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 ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

Галузь знань 17 «Електроніка, автоматизація та електронні комунікації»

Спеціальність 172 « Електронні комунікації та радіотехніка»

Назва освітньої програми Комп'ютерні мережі та Інтернет

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**
Доцент кафедри комп'ютерної інженерії та інноваційних технологій, кандидат технічних наук, доцент **Йона Лариса Григорівна**	0677463777	Yonalarisa66@gmail.com

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

Гарант освітньої програми к.т.н., доцент, _____ Денис РОЗЕНВАССЕР

Узгоджено
Начальник навчального відділу _____ Лілія САЄНКО

ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, напрям підготовки, освітньо-кваліфікаційний рівень</td><td colspan="2">Характеристика навчальної дисципліни</td></tr>
<tr><td>денна форма навчання</td><td>заочна форма навчання</td></tr>
<tr><td rowspan="6">Кількість кредитів – 4, загальна кількість годин – 120</td><td rowspan="6">Галузь 17 «Електроніка, автоматизація та електронні комунікації»

Спеціальність – 172 « Електронні комунікації та радіотехніка»</td><td colspan="2">обов’язкова</td></tr>
<tr><td colspan="2">Рік підготовки:</td></tr>
<tr><td colspan="2">3-й</td></tr>
<tr><td colspan="2">Семестр</td></tr>
<tr><td>6-й</td><td>6-й</td></tr>
<tr><td rowspan="12">Мова навчання – українська</td><td rowspan="12">Рівень вищої освіти – перший (бакалаврський) рівень</td><td colspan="2">Лекції</td></tr>
<tr><td>26 год.</td><td>8 год.</td></tr>
<tr><td colspan="2">Практичні, семінарські</td></tr>
<tr><td>26 год.</td><td>8 год.</td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>год.</td><td>год.</td></tr>
<tr><td colspan="2">Самостійна робота та індивідуальні завдання</td></tr>
<tr><td>68 год.</td><td>104 год.</td></tr>
<tr><td colspan="2">Вид контролю:</td></tr>
<tr><td>залік</td><td>залік</td></tr>
</table>

Захист інформації в телекомунікаційних системах є складовою частиною навчального процесу у підготовці фахівців зі спеціальності 172 «Електронні комунікації та радіотехніка», а також обов’язковим компонентом освітньої програми для здобуття освітнього рівня «бакалавр» та має на меті формування у здобувачів уявлення про принципи захисту інформації від порушення її конфіденційності, цілісності та доступності; розгляд концепції криптографічного захисту інформації, зокрема методів шифрування, автентифікації, керування криптографічними ключами та стеганографічного захисту.

Метою викладання навчальної дисципліни «Захист інформації в телекомунікаційних системах» є забезпечення здобувачів знаннями з питань принципів побудови криптографічних систем та проблем захисту інформації у системах комунікацій від порушення її конфіденційності, цілісності та доступності з урахуванням сучасного стану та перспективних напрямів розвитку криптографії та стеганографії.

ПРЕРЕКВІЗИТИ: знання і вміння, отримані студентом при вивченні навчальних дисциплін бакалаврської підготовки. Дисципліна базується на основних положеннях дисциплін*:* Вища математика; Теорія інформації та кодування;Телекомунікаційні системи та мережі.

ПОСТРЕКВІЗИТИ: знання і вміння, отримані здобувачем при вивченні ОК «Захист інформації в телекомунікаційних системах» є передумовою для вивчення дисципліни «Проєктування інформаційно-комунікаційних систем», виконання переддипломної практики та підготовки кваліфікаційної роботи.

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

У процесі реалізації програми дисципліни «Захист інформації в телекомунікаційних системах» формуються наступні компетентності із передбачених освітньо-професійною програмою «Комп'ютерні мережі та Інтернет» зі спеціальності 172 Електронні комунікації та радіотехніка.

Інтегральна компетентність

ІК-1. Здатність розв'язувати спеціалізовані задачі та практичні проблеми у галузі телекомунікацій та радіотехніки, що характеризуються комплексністю та невизначеністю умов.

