискретна математика», «Теорія інформації та кодування», «Комп'ютерні мережі».

ПОСТРЕКВІЗИТИ. Зміст дисципліни узгоджено з освітньо-професійною програмою підготовки фахівців з комп'ютерних наук та забезпечує необхідну теоретичну й практичну базу для подальшого вивчення дисциплін бакалаврської підготовки, практики та написанні кваліфікаційної роботи.

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

Інтегральна компетентність

Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі комп'ютерних наук або у процесі навчання, що передбачає застосування теорій та методів інформаційних технологій і характеризується комплексністю та невизначеністю умов.

Загальні компетентності (ЗК)

ЗК6. Здатність вчитися й оволодівати сучасними знаннями.

ЗК7. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

ЗК11. Здатність приймати обґрунтовані рішення.

ЗК14. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.

Спеціальні компетентності (СК)

СК1. Здатність до математичного формулювання та досліджування неперервних та дискретних математичних моделей, обґрунтовування вибору методів і підходів для розв'язування теоретичних і прикладних задач у галузі комп'ютерних наук, аналізу та інтерпретування.

СК14. Здатність застосовувати методи та засоби забезпечення інформаційної безпеки, розробляти й експлуатувати спеціальне програмне забезпечення захисту інформаційних ресурсів об'єктів критичної інформаційної інфраструктури.

СК17. Здатність проєктувати та керувати інформаційно-комунікаційними системами, забезпечувати розробку та супровід програмного забезпечення.

Програмні результати навчання (ПРН)

ПР1. Застосовувати знання основних форм і законів абстрактно-логічного мислення, основ методології наукового пізнання, форм і методів вилучення, аналізу, обробки та синтезу інформації в предметній області комп'ютерних наук.

ПР13. Володіти мовами системного програмування та методами розробки програм, що взаємодіють з компонентами комп'ютерних систем, знати мережні технології, архітектури комп'ютерних мереж, мати практичні навички технології адміністрування комп'ютерних мереж та їх програмного забезпечення.

ПР16. Розуміти концепцію інформаційної безпеки, принципи безпечного проектування програмного забезпечення, забезпечувати безпеку комп'ютерних мереж в умовах неповноти та невизначеності вихідних даних.

ПР18. Здійснювати проєктування та керування інформаційно-комунікаційними системами, забезпечувати розробку та супровід програмного забезпечення.

Заплановані результати навчання за навчальною дисципліною

Студент повинен знати:

– основні поняття та терміни інформаційної безпеки;

– принципи захисту інформації (конфіденційність, цілісність, доступність);

– об'єкти та суб'єкти захисту в інформаційно-комунікаційних системах;

– основні види загроз, моделі загроз і порушників; нормативно-правову базу захисту інформації в Україні;

– основи криптографічного захисту інформації, класичні методи шифрування, принципи роботи симетричних алгоритмів, мережі Фейстеля та SP-мереж;

– сучасні стандарти шифрування; принципи ідентифікації, автентифікації та електронного цифрового підпису;

– основи стеганографічного захисту;

– протоколи безпеки мережевих комунікацій;

– методи захисту мережевої інфраструктури, безпроводових і мобільних мереж;

– принципи управління інформаційною безпекою, оцінювання ризиків, моніторингу інцидентів, аудиту та тестування безпеки інформаційно-комунікаційних систем.

Студент повинен вміти:
– аналізувати загрози інформаційній безпеці;
– визначати об’єкти захисту в інформаційно-комунікаційних системах;
– будувати моделі загроз та порушників;
– застосовувати криптографічні методи для захисту інформації;
– використовувати системи ідентифікації та автентифікації;
– застосовувати електронний цифровий підпис;
– аналізувати безпеку мережевих протоколів;
– оцінювати ризики інформаційної безпеки;
– проводити базовий аудит інформаційної безпеки;
– розробляти комплексні заходи захисту інформації.

3. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Тема 1. Основи інформаційної безпеки в інформаційно-комунікаційних системах. Актуальність проблеми захисту інформації, основні принципи та об’єкти захисту в інфокомунікаційних системах. **Нормативно-правове забезпечення** захисту інформації в інформаційно-комунікаційних системах. Моделі загроз і порушників у інформаційно-комунікаційних системах мережах.

Тема 2. Криптографічні механізми захисту інформації. Основні поняття криптографічного захисту інформації. Класичні методи шифрування. Симетричні криптографічні алгоритми. Алгоритми шифрування на базі мережі Фейстеля. Сучасні стандарти шифрування, що побудовані на SP-мережі. Системи ідентифікації та автентифікації. Електронний цифровий підпис. Основи стеганографічного захисту інформації. Сумісне використання стеганографічного та криптографічного захисту інформації.

