

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ  
ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ  
ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ЗАТВЕРДЖУЮ

В.о. декана факультету комп'ютерних  
інформаційних технологій

Ігор ЯКИМЕНКО

“ ” 2023 р.

ЗАТВЕРДЖУЮ

В.о. проректора з науково-педагогічної  
роботи

Віктор ОСТРОВЕРХОВ

“ ” 2023 р.

ЗАТВЕРДЖУЮ

Директор навчально-наукового  
інституту новітніх освітніх  
технологій

Святослав ПИТЕЛЬ

“ ” 2023 р.

**РОБОЧА ПРОГРАМА**

з дисципліни «Захист інформації в комп'ютерних системах і мережах»

*ступінь вищої освіти – бакалавр*

галузь знань – 12 “Інформаційні технології”

спеціальність – 123 “Комп'ютерна інженерія”

освітньо-професійна програма – „Комп'ютерна інженерія”

Кафедра комп'ютерної інженерії

Форма навчання	Курс	Семестр	Лекції (год.)	Лабораторні (год.)	ІРС (год.)	Тренінг (год.), КПЗ	Самост. робота студ. (год.)	Разом (год.)	Залік сем.)	Екз. (сем.)
Денна	3	6	42	56	6	14	92	210	-	6
Заочна	3	6	8	4	-	-	198	210	-	6

Тернопіль – ЗУНУ

2023

31.08.2023  
Чай

Робоча програма складена на основі освітньо – професійної програми підготовки бакалавра галузі знань 12 “Інформаційні технології” напрямку підготовки 123 “Комп’ютерна інженерія”, затвердженої Вченою радою ЗУНУ (протокол № 9 від 26 травня 2021 р.).

Робочу програму склала к.т.н., доцент, зав.кафедри КІ

Леся ДУБЧАК

Робоча програма затверджена на засіданні кафедри комп’ютерної інженерії, протокол №1 від 28 серпня 2023 р.

Завідувач кафедри



---

Леся ДУБЧАК

Розглянуто та схвалено групою забезпечення спеціальності «Комп’ютерна інженерія», протокол №1 від 28 серпня 2023 р.

Голова ГЗС



---

Олег БЕРЕЗЬКИЙ

Гарант ОП «Комп’ютерна інженерія»



---

Леся ДУБЧАК

**СТРУКТУРА РОБОЧОЇ ПРОГРАМИ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ  
"ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ І МЕРЕЖАХ"**

**1. Опис дисципліни "Захист інформації в комп'ютерних системах і мережах"**

<b>Дисципліна – «Захист інформації в комп'ютерних системах»</b>	<b>Галузь знань, спеціальність, СВО</b>	<b>Характеристика навчальної дисципліни</b>
Кількість кредитів – 7	галузь знань – 12 „Інформаційні технології”	Статус дисципліни – обов’язкова Мова навчання – українська
Кількість залікових модулів: 4	Спеціальність – 123 „Комп’ютерна інженерія”	Рік підготовки: <i>Денна</i> - 3, <i>Заочна</i> – 3 Семестр: <i>Денна</i> – 6 <i>Заочна</i> – 6
Кількість змістових модулів – 4	Ступінь вищої освіти - бакалавр	Лекції: <i>Денна</i> - 42 год., <i>Заочна</i> – 8 год. Лабораторні заняття: <i>Денна</i> - 56 год. <i>Заочна</i> – 4 год.
Загальна кількість годин – <i>Денна</i> – 210 год., <i>Заочна</i> - 210 год.		Самостійна робота: <i>Денна</i> – 92 год. <i>Заочна</i> – 198 год. Тренінг, КПЗ – 14 год. Індивідуальна робота: <i>Денна</i> – 6 год.
Тижневих годин: <i>Денна</i> : 6 семестр: 14 год., з них аудиторних – 6,5 год.		Вид підсумкового контролю <i>Денна</i> : 6 семестр – екзамен <i>Заочна</i> : 6 семестр – екзамен

## **2. Мета й завдання вивчення дисципліни "Захист інформації в комп'ютерних системах і мережах"**

### **2.1. Мета вивчення дисципліни**

Програма та тематичний план дисципліни орієнтовані на отримання студентами навиків та знань щодо захисту інформації.

Студенти вивчають основи використання прикладного програмного забезпечення, яке використовується при захисті інформації, включаючи ознайомлення з вірусами та антивірусними програмами, методи ідентифікації та аутентифікації особи.