Загальні компетентності

ЗК-1. Здатність до абстрактного мислення, аналізу та синтезу.

ЗК-8. Вміння виявляти, ставити та вирішувати проблеми.

Спеціальні (фахові) компетентності

ПК-1. Здатність розуміти сутність і значення інформації в розвитку сучасного інформаційного суспільства.

ПК-2. Здатність вирішувати стандартні завдання професійної діяльності на основі інформаційної та бібліографічної культури із застосуванням інформаційно-комунікаційних технологій і з урахуванням основних вимог інформаційної безпеки.

ПК-5. Здатність використовувати нормативну та правову документацію, що стосується інформаційно-телекомунікаційних мереж, телекомунікаційних та радіотехнічних систем (закони України, технічні регламенти, міжнародні та національні стандарти, рекомендації Міжнародного союзу електрозв'язку і т.п.) для вирішення професійних завдань.

Програмні результати навчання

ПРН 8. Вміння застосовувати сучасні досягнення у галузі професійної діяльності з метою побудови перспективних телекомунікаційних систем, інфокомунікаційних, телекомунікаційних мереж, радіотехнічних систем та систем телевізійного й радіомовлення тощо.

ПРН 10. Здатність проводити випробування телекомунікаційних систем, інфокомунікаційних, телекомунікаційних мереж, радіотехнічних систем та систем телевізійного й радіомовлення у відповідності до технічних регламентів та інших

нормативних документів.

Заплановані результати навчання за навчальною дисципліною

У результаті вивчення цієї навчальної дисципліни здобувач має набути такі компетентності.

Знати:

- загрози та ризики витоку конфіденційної інформації для забезпечення захисту інформації в телекомунікаціях;
- методи захисту конфіденційної інформації;
- сучасні тенденції в галузі захисту інформації в телекомунікаціях;
- засоби захисту від несанкціонованого доступу до конфіденційної інформації;
- знати: основні етапи створення систем захисту інформації,
- принципи побудови симетричних та асиметричних криптографічних систем,
- концепцію криптосистем з відкритим ключем,
- керування криптографічними ключами,
- методи ідентифікації та автентифікації в телекомунікаційних системах
- основи стеганографічного захисту інформації.

Вміти:

- аналізувати загрози та джерела загроз для телекомунікаційних систем,
- використовувати основні методи захисту конфіденційної інформації;
- враховувати засоби одержання несанкціонованого доступу до конфіденційної інформації;
- виконувати розрахунки необхідних параметрів алгоритмів шифрування, розподілення ключів та цифрового підпису

3. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Тема 1. Актуальність проблеми захисту інформації в сучасних системах телекомунікації. Аналіз погроз інформації при передачі по каналах зв'язку. Методи захисту інформації в каналах зв'зку.

Тема 2. Основи архітектури систем захисту інформації. Принципи побудови систем захисту інформації. Класичні методи шифрування. Схема побудови складного шифру.

Тема 3. Алгоритми шифрування на базі мережі Фейстеля. Дослідження алгоритму шифрування DES. Методи підвищення криптостійкості системи. Алгоритм 3-DES. Особливості побудови криптосистеми IDEA.

Тема 4. Сучасні стандарти шифрування, що побудовані на SP-мережі. Схема SP-мережі. Реалізація SP-мережі в криптосистемах AES та ДСТУ 7624:2014 «Калина». Вимоги до побудови криптосистем. Режими роботи та функціональні перетворення.

Тема 5. Порівняльний аналіз симетричних криптосистем. Порівняння симетричних криптосистем за основними параметрами щодо криптостійкості.

Тема 6. Основи стеганографічного захисту інформації. Основні вимоги до побудови систем приховування факту передачі інформації. Класифікація стегосистем. Основні характеристики класичної, комп'ютерної та цифрової стеганографії.

Тема 7. Сумісне використання стеганографічного та криптографічного захисту інформації в телекомунікаційних системах. Проектування схеми системи криптографічного та стеганографічного захисту інформації.