Тема 3. Технічні засоби та протоколи захисту інформації в інформаційно-комунікаційних системах. Протоколи безпеки мережевих комунікацій. Захист мережевої інфраструктури. Інтеграція інтелектуального відеоспостереження в системи безпеки. Безпека безпроводових і мобільних мереж.

Тема 4. Управління безпекою інформаційно-комунікаційних систем. Управління ризиками в інформаційно-комунікаційних системах. Моніторинг, виявлення та реагування на інциденти. Аудит та тестування безпеки інформаційно-комунікаційних систем. Комплексні підходи до побудови систем інформаційної безпеки. Перспективи та сучасні тенденції захисту інформації в інформаційно-комунікаційних системах та мережах

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.	прак.	сам. роб.		лекц.	лаб.	прак.	сам. роб.
Тема 1. Основи інформаційної безпеки в інформаційно-комунікаційних системах. Актуальність проблеми захисту інформації, основні принципи та об'єкти захисту в інфокомунікаційних системах. **Нормативно-правове забезпечення** захисту інформації в інформаційно-комунікаційних системах. Моделі загроз і порушників у інформаційно-комунікаційних системах мережах.	30	4		10	16	30	4		2	24
Тема 2. Криптографічні механізми захисту інформації. Основні поняття криптографічного захисту інформації. Класичні методи шифрування. Симетричні криптографічні алгоритми. Алгоритми шифрування на базі мережі Фейстеля. Сучасні стандарти шифрування, що побудовані на SP-мережі. Системи ідентифікації та автентифікації. Електронний цифровий підпис. Основи стеганографічного захисту інформації. Сумісне використання стеганографічного та криптографічного захисту інформації.	40	6		10	24	40	2		2	36
Тема 3. Технічні засоби та протоколи захисту інформації в інформаційно-комунікаційних системах. Протоколи безпеки мережевих комунікацій. Захист мережевої інфраструктури. Інтеграція інтелектуального відеоспостереження в системи безпеки. Безпека безпроводових і мобільних мереж.	40	8		10	22	40	4		2	34
Тема 4. Управління безпекою інформаційно-комунікаційних систем. Управління ризиками в	40	8		10	22	40	2		2	36

інформаційно-комунікаційних системах. Моніторинг, виявлення та реагування на інциденти. Аудит та тестування безпеки інформаційно-комунікаційних систем. Комплексні підходи до побудови систем інформаційної безпеки. Перспективи та сучасні тенденції захисту інформації в інформаційно-комунікаційних системах та мережах										
Усього годин	**150**	**26**		**40**	**84**	**150**	**12**		**8**	**130**
ПІДСУМКОВИЙ КОНТРОЛЬ – ЕКЗАМЕН										

5. ПИТАННЯ ДО ПРАКТИЧНИХ ЗАНЯТЬ

№ з/п	Назва теми	Кількість годин	
		денна форма	заочна форма
1	**Тема 1. Основи інформаційної безпеки в інформаційно-комунікаційних системах**. Актуальність проблеми захисту інформації, основні принципи та об'єкти захисту в інфокомунікаційних системах. **Нормативно-правове забезпечення** захисту інформації в інформаційно-комунікаційних системах. Моделі загроз і порушників у інформаційно-комунікаційних системах мережах.	10	2
2	**Тема 2. Криптографічні механізми захисту інформації.** Основні поняття криптографічного захисту інформації. Класичні методи шифрування. Симетричні криптографічні алгоритми. Алгоритми шифрування на базі мережі Фейстеля. Сучасні стандарти шифрування, що побудовані на SP-мережі. Системи ідентифікації та автентифікації. Електронний цифровий підпис. Основи стеганографічного захисту інформації. Сумісне використання стеганографічного та криптографічного захисту інформації.	10	2
3	**Тема 3. Технічні засоби та протоколи захисту інформації в інформаційно-комунікаційних системах**. Протоколи безпеки мережевих комунікацій. Захист мережевої інфраструктури. Інтеграція інтелектуального відеоспостереження в системи безпеки. Безпека безпроводових і мобільних мереж.	10	2
4	**Тема 4. Управління безпекою інформаційно-комунікаційних систем.** Управління ризиками в інформаційно-комунікаційних системах. Моніторинг, виявлення та реагування на інциденти. Аудит та тестування безпеки інформаційно-комунікаційних систем. Комплексні підходи до побудови систем інформаційної безпеки. Перспективи та сучасні тенденції захисту інформації в інформаційно-комунікаційних системах та мережах	10	2
	Всього	**40**	**8**

