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

КРИПТОГРАФІЯ ТА КРИПТОАНАЛІЗ

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 28.08. 2025 року.

Розробники і викладачі	**Контактний тел.**	**E-mail**
доцент кафедри комп'ютерної інженерії та інноваційних технологій к.т.н., доцент **ЙОНА Лариса Григорівна**	+380677463777	Yonalarisa66@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

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 – 4

Загальна кількість годин – 120</td><td>Галузь – 12 Інформаційні технології</td><td colspan="2">обов’язкова</td></tr>
<tr><td rowspan="5">Спеціальність – 125 Кібербезпека та захист інформації</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td colspan="2">3-й</td></tr>
<tr><td colspan="2">Семестр</td></tr>
<tr><td>5-й</td><td>5-й</td></tr>
<tr><td colspan="2">Лекції</td></tr>
<tr><td rowspan="11">Мова навчання – українська</td><td rowspan="11">Рівень вищої освіти – перший (бакалаврський) рівень</td><td>26 год.</td><td>4 год.</td></tr>
<tr><td colspan="2">Практичні, семінарські</td></tr>
<tr><td>20 год.</td><td>4 год.</td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>6 год.</td><td>2 год.</td></tr>
<tr><td colspan="2">Самостійна робота та індивідуальні завдання</td></tr>
<tr><td>68 год.</td><td>110 год.</td></tr>
<tr><td colspan="2">Вид контролю:</td></tr>
<tr><td>Екзамен</td><td>Екзамен</td></tr>
</table>

Криптографія та криптоаналіз є складовою частиною навчального процесу у підготовці фахівців зі спеціальності 125 «Кібербезпека та захист інформації», а також обов’язковим компонентом освітньої програми для здобуття освітнього рівня «бакалавр» та має на меті формування у здобувачів уявлення про принципи побудови симетричних та асиметричних криптографічних систем, проблеми захисту інформації від порушення її конфіденційності, цілісності та доступності; принципи побудови та режими роботи блокових алгоритмів шифрування; розгляд концепції криптосистем з відкритим ключем; методи побудови схем електронно-цифрових підписів та керування криптографічними ключами, а також методи криптоаналізу для оцінки надійності систем захисту.

Метою викладання навчальної дисципліни Криптографія та криптоаналіз є забезпечення здобувачів знаннями з питань принципів побудови криптографічних систем та проблем захисту інформації у системах комунікацій з урахуванням сучасного стану та перспективних напрямів розвитку криптології; формує критичне мислення щодо вибору та впровадження засобів захисту інформації.

ПРЕРЕКВІЗИТИ. Передумовами є знання з Вищої математики (ОК 5), Теорії ймовірностей та математичної статистики (ОК 6), Дискретної математики (ОК 9), «Захисту інформації в інфокомунікаційних системах та мережах» (ОК 12) та Теорії інформації та кодування (ОК 25).

ПОСТРЕКВІЗИТИ. Знання алгоритмів шифрування та методів криптоаналізу є необхідними при вивченні «Комплексних систем захисту інформації» (ОК 24), «Систем технічного захисту інформації» (ОК 31), «Безпеки програм та даних» (ОК 16), «Управління інформаційною та кібербезпекою» (ОК 30), «Основ цифрової криміналістики» (ОК 26) та «Етичного хакінгу та тестування на проникнення» (ОК 18).

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

У процесі реалізації програми дисципліни «Криптографія та криптоаналіз» 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 2. Знання та розуміння предметної області та розуміння професійної діяльності

Спеціальні (фахові, предметні) компетентності

СК 4. Здатність забезпечувати захист інформації в інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації.

СК 8. Здатність застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.

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 «Криптографія та криптоаналіз» забезпечує досягнення програмних результатів навчання (РН), передбачених освітньою програмою:

РН 7. Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення і передачі сигналів тощо, принципи, методи, поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності

РН 9. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації

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

РН 19. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів.

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.

3. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Змістовий модуль 1. Криптографічні методи захисту інформації

Тема 1. Криптологія: основні поняття та історичний розвиток.

Поняття інформаційної безпеки та роль криптографії. Історичний розвиток криптографії: від класичних шифрів до сучасних алгоритмів. Базові терміни та визначення: шифр, ключ, криптосистема, криптоаналіз.

Тема 2. Основи архітектури криптосистем. Структурні елементи криптосистеми. Моделі побудови та взаємодії компонентів. Принципи безпеки та їх реалізація.

Тема 3. Потокові симетричні шифри. Блокові симетричні шифри.

Принципи роботи потокових шифрів. Основні приклади та застосування. Архітектура блокових шифрів, Принцип каскадування. Шифри на базі мережі Фейстеля: 3-DES, IDEA, ДСТУ 28147-2009. Шифри на базі SP-мережі: AES, ДСТУ 7624:2014. Режими роботи симетричних алгоритмів.

Тема 4. Асиметричні методи шифрування.

Концепція асиметричних криптосистем. Обчислення відкритого та закритого ключа, математичні основи асиметричних систем. Призначення двоключових алгоритмів. Алгоритми RSA, Ель Гамаля. Криптосистеми на еліптичних кривих.

Тема 5. Протоколи керування криптографічними ключами.

Принципи керування криптографічними ключами: генерування, накопичування та розподілення ключів. Протокол Діффі-Геллмана, MQV, Kerberos, Needham-Schroeder.

Тема 6. Стандарти та схеми електронного підпису. Призначення електронного підпису. Автентифікація документу. Електронний підпис RSA, недоліки алгоритму. Види електронних підписів.

Змістовий модуль 2. Дослідження методів криптоаналізу

Тема 7. Теоретична та практична стійкість. Поняття стійкості. Рівні стійкості: індивідуальна, групова, інституційна, державна. Ключові характеристики теоретичної стійкості (адаптивність, гнучкість, відновлення). Моделі та типології стійкості в соціології, психології та кібербезпеці. Взаємозв'язок між стійкістю та безпекою.

Тема 8. Криптоаналіз шифрів перестановки. Властивості перестановочних шифрів та їх криптостійкість. Основні принципи криптоаналізу перестановочних шифрів. Частотний аналіз як метод розкриття перестановки. Використання статистичних характеристик тексту. Метод проб і помилок (brute force) та його обмеження. Алгоритмічні підходи до відновлення перестановки. Використання відомих відкритих текстів (known plaintext attack). Використання частково відомих відкритих текстів (cribs).

Тема 9. Криптоаналіз шифрів одноалфавітної заміни.

Властивості та криптостійкість одноалфавітних шифрів. Частотний аналіз як основний метод розкриття шифрів заміни. Використання статистичних характеристик природної мови. Використання відомих відкритих текстів (known plaintext attack). Використання частково відомих відкритих текстів (cribs). Алгоритмічні та програмні підходи до криптоаналізу.

Тема 10. Криптоаналіз шифрів багатоалфавітної заміни.

Властивості та криптостійкість багатоалфавітних шифрів. Основні принципи криптоаналізу багатоалфавітних шифрів. Частотний аналіз у випадку багатоалфавітної заміни. Метод Kasiski для визначення довжини ключа. Індекс відповідності (Index of Coincidence) як інструмент криптоаналізу. Використання відомих відкритих текстів (known plaintext attack). Використання ключових слів та "cribs" для відновлення шифру. Програмні методи криптоаналізу.

Тема 11. Диференціальний та лінійний криптоаналіз.

Основні принципи лінійного криптоаналізу. Використання лінійних апроксимацій для опису роботи шифру. Ймовірності відхилення від рівномірного розподілу. Приклади застосування лінійного криптоаналізу до блочних шифрів. Обмеження та складність методу. Порівняння диференціального та лінійного криптоаналізу. Методи комбінованого використання для посилення криптоаналізу.

Тема 12. Методи факторизації. Методи дискретного логарифмування.