### **2.2 Завдання вивчення дисципліни**

Завдання курсу полягає в ознайомленні студентів з основами побудови та використання систем захисту інформації в комп'ютерних системах, а також прищеплення практичних навиків роботи з існуючими сучасними системами захисту інформації, зокрема, криптографічними.

### **2.3. Найменування та опис компетентностей, формування котрих забезпечує вивчення дисципліни:**

K11. Здатність застосовувати законодавчу та нормативно- правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі комп'ютерної інженерії.

K14. Здатність забезпечувати захист інформації, що обробляється в комп'ютерних та кіберфізичних системах та мережах з метою реалізації встановленої політики інформаційної безпеки.

K20. Здатність здійснювати організацію робочих місць, їхнє технічне оснащення, розміщення комп'ютерного устаткування, використання організаційних, технічних, алгоритмічних та інших методів і засобів захисту інформації.

### **2.4 Передумови для вивчення дисципліни**

Зазначена дисципліна включена до циклу дисциплін професійної підготовки за переліком програми. У структурно-логічній схемі навчання зазначена дисципліна розміщена на IV-му курсі. Вивчення курсу "Захист інформації в комп'ютерних системах і мережах" передбачає наявність систематичних та ґрунтовних знань із дисциплін «Комп'ютерні системи», «Системи обробки розподілених баз даних», «Паралельні та розподілені комп'ютерні системи», цілеспрямованої роботи над вивченням спеціальної

літератури, активної роботи на лекціях та практичних заняттях, самостійної роботи.

## **2.5. Результати навчання.**

В результаті вивчення дисципліни студенти повинні:

ПРН1. Знати і розуміти наукові положення, що лежать в основі функціонування комп'ютерних засобів, систем та мереж.

ПРН4. Знати та розуміти вплив технічних рішень в суспільному, економічному, соціальному і екологічному контексті.

ПРН6. Вміти застосовувати знання для ідентифікації, формулювання і розв'язування технічних задач спеціальності, використовуючи методи, що є найбільш придатними для досягнення поставлених цілей.

ПРН9. Вміти застосовувати знання технічних характеристик, конструктивних особливостей, призначення і правил експлуатації програмно-технічних засобів комп'ютерних систем та мереж для вирішення технічних задач спеціальності.

## **3. Програма навчальної дисципліни**

### **"Захист інформації в комп'ютерних системах і мережах"**

#### **Змістовий модуль 1. Основи систем захисту інформації у КС Тема**

##### **1. Вступ. Поняття захисту інформації.**

Інформаційна безпека комп'ютерних систем. Вразливість комп'ютерних систем. Канали витоку інформації, атака та вторгнення в КС. Класифікація загроз безпеці інформації та інформаційним системам. Перехват, переривання. Модифікація та фальсифікація. Радіотехнічне, організаційне, комунікаційне, програмно-технічне.

Література: 1-3.

**Тема 2.** Політика безпеки інформації. Законодавча база захисту інформації в Україні.

Політика безпеки. Нормативно-правове та організаційне забезпечення безпеки. Комунікаційно-технічне забезпечення. Програмне забезпечення. Література: 2, 6, 8, 11.

#### **Змістовий модуль 2. Управління доступом та розмежування прав доступу до інформації**

**Тема 3.** Зміст етапів ідентифікації, авторизації та автентифікації користувачів.

Етапи ідентифікації, авторизації та автентифікації користувачів Прості паролі. Способи формування та реєстрації паролів. «Слабкі» паролі. Характеристики парольного захисту.

Література: 1, 2, 12.

**Тема 4.** Модифікації системи паролів. Механізми розширення прав доступу.

Паролі одноразові, ідентифікатори, секретні функції, процедури «рукостискання». Списки доступу, мандатні списки. Механізми розширення прав доступу. Принцип мінімальних привілей.

Література: 1-3.

**Змістовий модуль 3. Атаки на системи захисту інформації та методи захисту від них.**

**Тема 5.** Основні типи атак та методи захисту від них.

Модель системи захисту Adept-50. Типи об'єктів та категорій. Модель простору безпеки Хартсона. Домени повноважень користувачів.

Література: 2, 5, 13, 14.