6. САМОСТІЙНА РОБОТА

До самостійної роботи здобувачів щодо вивчення дисципліни «Захист інформації в інформаційно-комунікаційних системах» 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	**Тема 1. Основи інформаційної безпеки в інформаційно-комунікаційних системах**. Аналіз загроз інформації при передачі по каналах зв'язку. Методи захисту інформації в каналах зв'зку. Поняття інформаційної безпеки у інформаційно-комунікаційних систем. Ключові принципи захисту: конфіденційність, цілісність, доступність. Типові загрози та вразливості у мережах зв'язку. Об'єкти захисту, класифікація засобів захисту. Роль політик безпеки. Поняття загрози та порушника: визначення, класифікація, приклади. Взаємозв'язок між моделями загроз і порушників. Практичне застосування моделей загроз та порушників, використання у проектуванні політик безпеки та систем захисту інфокомунікаційних мереж. Законодавча база України у сфері інформаційної безпеки та захисту інформації. Міжнародні нормативні документи та стандарти (ISO/IEC 27000-series, рекомендації ITU, директиви ЄС).	16	24
2	**Тема 2. Криптографічні механізми захисту інформації.** Призначення криптографічного захисту. Архітектура інформаційно-комунікаційних систем та точки вразливості. Принципи побудови систем захисту інформації. Схема побудови складного шифру. Особливості та призначення симетричних криптосистем. Дослідження алгоритму шифрування DES. Режими роботи та недоліки. Методи підвищення криптостійкості криптосистеми. Алгоритм 3-DES. Криптосистема IDEA. Схема SP-мережі. Реалізація SP-мережі в криптосистемах AES та ДСТУ 7624:2014 «Калина». Прості методи автентифікації за паролем. Біометричні методи автентифікації. Класифікація асиметричних криптосистем за призначенням. Метод генерування та розподілення ключів Діффі-Хеллмана. Процедури генерування асиметричної пари ключів та система шифрування RSA. Процедура шифрування в криптосистемі Ель–Гамаля. Біометрико-криптографічні перетворення при підтвердженні справжності користувача. Багатофакторна автентифікація. Методи побудови схем електронного підпису. Процедура створення підпису в адгоритмі RSA. Різновиди ЕП.	24	36

3	**Тема 3. Технічні засоби та протоколи захисту інформації в інформаційно-комунікаційних системах**. Призначення протоколів безпеки (SSL/TLS. IPsec, SSH, HTTPS, Kerberos, S/MIME та PGP). Загрози та методи захисту мережевої інфраструктури. Типові загрози (перехоплення трафіку, атаки «людина посередині» (MITM), підроблені точки доступу, IMSI-catchers, шкідливі мобільні додатки). Методи захисту Wi-Fi мереж (WPA2/WPA3, сегментація мережі, контроль доступу). Поняття, структура, типи політик. Політики Zero Trust, адаптивні політики безпеки, інтеграція з хмарними сервісами.	22	34
4	**Тема 4. Управління безпекою інформаційно-комунікаційних систем.** Методологія управління ризиками. Управління ризиками інформаційної безпеки (ISO/IEC 27005). NIST Risk Management Framework. Методики OCTAVE, FAIR. Засоби захисту (IDS/IPS, SIEM, криптографічні рішення). Принципи безперервного моніторингу. Використання SIEM-систем (Security Information and Event Management). Системи IDS/IPS (Intrusion Detection/Prevention Systems). План реагування на інциденти (Incident Response Plan). Методології аудиту (ISO/IEC 27001, COBIT, NIST). Рекомендації з безпеки (ISO/IEC 27002). OWASP Testing Guide для веб-додатків. Рекомендації CERT щодо тестування та аудиту. Принципи побудови системи. Принцип «захист у глибину» (defense in depth). Значення інформаційної безпеки в умовах цифрової трансформації. Тенденції розвитку технологій захисту. Використання штучного інтелекту та машинного навчання для виявлення аномалій. Автоматизація реагування на інциденти (SOAR-платформи). Інтеграція кібербезпеки у всі бізнес-процеси. Використання квантових технологій для криптографії майбутнього.	22	36
	Всього	**84**	**130**

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 тощо.	**50%**	**100%**
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

