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 ІНФОКОМУНІКАЦІЙНИХ СИСТЕМАХ ТА МЕРЕЖАХ

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**
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

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>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">2-й</td></tr>
<tr><td colspan="2">Семестр</td></tr>
<tr><td>3-й</td><td>3-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>6 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>10 год.</td><td>2 год.</td></tr>
<tr><td colspan="2">Самостійна робота та індивідуальні завдання</td></tr>
<tr><td>94 год.</td><td>138 год.</td></tr>
<tr><td colspan="2">Вид контролю:</td></tr>
<tr><td>Екзамен</td><td>Екзамен</td></tr>
</table>

Дисципліна «Захист інформації в інфокомунікаційних системах та мережах» є обов'язковою складовою освітньо-професійної програми підготовки бакалаврів зі спеціальності 125 «Кібербезпека та захист інформації» та спрямована на формування у здобувачів системних знань і практичних навичок щодо забезпечення конфіденційності, цілісності та доступності інформації під час її передавання, оброблення та зберігання в мережевих середовищах. Дисципліна охоплює криптографічні методи захисту, протоколи безпечної комунікації, технічні засоби мережевої безпеки, стеганографічні підходи та організаційні заходи протидії загрозам у інфокомунікаційних системах.

Метою викладання дисципліни є забезпечення здобувачів фундаментальними знаннями з принципів побудови захищених мережевих архітектур, механізмів шифрування та автентифікації, а також набуття практичних умінь застосовувати симетричні та асиметричні криптоалгоритми, налаштовувати протоколи безпеки (SSL/TLS, IPsec, SSH), аналізувати загрози мережевого рівня та впроваджувати технічні засоби захисту інформації відповідно до вимог нормативних документів та сучасних стандартів кібербезпеки.

ПРЕРЕКВІЗИТИ. Передумовами для вивчення дисципліни є базові знання з програмування («Основи програмування», ОК8), математики (ОК5, ОК9), початкові уявлення про сферу («Вступ до спеціальності», ОК11), а також паралельне вивчення «Комп'ютерних мереж» (ОК13) та «Теорії інформації та кодування» (ОК25).

ПОСТРЕКВІЗИТИ. Знання та навички із захисту інформації в мережах є базою для вивчення «Безпеки програм та даних» (ОК16), «Основ Web-безпеки» (ОК22), «Криптографія та криптоаналіз» (ОК23), «Комплексних систем захисту інформації» (ОК24), «Систем технічного захисту інформації» (ОК31), «Управління інформаційною та кібербезпекою» (ОК30), «Етичного хакінгу та тестування на проникнення» (ОК18), «Безпеки бездротових мереж Інтернету речей (IoT)» (ОК27), а також при виробничій практиці (ОК34) та підготовці кваліфікаційної роботи (ОК 6).

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 1. Здатність застосовувати законодавчу та нормативно правову базу, а також державні та міжнародні вимоги, практики і стандарти у професійній діяльності

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

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

СК 7. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою.

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.

Навчальна дисципліна «Захист інформації в інфокомунікаційних системах та мережах» 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 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 8. Застосовувати знання и розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної галузі кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення.

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

РН 11. Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахування вимог до захисту інформації.

РН 12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки.

РН 13. Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних і програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних й інформаційно-комунікаційних систем та/або інфраструктури організації в цілому.

РН 18. Аналізувати, застосовувати методи та засоби криптографічного

3. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Тема 1. Основи інформаційної безпеки в інфокомунікаційних системах. Поняття інформаційної безпеки та її складові (конфіденційність, цілісність, доступність). Загрози та вразливості інформаційних систем. Класифікація атак та методи їх реалізації. Міжнародні та національні стандарти інформаційної безпеки. Організаційні та правові аспекти захисту інформації.

Тема 2. Криптографічні механізми захисту інформації. Основні поняття криптографічного захисту: шифрування, розшифрування, дешифрування, ключі. Класичні методи шифрування. Симетричні та асиметричні алгоритми та їх розподілення за призначенням.

Тема 3. Системи ідентифікації, автентифікації та електронний підпис. Методи ідентифікації користувачів. Однофакторна та багатофакторна автентифікація. Біометричні системи автентифікації. Автентифікація документів. Електронний підпис: принципи роботи, правове регулювання. Використання токенів, смарт-карт та мобільних додатків.