Поняття факторизації та її роль у криптографії. Класичні методи факторизації: метод

пробних дільників, метод Ферма, метод Полларда (ρ-алгоритм). Сучасні методи факторизації: квадратичне решето (Quadratic Sieve); метод числового решета (Number Field Sieve). Ефективність різних методів факторизації залежно від розміру числа. Складність факторизаційних алгоритмів. Класичні методи обчислення дискретного логарифма: метод проб і помилок (brute force), метод “baby-step giant-step” (Шенкса). Порівняння ефективності різних методів дискретного логарифмування. Складність алгоритмів дискретного логарифмування. Взаємозв’язок факторизації та дискретного логарифмування у криптоаналізі.

Тема 13. Стійкість та криптоаналіз схем електронного підпису.

Види атак на електронний підпис: атаки на ключ, атаки на алгоритм, атаки на реалізацію (side-channel attacks). Захист від підробки підпису та повторного використання. Методи атак із використанням відомих відкритих текстів та підписів. Використання колізій хеш-функцій для компрометації підпису. Взаємозв’язок між стійкістю та криптоаналізом.

Тема 14. Сучасні тенденції та практичні аспекти криптоаналізу.

Поняття криптоаналізу та його роль у сучасній криптографії. Використання алгоритмів машинного навчання та штучного інтелекту у криптоаналізі. Перспективи розвитку криптоаналізу в умовах квантових та постквантових технологій.

4. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Назви змістових модулів і тем	Кількість годин									
	денна форма					Заочна форма				
	усього	у тому числі				усього	у тому числі			
		лк	лб.	пр.	сам. роб.		лекц.	лр.	пр.	сам. роб.
Змістовий модуль 1. Криптографічні методи захисту інформації										
Тема 1. Криптологія: основні поняття та історичний розвиток.	8	2		2	4	6				6
Тема 2. Основи архітектури криптосистем.	8	2		2	4	8				8
Тема 3. Потокові симетричні шифри. Блокові симетричні шифри.	10	2		2	6	10	2			8
Тема 4. Асиметричні методи шифрування.	10	2		2	6	8				8
Тема 5. Протоколи керування криптографічними ключами.	10	2		2	6	8				8
Тема 6. Стандарти та схеми електронного підпису	6			2	4	8				8
Змістовий модуль 2. Дослідження методів криптоаналізу										
Тема 7. Теоретична та практична стійкість.	8	2		2	4	8				8
Тема 8. Криптоаналіз шифрів перестановки	10	2	2		6	10		2		8
Тема 9. Криптоаналіз шифрів одноалфавітної заміни.	10	2	2		6	10	2			8
Тема 10. Криптоаналіз шифрів багатоалфавітної заміни.	8	2	2		4	10			2	8
Тема 11. Диференціальний та лінійний криптоаналіз.	8	2		2	4	8				8
Тема 12. Методи факторизації. Методи дискретного логарифмування.	8	2		2	4	10			2	8
Тема 13. Стійкість та криптоаналіз схем електронного підпису.	10	2		2	6	8				8
Тема 14. Сучасні тенденції та практичні аспекти криптоаналізу	6	2			4	8				8
Усього годин	**120**	**26**	**6**	**20**	**68**	**120**	**4**	**2**	**4**	**110**
ПІДСУМКОВИЙ КОНТРОЛЬ – ЕКЗАМЕН										

5. ПРАКТИЧНІ РОБОТИ

Назва теми	Кількість годин	
	Денна форма	Заочна форма
1. Дослідження класичних методів шифрування.	2	
2. Поєднання криптографії та стеганографії в класичних шифрах.	2	
3. Принципи побудови композиційних шифрів.	2	
4. Дешифрування класичних шифрів	2	2

5. Дослідження шифрів на базі мережі Фейстеля. ДСТУ 28147–2009	2	
6. Дослідження стандарту шифрування AES.	2	
7. Дослідження методу розподілення ключів.	2	
8. Дослідження методів асиметричного шифрування.	2	
9. Принципи побудови електронного підпису.	2	
10. Дослідження методів криптоаналізу.	2	2
Всього	**20**	**4**