Питання до підсумкового контролю

1. Поняття інформаційної безпеки та її значення в інформаційно-комунікаційних системах.
2. Основні принципи інформаційної безпеки (конфіденційність, цілісність, доступність).
3. Основні об’єкти та суб’єкти захисту в інформаційно-комунікаційних системах.
4. Основні загрози інформаційній безпеці в інформаційно-комунікаційних системах.
5. Моделі загроз у системах захисту інформації.
6. Моделі порушників та їх класифікація.
7. Нормативно-правове забезпечення захисту інформації в Україні.
8. Поняття криптографічного захисту інформації та його основні задачі.
9. Основні терміни та елементи криптографічних систем.
10. Класичні методи шифрування та їх характеристика.
11. Симетричні криптографічні алгоритми та принцип їх роботи.
12. Структура та принцип роботи мережі Фейстеля.
13. Криптографічні алгоритми, побудовані на основі мережі Фейстеля.
14. Принцип побудови SP-мереж у сучасних алгоритмах шифрування.
15. Сучасні стандарти криптографічного шифрування.
16. Поняття та принципи роботи систем ідентифікації.
17. Методи та механізми автентифікації користувачів.
18. Електронний цифровий підпис та його призначення.
19. Основні принципи роботи електронного цифрового підпису.
20. Поняття стеганографії та її застосування у захисті інформації.
21. Основні методи стеганографічного захисту інформації.
22. Сумісне використання криптографії та стеганографії.
23. Протоколи безпеки мережевих комунікацій.
24. Основні методи захисту мережевої інфраструктури.
25. Засоби та технології забезпечення безпеки комп’ютерних мереж.
26. Безпека безпроводових мереж та основні загрози.
27. Особливості захисту мобільних мереж.
28. Управління ризиками в інформаційно-комунікаційних системах.
29. Моніторинг, виявлення та реагування на інциденти інформаційної безпеки.
30. Аудит, тестування безпеки та сучасні тенденції розвитку систем захисту інформації.

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[1], 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.

[1] Індивідуально-консультативна робота викладача зі здобувачами

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.

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 . Криптографічний захист інформації: Навч. посіб./ Йона Л.Г., Онацький О.В., Бєлова Ю.В. - Одеса: ДУІТЗ, 2023. – 250 с.

2. Жилін А. В., Шаповал О. М., Успенський О. А. Технології захисту інформації в інформаційно-телекомунікаційних системах: навчальний посібник. Київ: КПІ ім. Ігоря Сікорського, 2020.

3. Остапов С. Е., Євсеєв С. П., Король О. Г. Кібербезпека: сучасні технології захисту: навчальний посібник. Львів: Новий Світ-2000, 2020.

4. Andress J. The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice. – 3rd ed. – Amsterdam : Elsevier, 2020. – 240 p.

5. Комплекс навчально-методичного забезпечення навчальної дисципліни "Захист систем електронної комерції та мультисервісних систем", освітньо-кваліфікаційний рівень бакалавр для спеціальності 125 - Кібербезпека [Електронний ресурс] : освітня програма підготовки "Управління інформаційною безпекою" / ХНУРЕ ; розроб. Т.А. Радівілова. – Харків, 2019. – 397 с.

5. Stallings W. Effective Cybersecurity: A Guide to Using Best Practices and Standards. – Boston : Addison-Wesley, 2018. – 336 p.

6. ДСТУ ISO/IEC 27001:2023. Інформаційна безпека, кібербезпека та захист приватності. Системи управління інформаційною безпекою. Вимоги. – Київ : ДП «УкрНДНЦ», 2023.

7. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements. – Geneva : ISO, 2022.

Допоміжна

8. Андерсон Р. Дж. Інженерія безпеки: посібник для створення захищених систем. Пер. з англ. Київ: Логос, 2010.

9. Mulesa, O., Horvat, P., Radivilova, T., Sabadosh, V., Baranovskyi, O., & Duran, S. (2023). Design of mechanisms for ensuring the execution of tasks in project planning . Eastern-European Journal of Enterprise Technologies, 2(4 (122), 16–22.

10. Lyudmyla Kirichenko, Tamara Radivilova, Oksana Pichugina, Larysa Chala, Danyil Khandak. Trend Detection in Short Time Series Using Discrete Wavelet Transform. Proceedings of the

IX International Scientific Conference "Information Technology and Implementation" (IT&I-2022). Kyiv, Ukraine, November 30 - December 02, 2022. Vol.3347, pp.159-168.

11. Lyudmyla Kirichenko, Tamara Radivilova, Juliia Stepanenko. Applying Recurrence Plots to Classify Time Series. Proceedings of the 5th International Conference on Computational Linguistics and Intelligent Systems (COLINS 2021). Volume I: Main Conference, Lviv, Ukraine, April 22-23, 2021. Vol.2870. pp. 1770-1780.

12. Radivilova, T., Kirichenko, L., Tawalbeh, M., & Ilkov, A. (2021). Виявлення аномалій в телекомунікаційному трафіку статистичними методами. Електронне фахове наукове видання "Кібербезпека: освіта, наука, техніка, 3(11), 2021, 183-194.

Інформаційні ресурси

1 Національна бібліотека України ім. В.І. Вернадського. URL: http://www.nbuv.gov.ua.
2 Портал кіберполіції України. URL: https://cyberpolice.gov.ua/
3 ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Женева: International Organization for Standardization, 2022. Режим доступу: https://www.iso.org/standard/27001