Тема 4. Протоколи безпеки мережевих комунікацій. Основи захищених протоколів (SSL/TLS, HTTPS). Поняття VPN та IPSec. Приклади використання у повсякденних сервісах (онлайн-банкінг, електронна пошта, корпоративні системи).

Тема 5. Технічний захист мережевої інфраструктури.
Ознайомлення з поняттям «мережева інфраструктура». Базові принципи захисту: міжмережеві екрани, антивірусні системи, резервне копіювання. Відеоспостереження як елемент комплексної системи технічного захисту інформації. Приклади типових атак на інфраструктуру (DoS, MITM) та прості методи протидії.

Тема 6. Комплексні системи захисту інформації. Принципи побудови КСЗІ: системність, комплексність, багаторівневість**.** Політика безпеки: структура, цілі, відповідальність. Ролі та обов'язки персоналу: адміністратор безпеки, користувачі, аудитори**.** Документування та регламентація процесів. Методи оцінювання захищеності. Вимоги до КСЗІ згідно з ДСТУ та міжнародними стандартами ISO/IEC 27001.

Тема 7. Стеганографія та комплексні технічні системи захисту. Основи стеганографії та прихованих каналів передачі інформації. Методи приховування даних у цифрових медіа. Виявлення та протидія стеганографічним атакам. Інтеграція стеганографії з криптографічними методами. Комплексні системи захисту інформації: DLP, SIEM, SOC.

4. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Назви змістових модулів і тем	Кількість годин									
	денна форма					Заочна форма				
	усього	у тому числі				усього	у тому числі			
		лекц.	лабор	практ	сам. роб.		лекц.	лабор	практ	сам. роб.
Тема 1. Основи інформаційної безпеки в інфокомунікаційних системах.	16	2		2	12	20	2			18
Тема 2. Криптографічні механізми захисту інформації. Основні поняття криптографічного захисту.	18	4		2	12	22			2	20
Тема 3. Системи ідентифікації, автентифікації та електронний підпис.	22	4	2	2	14	22	2			20
Тема 4. Протоколи безпеки мережевих комунікацій.	24	4	2	4	14	20				20
Тема 5. Технічний захист мережевої інфраструктури.	24	4	2	4	14	22		2		20
Тема 6. Безпека бездротових і мобільних мереж.	22	4	2	2	14	22			2	20
Тема 7. Стеганографія та комплексні технічні системи захисту.	24	4	2	4	14	22	2			20
Усього годин	**150**	**26**	**10**	**20**	**94**	**150**	**6**	**2**	**4**	**138**
ПІДСУМКОВИЙ КОНТРОЛЬ – **Екзамен**										

5. ПРАКТИЧНІ РОБОТИ

Назва теми	Кількість годин	
	Денна форма	Заочна форма
1. Математичні основи криптографії.	2	
2. Дослідження шифрів перестановки.	2	
3. Дослідження шифрів простої заміни.	2	
4. Дослідження шифрів складної заміни.	2	2
5. Дослідження блоку функційного перетворення у криптосистемі DES.	2	
6. Дослідження методів багатофакторної автентифікації.	2	
7. Інтеграція інтелектуального відеоспостереження в системи безпеки.	2	
8. Дослідження режимів роботи стандарту шифрування AES.	2	
9. Дослідження протоколу безпеки TLS.	2	
10. Сумісне використання стеганографічного та криптографічного захисту.	2	2
Всього	**20**	**4**

6. ЛАБОРАТОРНІ РОБОТИ

Назва теми	Кількість годин	
	Денна форма	Заочна форма
1. Дослідження шифру простої заміни Цезаря.	2	2
2. Дослідження біграмного шифру Плейфера.	2	
3. Моделювання процесів шифрування за допомогою операції XOR	2	
4. Дослідження алгоритму DES.	2	
5. Дослідження стандарту шифрування AES.	2	
Всього	**10**	**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