Тема 8. Принципи керування ключовою системою. Ключова система, генерування та розподілення ключів.

Тема 9. Асиметричні алгоритми шифрування. Особливості побудови систем з відкритим ключем.

Тема 10. Принципи керування ключовою системою. Генерування, накопичування. та розподілення ключів Метод генерування та розподілення ключів Діффі-Хеллмана.

Тема 11. Криптосистема Ель Гамаля. Процедури шифрування в криптосистемі Ель–Гамаля.

Тема 12. Алгоритм шифрування в криптосистемі RSA. Процедури генерування асиметричної пари ключів та система шифрування RSA.

Тема 13. Системи ідентифікації та автентифікації. Прості методи автентифікації за паролем. Біометричні методи автентифікації. Біометрико-криптографічні перетворення при підтвердженні справжності користувача. Багатофакторна автентифікація.

Тема 14. Методи побудови схем електронного підпису. Процедура створення підпису в алгоритмі RSA. Різновиди ЕП.

4. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Назви змістових модулів і тем	Кількість годин							
	денна форма				Заочна форма			
	усього	у тому числі			усього	у тому числі		
		лекц.	практ.	сам. роб.		лекц.	прак	сам. роб.
Тема 1 Актуальність проблеми захисту інформації в сучасних системах телекомунікації.	8	2	2	4	8	2		6
Тема 2. Основи архітектури систем захисту інформації.	8	2	2	4	8		2	6
Тема 3. Алгоритми шифрування на базі мережі Фейстеля.	8	2	2	4	8			8
Тема 4. Сучасні стандарти шифрування, що побудовані на SP-мережі.	8	2	2	4	8			8
Тема 5. Порівняльний аналіз симетричних криптосистем.	8	2	2	4	8			8
Тема 6. Основи стеганографічного захисту інформації.	8	2	2	4	8	2		6
Тема 7. Сумісне використання стеганографічного та криптографічного захисту інформації в телекомунікаційних системах.	8	2	2	4	8		2	6
Тема 8. Принципи керування ключовою системою.	8	2	2	4	8	2		6
Тема 9. Асиметричні алгоритми шифрування.	8	2	2	4	8		2	6
Тема 10. Дослідження розподілу асиметричних криптосистем за призначенням	8	2	2	4	8			8
Тема 11. Криптосистема Ель Гамаля.	10		2	8	10			10
Тема 12. Алгоритм шифрування в криптосистемі RSA.	10	2	2	6	10		2	8
Тема 13. Системи ідентифікації та автентифікації.	10	2	2	6	10	2		8
Тема 14. Методи побудови схем електронного підпису.	10	2		8	10			10
Усього годин	**120**	**26**	**26**	**68**	**120**	**8**	**8**	**104**
ПІДСУМКОВИЙ КОНТРОЛЬ – залік								

5. ПРАКТИЧНІ ЗАНЯТТЯ

№ з/п	Назва теми	Кількість годин	
		Денна форма	Заочна форма
1	Модулярні обчислення в криптографічних перетвореннях.	4	2

2	Шифрування за допомогою шифрів перестановки.	4	
3	Шифрування за допомогою шифрів заміни.	4	2
4	Принципи побудови криптографічних систем.	4	
5	Дослідження стеганографічних методів захисту.	4	2
6	Дослідження методу генерації та розподілення ключів Діффі і Хеллмана.	4	2
7	Генерування та перевірка електронного підпису RSA.	2	
	Всього	26	8

6. САМОСТІЙНА РОБОТА

До самостійної роботи студентів щодо вивчення дисципліни «**Інформаційна безпека інноваційної діяльності»** включаються наступні тематики завдання.