6. ЛАБОРАТОРНІ РОБОТИ

Назва теми	**Кількість годин**	
	Денна форма	**Заочна форма**
1. Криптоаналіз шифрів перестановки	2	2
2. Криптоаналіз шифрів одноалфавітної заміни.	2	
3. Криптоаналіз шифрів багатоалфавітної заміни.	2	
Всього	**6**	**2**

7. САМОСТІЙНА РОБОТА

До самостійної роботи студентів щодо вивчення дисципліни 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 контрольних робіт.
7. Підготовка до підсумкового контролю.

Тематика та питання до самостійної підготовки та індивідуальних завдань

№	Тема	Кількість годин	
		Денна	Заочна
1	**Тема 1. Криптологія: основні поняття та історичний розвиток**. Криптографія в класичних шифрах.	4	6
2	**Тема 2. Основи архітектури криптосистем.** Класифікація та призначення криптографічних перетворень.Принцтпи побудови криптосистем.	4	8
3	**Тема 3. Сучасні симетричні криптосистеми.** Особливості побудови ДСТУ 7624:2014.	6	8
4	**Тема 4. Асиметричні методи шифрування.** Криптосистеми RSA та Ель Гамаля.	6	8
5	**Тема 5. Протоколи керування криптографічними ключами.** Протокол Діффі-Геллмана, MQV, Kerberos, Needham-Schroeder.	6	8
6	**Тема 6. Стандарти та схеми електронного підпису.** Електронний підпис Шнорра, Ніберга-Рюпеля	4	8
7	**Тема 7. Теоретична та практична стійкість.** Статистичний аналіз криптограм, статистичні моделі Шеннона і Маркова та їх застосування в крипто аналізі.	4	8
8	**Тема 8. Криптоаналіз шифрів перестановки**	6	8
9	**Тема 9. Криптоаналіз шифрів одноалфавітної заміни.** Криптоаналіз омофоніческой (гомофоніческой) заміни.	6	8
10	**Тема 10. Криптоаналіз багатоалфавітної заміни.** Частотний криптоаналіз. Метод Казіскі, Фрідмана.	4	8
11	**Тема 11. Диференціальний та лінійний криптоаналіз.** Аналіз режимів роботи симетричних алгоритмів шифрування.	4	8
12	**Тема 12. Методи факторизації. Методи дискретного логарифмування.** Метод решета у числовому полі. Метод Полларда	4	8
13	**Тема 13. Стійкість та криптоаналіз схем електронного підпису.** Класифікація атак на схеми електронного підпису.	6	8
14	**Тема 14. Сучасні тенденції та практичні аспекти криптоаналізу**	4	8
	Всього	**68**	**110**

8. 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, екзамен

Питання до екзамену

1. Дайте визначення понять «шифр», «ключ», «криптосистема», «криптоаналіз».
2. Поясніть роль криптографії в системі інформаційної безпеки.
3. Назвіть структурні елементи криптосистеми та поясніть їх функції.
4. Які принципи безпеки реалізуються в сучасних криптосистемах?
5. Поясніть принцип роботи потокових симетричних шифрів та наведіть приклади їх застосування.
6. Охарактеризуйте архітектуру блокових шифрів на базі мережі Фейстеля.
7. Дати характеристику криптосистеми AES.
8. Дати характеристику криптосистеми ДСТУ 7624:2014.
9. Порівняйте алгоритми AES та ДСТУ 7624:2014.
10. Поясніть математичні основи алгоритму RSA.
11. У чому полягає перевага криптосистем на еліптичних кривих?
12. Опишіть принцип роботи протоколу Діффі-Геллмана.
13. Які особливості має протокол Kerberos?
14. Поясніть призначення електронного підпису та його роль у автентифікації документів.
15. Які недоліки має алгоритм RSA для електронного підпису?
16. Дайте визначення поняття «криптостійкість».
17. Опишіть методи криптоаналізу перестановочних шифрів.
18. Як застосовується частотний аналіз для розкриття перестановки?
19. Які особливості має криптостійкість одноалфавітних шифрів?
20. Опишіть алгоритмічні підходи до криптоаналізу одноалфавітних шифрів.
21. У чому полягає метод Kasiski для визначення довжини ключа?
22. Поясніть принципи лінійного криптоаналізу.
23. Порівняйте диференціальний та лінійний криптоаналіз.
24. В чому суть метод Полларда (ρ-алгоритм).
25. У чому полягає метод «baby-step giant-step»?
26. Які види атак застосовуються проти електронного підпису?
27. Як колізії хеш-функцій можуть призвести до компрометації підпису?
28. Які перспективи розвитку криптоаналізу в умовах квантових технологій?
29. Як алгоритми машинного навчання застосовуються у криптоаналізі?
30. Поясніть принцип каскадування блокових шифрів та його значення для підвищення стійкості.