**Тема 6.** Канали витоку інформації. Сучасні атаки на реалізацію та відповідні методи протидії.

Модель системи захисту Бела і Лападули. Матриця прав доступу. Потіки запитів суб'єктів до об'єктів. Модель моніторингу безпеки. Лічильники небезпечних подій. Вектор індикації аномалій в діях користувачів.

Література: 2, 17.

**Змістовий модуль 4. Захист інформації в комп'ютерних системах.**

**Тема 7.** Найпростіші шифри.

Перестановки та підстановки. Шифри «Скітала», Полібія, Цезаря. Шифри Плейфера, Уїтстона. Шифрувальні таблиці. Роторні машини. Маскування. Шифр Вернама.

Література: 1, 3, 12, 14.

**Тема 8.** Симетричні криптоалгоритми.

Система Люцифер. Стандарт DES. Функція шифрування та управління ключами. Режими ECB,CBC,OFB,CFB.

Література: 1, 6, 9, 12.

**Тема 9.** Асиметричні криптоалгоритми.

Алгоритм асиметричного шифрування інформації. Алгоритм Діффі-Хелмана. Алгоритм Ель-Гамаля.

Література: 1, 6, 12.

**Тема 10.** Електронний цифровий підпис.

Blowfish, RC-5, CAST-128. Хеш-згортка повідомлень. Алгоритми MD-5, SHA, ГОСТ 34.11-94.

Література: 4, 12.

**Змістовий модуль 5. Захист інформації в комп'ютерних мережах.**

**Тема 11.** Захист інформації в комп'ютерних та Wi-Fi мережах. Захист мобільного зв'язку.

Особливості Wi-Fi мереж. Основні атаки в Wi-Fi мережах та методи захисту від них. Захист мобільного зв'язку.

Література: 6, 7, 14.

**Тема 12.** Internet-банкінг, POS-термінали, банкомати. Методи захисту фінансових даних.

Поняття інтернет-банкінгу. Апаратні засоби здійснення платежів та методи їх захисту. Захист особистих фінансових даних.

Література: 4, 12.

#### 4. Структура залікового кредиту дисципліни "Захист інформації в комп'ютерних системах мережах"

(денна форма навчання)

	Кількість годин					
	Лекції	Лабораторні заняття	Самостійна робота	Індивідуальна робота	Тренінг, КПЗ	Контрольні заходи
<b>Змістовий модуль 1</b>						
Тема 1. Вступ. Поняття захисту інформації.	2	4	6		2	опитування
Тема 2. Політика безпеки інформації. Законодавча база захисту інформації в Україні	2	6	8			опитування

<b>Змістовий модуль 2</b>						
Тема 3. Зміст етапів ідентифікації, авторизації та автентифікації користувачів..	2	4	8		2	опитування
Тема 4. Модифікації системи паролів. Механізми розширення прав доступу.	2	6	8			опитування
<b>Змістовий модуль 3</b>						
Тема 5. Основні типи атак та методи захисту від них	2	4	8	1	6	опитування
Тема 6. Канали витоку інформації. Сучасні атаки на реалізацію та відповідні методи протидії.	4	4	8	1		опитування
Тема 7. Захист інформації в комп'ютерних системах..	4	6	8	1		опитування
Тема 8. Симетричні криптоалгоритми.	4	6	8			опитування
Тема 9. Асиметричні криптоалгоритми.	4	4	8			опитування
Тема 10. Електронний цифровий підпис.	4	6	6	1		опитування
<b>Змістовий модуль 4</b>						
Тема 11. Захист інформації в комп'ютерних та Wi-Fi мережах. Захист мобільного зв'язку.	4		6	1	4	опитування



Тема 12. Internet-банкінг, POS-термінали, банкомати. Методи захисту фінансових даних.	8	6	12	1		опитування
<b>Разом</b>	<b>42</b>	<b>56</b>	<b>92</b>	<b>6</b>	<b>14</b>	

**(заочна форма навчання)**

	Кількість годин			
	Лекції	Лабораторні заняття	Самостійна робота	Індивідуальна робота

**Змістовий модуль 1**

Тема 1. Вступ. Поняття захисту інформації.			12	
Тема 2. Політика безпеки інформації. Законодавча база захисту інформації в Україні	1	1	12	

**Змістовий модуль 2**

Тема 3. Зміст етапів ідентифікації, авторизації та автентифікації користувачів..		1	12	
Тема 4. Модифікації системи паролів. Механізми розширення прав доступу.	1		12	