Тематика та питання до самостійної підготовки та індивідуальних завдань

№ з/п	Назва теми	Кількість годин	
		денна форма	заочна форма
1	**Тема 1.** Вивчення Положення закону «Про національну безпеку України»	4	6
2	**Тема 2.** основні методи захисту в комунікаціях.	4	6
3	**Тема 3.** Дослідження класичних шифрів. Принцип рівноміцного захисту.	4	8
4	**Тема 4.** Принципи побудови SP-мережі.	4	8
5	**Тема 5.** Дослідження порівняльних характеристик сучасних криптосистем, що використовуються для захисту конфіденційної інформації**.**	4	8
6	**Тема 6.** Дослідження стеганографічних методів захисту інформації.	4	6
7	**Тема 7.** Побудова схеми сумісного використання криптографічних та стеганографічних методів захисту інформації.	4	6
8	**Тема 8.** Обчислення спільного ключа методом Діффі і Хеллмана.	4	6
9	**Тема 9.** Односпрямовані функції. Використання геш-функцій в асиметричних системах.	4	6
10	**Тема 10.** Класифікація асиметричних криптосистем за призначенням.	4	8
11	**Тема 11.** Шифрування за алгоритмом Ель Гамаля.	8	10
12	**Тема 12.** Шифрування за алгоритмом RSA.	6	8

13	**Тема 13.** Дослідження методів ідентифікації та автентифікації користувача.	6	8
14	**Тема 14.** Дослідження методів автентифікації документу за допомогою електронного підпису.	8	10
	Всього	**68**	**104**

7. ВИДИ ТА МЕТОДИ КОНТРОЛЮ

Робоча програма навчальної дисципліни передбачає наступні види та методи контролю:

Види контролю	Складові оцінювання
поточний контроль, який здійснюється у ході: проведення практичних занять, виконання самостійної роботи, індивідуальних завдань, дослідна робота здобувача тощо.	100%

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

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

(поточний контроль, підсумковий контроль, загальний результат оцінювання)

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[1], перевірка конспектів навчальних текстів тощо	**20**

[1] Індивідуально-консультативна робота викладача зі здобувачами

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 здобувача мають фрагментарний, поверховий характер;
- «4» - оцінюється правильна і обґрунтована відповідь (письмова робота), з якої видно, що здобувач 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 екзамену / заліку)

Рівень знань оцінюється:

- «відмінно» / «зараховано» А - від 90 до 100 балів. Здобувач виявляє особливі творчі здібності, вміє самостійно знаходити та опрацьовувати необхідну інформацію, демонструє знання матеріалу,

проводить узагальнення і висновки. Був присутній на лекціях та 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. Здобувач володіє знаннями матеріалу, але допускає незначні помилки у формуванні термінів, категорій, проте за допомогою викладача швидко орієнтується і знаходить правильні відповіді. Був присутній на лекціях та 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. Здобувач відтворює значну частину теоретичного матеріалу, виявляє знання і розуміння основних положень, з допомогою викладача може аналізувати навчальний матеріал, але дає недостатньо обґрунтовані, невичерпні відповіді, допускає помилки. При цьому враховується наявність конспекту з виконаними завданнями до самостійної роботи, реферату та активність у науково-дослідній роботі;
- «задовільно» / «зараховано» D - від 64 до 73 балів. Здобувач 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. Здобувач 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. Здобувач володіє матеріалом на рівні окремих фрагментів, що становлять незначну частину навчального матеріалу.
- «незадовільно з обов'язковим повторним вивченням дисципліни» / «не зараховано» F – від 1 до 34 балів. Здобувач не володіє навчальним матеріалом.

Таблиця відповідності результатів контролю знань за різними шкалами

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

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.

13. Сучасні криптографічні системи. Навчальний посібник. С.М. Горохов, Л.Г. Йона, О.В. Онацький, під керівництвом проф. М.В. Захарченка Одеса: ВЦ ОНАЗ ім. О.С. Попова, 2007. – 152 с.

14. Асиметричні методи шифрування: Навч. посіб. / Онацький О.В., Йона Л.Г., Шинкарчук Т.М.; за ред. М. В. Захарченка. – Одеса: ОНАЗ ім. О. С. Попова, 2010. – 164 с.

Інформаційні ресурси

15. 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

16. Національна бібліотека України ім. В.І. Вернадського. URL: http://www.nbuv.gov.ua.

17. Портал кіберполіції України. URL: https://cyberpolice.gov.ua/