9. 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 тарозкладу 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 тарозкладу 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 підготовку 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 ІСПИТ (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.

10. 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		

11. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

1. Про внесення змін до Закону України "Про інформацію" № 2938-VI від 13.01.2011. – Відомості Верховної Ради України 2011, № 32, ст. 313.
2. Закон України "Про захист персональних даних" № 2297-VI від 01.06.2010. – Відомості Верховної Ради України 2010, № 34, ст. 481.
3. Закон України "Про критичну інфраструктуру" № 2684-IX від 18.10.2022.
4. Онацький О.В., Йона Л.Г., Бєлова Ю.В. Криптографічний захист інформації: Навч. посібник. - Одеса: Одеса : «Астропринт» 2023. 252с. https://surl.li/onvhbl
5. Йона Л.Г., Онацький О.В., Швець О.В. Системи банківської безпеки: Навч. посібник.- Одеса: ДУІТЗ. 2022. 192с. https://surl.lt/hpdpub
6. Онацький О.В. Методологія створення комплексної системи захисту інформації / Прикладная радиоэлектроника: науч.-техн. журнал ХНУР – 2014. Том 13. – № 3 – С. 350-356.
7. Онацький О. В., Йона Л. Г. Криптографічні системи : навчальний посібник з дисциплін "Криптографія та криптоаналіз" для освітньо-професійної підготовки бакалаврів в галузі знань 12 "Інформаційні технології" за спеціальністю 125 "Кібербезпека" / О. В. Онацький, Л. Г. Йона. – Одеса : Міжнародний гуманітарний університет, 2023. – 156 с. https://surl.li/oqiqhk
8. НД ТЗІ 3.7-003-2023 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-комунікаційній системі (Наказ Адміністрації Держспецзв'язку від 28.10.

Допоміжна

9. ДСТУ ISO/IEC 27002:2015 Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки.
10. Schneier B. Applied Cryptography: Protocols, Algorithms and Source Code in C: 20th Anniversary Edition. Wiley, 2015. 784 p.

11. Остапо С. Е., Євсеєв С. П., Король О. Г. Технології захисту інформації: навч. посіб. Харків: ХНЕУ, 2013. 476 с.

Інформаційні ресурси

12. ДСТУ 4145-2002. URI: https://dbn.co.ua/load/normativy/dstu/4145/5-1-0-1798
13. AES Rijndael Cipher explained as a Flash animation. URI: https://www.youtube.com/watch?v=gP4PqVGudtg
14. DES Animation. URI: https://www.youtube.com/watch?v=Vcld7CMAnNs
15. Presentation over Cryptographic Primitives (RC4). URI: https://www.youtube.com/watch?v=KM-xZYZXElk
16. IDEA algorithm. URI: https://www.youtube.com/watch?v=vt1Zfs_qz3Q
17. Сайт Державної служби спеціального зв'язку та захисту інформації. URL: https://cip.gov.ua/ua
18. Сайт Computer Emergency Response Team of Ukraine. URL: https://cert.gov.ua
19. https://zakon.rada.gov.ua/laws