**Змістовий модуль 3**

Тема 5. Основні типи атак та методи захисту від них	1		12	
Тема 6. Канали витоку інформації.			12	

Тема 7. Захист інформації в комп'ютерних системах..	1		12	
Тема 8. Симетричні криптоалгоритми.	1	1	12	
Тема 9. Асиметричні криптоалгоритми.	1	1	22	
Тема 10. Електронний цифровий підпис.	1		22	
<b>Змістовий модуль 4</b>				
Тема 11. Захист інформації в комп'ютерних та Wi-Fi мережах. Захист мобільного зв'язку.	1		29	
Тема 12. Internet-банкінг, POS-термінали, банкомати. Методи захисту фінансових даних.			29	
<b>Разом</b>	<b>8</b>	<b>4</b>	<b>198</b>	

## 5. Тематика лабораторних занять

### Лабораторна робота №1.

**Тема:** Шифрування файлів та папок засобами Secure IT.

**Мета:** Вивчити засіб захисту інформації Secure IT.

Питання для обговорення:

1. Методи шифрування
2. Парольний захист.
3. Процедура дешифрування.

Література: 4, 9, 12.

### Лабораторна робота №2.

**Тема:** Захист текстових документів в Microsoft Word.

**Мета:** Навчитися захищати документ засобами Microsoft Word.

Питання для обговорення:

1. Методи захисту.
2. Простий пароль.
3. Модифікація прав доступу.

Література: 2, 13.

### **Лабораторна робота №3.**

**Тема:** Захист інформації засобами ОС Windows.

**Мета:** Навчитися захищати інформацію засобами ОС Windows.

Питання для обговорення: 1.

Технологія BitLocker.

2. Технологія AppLocker.

3. Батьківський контроль.

Література: 2, 5, 13.

### **Лабораторна робота №4.**

**Тема:** Захист інформації за допомогою антивірусних програм.

**Мета:** Вивчити можливості сучасних антивірусних програм.

Питання для обговорення:

1. Антивірусні програми.

2. Функції мережевого екрана.

3. Журнал активності.

Література: 14, 17.

### **Лабораторна робота №5.**

**Тема:** Розробка та дослідження засобів ідентифікації користувачів в комп'ютерних системах.

**Мета:** Навчитися здійснювати ідентифікацію користувачів комп'ютерних систем.

Питання для обговорення:

1. Процедура ідентифікації.

2. Методи ідентифікації.

3. Рівні захисту КС.

Література: 9, 13-15.

### **Лабораторна робота №6.**

**Тема:** Розробка та дослідження засобів аутентифікації користувачів в комп'ютерних системах.

**Мета:** Навчитися здійснювати аутентифікацію користувачів комп'ютерних систем.

Питання для обговорення:

1. Процедура аутентифікації.
2. Методи аутентифікації.
3. Процедура авторизації.

Література: 9, 13-15.

### **6. Комплексне практичне індивідуальне завдання**

Варіанти КПЗ з дисципліни "Захист інформації в комп'ютерних системах":

1. Зашифрувати шифром одноразового блокноту фразу «акції продано» ключем 10010 00111 11100 01001 10100 00000 00001 01101 01111 01100 01111 00001.
2. Зашифрувати шифром одноразового блокноту фразу «система нестійка» ключем 11100 00101 10011 00111 11110 00011 01010 00001 10101 01111 01100 01111 00001 10101 010101.
3. Розшифрувати криптотекст 010011 001100 110010 000101 101101 011001 111100 011010 000010 010100 000111 000011 000001 011110 011100 010011 за допомогою ключа 000000 011000 111000 001010 100110 001111 111100 000101 010100 000000 000001 010101 011111 001100 011111 000001.
4. Розшифрувати криптотекст 011111 011101 101001 010010 010100 000111 010001 111110 100111 101010 за допомогою ключа 010000 001111 111111 000001 000000 010101 010100 111110 110110 111000.
5. Здійснити шифрування фрази «Повідомлення доставлено» за алгоритмом DES.
6. Здійснити шифрування фрази «Повідомлення доставлено» за алгоритмом RC5.
7. Здійснити шифрування фрази «Повідомлення доставлено» за алгоритмом RSA.
8. Здійснити шифрування фрази «Повідомлення доставлено» за алгоритмом Ель-Гамала.
9. Здійснити шифрування фрази «Повідомлення доставлено» за алгоритмом Геффе.
10. Розробити систему захисту інформації магазину.
11. Розробити систему захисту інформації школи.
12. Розробити систему захисту інформації великої корпорації.
13. Описати алгоритм роботи та сфери застосування токєрів.
14. Описати алгоритм роботи та сфери застосування сучасних програмних засобів захисту інформації.