№ з/п	Назва теми	Кількість годин	
		денна форма	заочна форма
1	Тема 1. Основи інформаційної безпеки в інфокомунікаційних системах. Поняття інформаційної безпеки у інфокомунікаційних системах. Ключові принципи захисту: конфіденційність, цілісність, доступність. Типові загрози та вразливості у мережах зв'язку.	12	18
2	Тема 2. Криптографічні механізми захисту інформації. Основні поняття криптографічного захисту. Симетричні та асиметричні алгоритми шифрування (DES, AES, RSA, Ель Гамаля). Розподілення ключів(Метод Діффі-Геллмана). Сучасні стандарти шифрування на базі SP-мереж та вітчизняні стандарти (ДСТУ «Калина»).	12	20
3	Тема 3. Системи ідентифікації, автентифікації та електронний підпис. Методи автентифікації користувачів і пристроїв. Біометричні та багатофакторні методи. Процедури створення та перевірки електронного цифрового підпису.	14	20
4	Тема 4. Протоколи безпеки мережевих комунікацій. Призначення протоколів безпеки (SSL/TLS, IPsec, SSH, HTTPS, Kerberos). Захист даних під час передачі мережевими каналами та організація віртуальних приватних мереж.	14	20
5	Тема 5. Технічний захист мережевої інфраструктури. Загрози та методи захисту мережевої інфраструктури. Використання засобів виявлення	14	20

	та запобігання вторгненням (IDS/IPS) на технічному рівні. Сегментація мережі та контроль доступу.		
6	Тема 6. Безпека бездротових і мобільних мереж. Типові загрози бездротових мереж (перехоплення трафіку, MITM, підроблені точки доступу). Методи захисту Wi-Fi мереж (WPA2/WPA3) та безпека мобільних додатків.	14	20
7	Тема 7. Стеганографія та комплексні технічні системи захисту. Основні вимоги до побудови систем приховування факту передачі інформації. Сумісне використання стеганографічного та криптографічного захисту. Технічні засоби захисту від витоку інформації.	14	20
	Всього	**94**	**138**

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 інформаційної безпеки та назвіть її основні складові.
2. Які існують типи загроз інформаційним системам?
3. Поясніть різницю між вразливістю та атакою.
4. Що таке шифрування, розшифрування та дешифрування?
5. Симетричні та асиметричні алгоритми шифрування.
6. Приклади класичних методів шифрування.
7. Які є методи ідентифікації користувачів?
8. Поясніть відмінності між однофакторною та багатофакторною автентифікацією.
9. Що таке електронний підпис ?
10. Які засоби використовуються для автентифікації?
11. Які основні функції протоколів SSL/TLS?
12. Що таке VPN та IPSec, і для чого вони застосовуються?
13. Наведіть приклади використання захищених протоколів у повсякденних сервісах.
14. Що таке мережева інфраструктура та які її основні елементи?
15. Які функції виконують міжмережеві екрани?
16. Як відеоспостереження може бути елементом системи захисту інформації?
17. Назвіть принципи побудови комплексних систем захисту інформації (КСЗІ).
18. Які є властивості інформації, що захищається?
19. Що таке політика безпеки та які її основні складові?
20. Які ролі та обов’язки мають адміністратор безпеки, користувачі та аудитори?

21. Які вимоги до КСЗІ встановлюють стандарти ISO/IEC 27001 та ДСТУ?
22. Що таке стеганографія та приховані канали передачі інформації?
23. Дати поняття конфіденційності, цілісності та доступності інформації?
24. Які переваги та недоліки біометричних систем автентифікації?
25. Яким чином захищається властивість інформації конфіденційність?
26. Яким чином захищається властивість інформації цілісність?
27. Що може бути ключем в шифрах перестановки?
28. Що може бути ключем в шифрах заміни?
29. В чому суть метода гамування?
30. Від чого залежить довжина гами шифру?

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» А - 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

<table>
<tr><th rowspan="2">100-бальною шкалою</th><th rowspan="2">Шкала за ECTS</th><th colspan="2">За національною шкалою</th></tr>
<tr><th>екзамен</th><th>залік</th></tr>
<tr><td>90-100</td><td>A</td><td>Відмінно</td><td rowspan="5">Зараховано</td></tr>
<tr><td>82-89</td><td>B</td><td rowspan="2">Добре</td></tr>
<tr><td>74-81</td><td>C</td></tr>
<tr><td>64-73</td><td>D</td><td rowspan="2">Задовільно</td></tr>
<tr><td>60-63</td><td>E</td></tr>
<tr><td>35-59</td><td>FX</td><td rowspan="2">Незадовільно</td><td rowspan="2">Не зараховано</td></tr>
<tr><td>1-34</td><td>F</td></tr>
</table>

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