15. Дослідити базу та можливості антивірусної програми 16. Дослідити базу та можливості існуючого фаєрвола.
17. Дослідити можливості захисту інформації сучасних операційних систем.
18. Шлюзи мережевого рівня.
19. Шлюзи прикладного рівня.
20. Основні схеми мережевого захисту на базі міжмережевих екранів.
21. Схема мережевий екран – фільтруючий маршрутизатор.
22. Мережевий екран на базі двопортового шлюза.
23. Схема мережевого екрану на базі екранованого шлюза.
24. Основні алгоритми програмних методів захисту.
25. Системи Firewall.
26. Універсальна електронна платіжна система UEPS.
27. Особливості функціонування протоколу SET.
28. Технологічні рішення для захисту платежів під час електронної торгівлі.
29. Проблеми захисту інформації в комп'ютерних мережах.
30. Види атак на захищену інформаційну систему.
31. Апаратно–програмні засоби захисту інформації.
32. Принципи проектування ефективної системи захисту інформації.

## 7. Самостійна робота студентів

(денна форма навчання)

№ п/п	Тематика
1	Законодавчі аспекти захисту інформації.
2	Основні загрози безпеки інформації. Забезпечення безпеки інформації в комп'ютерних системах і мережах.
3	Проблема ідентифікації користувача та механізми підтвердження його істинності.
4	Основні поняття і концепції ідентифікації та електронного цифрового підпису.
5	Проблема ідентифікації користувача та механізми підтвердження його істинності.
6	Основні поняття і концепції ідентифікації та електронного цифрового підпису.
7	Взаємна перевірка істинності користувачів.

8	Біометрична ідентифікація особи.
9	Електронний цифровий підпис.
10	Вітчизняні стандарти електронного цифрового підпису.
11	Особливості функціонування міжмережевих екранів.
12	Основні компоненти міжмережевих екранів.
13	Фільтруючі маршрутизатори.

**(заочна форма навчання)**

<b>№ п/п</b>	<b>Тематика</b>
1	Законодавчі аспекти захисту інформації.
2	Основні загрози безпеки інформації. Забезпечення безпеки інформації в комп'ютерних системах і мережах.
3	Проблема ідентифікації користувача та механізми підтвердження його істинності.
4	Основні поняття і концепції ідентифікації та електронного цифрового підпису.
5	Проблема ідентифікації користувача та механізми підтвердження його істинності.
6	Основні поняття і концепції ідентифікації та електронного цифрового підпису.
7	Взаємна перевірка істинності користувачів.
8	Біометрична ідентифікація особи.
9	Електронний цифровий підпис.
10	Вітчизняні стандарти електронного цифрового підпису.

**8 Організація та проведення тренінгу з дисципліни «Захист інформації в комп'ютерних системах»**

<b>№</b>	<b>Вид роботи</b>	<b>Порядок проведення тренінгу п/п</b>
1	Огляд сучасних засобів захисту – розгляд сучасних програмних та інформації комп'ютерної системи апаратних засобів захисту інформації, що відповідають ДСТУ;	– вибір засобу захисту відповідно до політики безпеки

2	Розгляд процесу розробки – постановка завдання; політики безпеки – вибір методів захисту інформації, відповідно до ТЗ;	– опис апаратних та програмних засобів захисту інформації; – аналіз стійкості розробленої системи захисту
3	Розробка політики безпеки згідно – розробка та аналіз ТЗ; індивідуального завдання – вибір методів захисту інформації;	– опис вибраних апаратних та програмних засобів захисту інформації; – аналіз стійкості розробленої системи захисту

## 9. Засоби оцінювання та методи демонстрування результатів навчання

У навчальному процесі застосовуються: лекції, в тому числі з використанням мультимедіапроектора та інших ТЗН; практичні заняття; індивідуальні заняття, самостійна робота студента, робота в Інтернет.

У процесі вивчення дисципліни "Захист інформації в комп'ютерних системах" використовуються наступні засоби оцінювання та методи демонстрування результатів навчання:

- поточні опитування;
- залікове модульне тестування та опитування;
- презентації результатів виконання завдань та досліджень;
- оцінювання результатів КППЗ;
- студентські презентації та виступи на наукових заходах;
- завдання на лабораторному обладнанні;
- ректорська контрольна робота; – комплексний іспит; – екзамен.

## 10. Критерії, форми поточного та підсумкового контролю

В процесі вивчення дисципліни "Захист інформації в комп'ютерних системах" використовуються наступні методи оцінювання навчальної роботи студента:

- поточне тестування та опитування;
- підсумкове тестування по кожному змістовому модулю;
- ректорська контрольна робота;
- підсумкова оцінка за комплексне практичне індивідуальне завдання, враховуючи поточне опитування;
- підсумковий письмовий екзамен.

Підсумковий бал (за 100-бальної шкалою) з дисципліни "Захист інформації в комп'ютерних систем" визначається як середньозважена величина, в залежності від питомої ваги кожної складової залікового кредиту:

Заліковий модуль 1	Заліковий модуль 2	Заліковий модуль 3 (підсумкова оцінка за КПЗ)	Заліковий модуль 4 (екзамен)	Разом
20 %	20 %	20 %	40 %	100 %
1. Усне опитування під час заняття (6 тем по 5 балів = 30 балів) 2. Письмова робота = 70 балів	1. Усне опитування під час заняття (6 тем по 5 балів = 30 балів) 2. Письмова робота = 70 балів	1. Написання та захист КПЗ = 80 балів. 2. Виконання завдань під час тренінгу = 20 балів	1. Тестові завдання (25 тестів по 2 бали за тест) – макс. 50 балів 2. Завдання. 1 – макс. 25 балів 3. Завдання. 2 – макс. 25 балів	100

#### Шкала оцінювання:

За шкалою університету	За національною шкалою	За шкалою ECTS
90-100	Відмінно	A (відмінно)
85-89	Добре	B (дуже добре)
75-84		C (добре)
65-74	Задовільно	D (задовільно)
60-64		E (достатньо)
35-59	Незадовільно	FX (незадовільно, з можливістю повторного складання)
1-34		F (незадовільно, з обов'язковим повторним курсом)

#### 11. Інструменти, обладнання та програмне забезпечення, використання яких передбачає навчальна дисципліна

№	Найменування	Номер теми
1.	Антивірусні програми, фаєрволи	5, 6
2.	Операційні системи	3, 4, 6
3.	Secure IT	8, 9



4.	Java, C++, Python Trial Version	10-12
----	---------------------------------	-------

## РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

1. Гапак О. М., Балога С.І. Захист інформації в комп'ютерних системах. Ужгород: УжНУ, 2021 184 с.
2. Гребенюк А.М. Управління інформаційною безпекою: конс. лекцій. ДніпроЖ: ДДУВС ,2019. 68 с.
3. Державна служба спеціального зв'язку та захисту інформації України: вебсайт. URL: <https://сір.gov.ua/ua/news> (дата звернення 25.08.2022).
4. Захарченко М. В., Онацький О. В., Йона Л. Г., Шинкарчук Т. М. Асиметричні методи шифрування в телекомунікаціях: навч. посіб. Одеса: ОНАЗ ім. О. С. Попова, 2011. 184 с.
5. Краснобрижий І.В., Прокопов С.О., Рижков Е.В. Інформаційне забезпечення професійної діяльності : навч. посіб. Дніпро : ДДУВС, 2018. 218 с.
6. Нормативно-правове забезпечення інформаційної безпеки: Збірник нормативно-правових до кументів / Уклад. О.Г. Корченко, Ю.О. Дрейс. Житомир : ЖВІ НАУ, 2018. 280 с.
7. Семкин С. Н., Семкин А. Н. Основи інформаційної безпеки об'єктів обробки інформації: Наук.-практ. посібник. Орел: 2018. 300 с.
8. Юдін О.К., Корченко О.Г., Конахович Г.Ф. Захист інформації в мережах передачі даних: Підручник. К.: Вид-во DIRECTLINE, 2019. 714 с.
9. Binance academy: веб-сайт. URL: <https://academy.binance.com/uk> (дата звернення 22. 08. 2022).