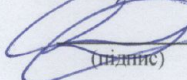


Міністерство освіти і науки України  
Національний аерокосмічний університет ім. М. Є. Жуковського  
«Харківський авіаційний інститут»

Кафедра інформаційних технологій проектування (№ 105)

**ЗАТВЕРДЖУЮ**

Голова НМК 2

 Дмитро КРИЦЬКИЙ  
(підпис) (ім'я та прізвище)

« 31 »  2023 р.

**РОБОЧА ПРОГРАМА *ОБОВ'ЯЗКОВОЇ*  
НАВЧАЛЬНОЇ ДИСЦИПЛІНИ**

Технології захисту інформації  
(назва навчальної дисципліни)

Галузь знань: 12 «Інформаційні технології»  
(шифр і найменування галузі знань)

Спеціальність: 122 «Комп'ютерні науки»  
(код і найменування спеціальності)

Освітня програма: «Інформаційні технології проектування»  
(найменування освітньої програми)

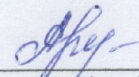
**Форма навчання: денна**

**Рівень вищої освіти: перший (бакалаврський)**

**Харків 2023 рік**



Розробник: доцент, к.т.н. каф.105 Аліна АРТЬОМОВА  
(прізвище та ім'я, посада, науковий ступінь і вчене звання)

  
(підпис)

Робочу програму розглянуто на засіданні кафедри інформаційних технологій проектування 105

(назва кафедри)

Протокол № 1 від «30» 08 2023 р.

В.о. зав. кафедри 105

  
(підпис)

Андрій БИКОВ  
(ім'я та прізвище)

## 1. Опис навчальної дисципліни

Найменування показників	Галузь знань, спеціальність, освітня програма, рівень вищої освіти	<b>Характеристика навчальної дисципліни</b>
Кількість кредитів – 4,5	<p><b>Галузь знань</b> 12 «Інформаційні технології»</p> <p><b>Спеціальність</b> 122 «Комп'ютерні науки»</p> <p><b>Освітня програма</b> «Інформаційні технології проектування»</p> <p><b>Рівень вищої освіти:</b> перший (бакалаврський)</p>	денна форма навчання
Модулів – 2		<i>Обов'язкова</i>
Змістових модулів – 2		<b>Навчальний рік</b> 2023/2024
Індивідуальне завдання «Використання блочних алгоритмів шифрування для захисту інформації в мережі».		<b>Семестр</b> 7-й
(назва)		<b>Лекції*</b>
Загальна кількість годин – 64 / 135		32 год.
		<b>Практичні, семінарські</b> 0 год.
		<b>Лабораторні*</b>
		32 год.
		<b>Самостійна робота</b> 71 год.
Тижневих годин для денної форми навчання: аудиторних – 4 самостійної роботи студента – 4,43	<b>Вид контролю</b>  іспит	

Співвідношення кількості годин ауд. занять до сам. роботи становить для денної форми  $(32 + 32) / 71 = 0,9$ .

\* Аудиторне навантаження може бути зменшене або збільшене на одну годину залежно від розкладу занять.

## 2. Мета та завдання навчальної дисципліни

**Мета вивчення:** вивчення сучасних методів, технологій та засобів захисту інформації в автоматизованих системах.

**Завдання:** вивчення комплексу організаційних (законодавча база, вимоги до персоналу та інше) та технологічних (алгоритми та протоколи, що застосовуються у криптографії) дій, що виконуються для забезпечення інформаційної безпеки автоматизованих систем.

Згідно з вимогами освітньо-професійної програми студенти повинні досягти таких **компетентностей:**

**ЗК2.** Здатність застосовувати знання у практичних ситуаціях.

**ЗК3.** Знання та розуміння предметної області та розуміння професійної діяльності.

**ЗК12.** Здатність оцінювати та забезпечувати якість виконуваних робіт

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

**Програмні результати навчання:**

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

**Результати навчання:**

знати:

- класифікацію основних погроз інформаційної безпеки;
- основні принципи забезпечення інформаційної безпеки;
- принципи захисту інформації від погроз порушення конфіденційності;
- принципи захисту інформації від погроз порушення цілісності;
- принципи захисту інформації від погроз порушення доступу;
- принципи захисту інформації від погроз розкриття параметрів системи;
- методологію побудови захищених автоматизованих систем.

вміти:

- розробити інструкції персоналу автоматизованої системи;
- розробляти криптографічні системи з використанням симетричних алгоритмів шифрування;
- розробляти криптографічні системи з використанням асиметричних алгоритмів шифрування;
- реалізовувати алгоритми основних хеш функцій;
- реалізовувати алгоритми електронно-цифрового підпису та його контролю;
- реалізовувати процедуру встановлення безпечного з'єднання.

**Міждисциплінарні зв'язки:** Операційні системи; Комп'ютерні мережі.

## 3. Програма навчальної дисципліни

### Модуль 1.

**Змістовний модуль 1. Безпека та захист даних.**

#### **Тема 1. Поняття інформаційної безпеки.**

Поняття інформації. Склад автоматизованої системи для зберігання и обробки інформації. Склад інформації. Поняття загрози інформаційної безпеки в автоматизованих системах і класифікація погроз.

#### **Тема 2. Методи забезпечення інформаційної безпеки.**

Структуризація методів забезпечення інформаційної безпеки за рівнями доступу та основними методами реалізації погроз. Рівні, методи та принципи забезпечення інформаційної безпеки в автоматизованих системах.

### **Тема 3. Забезпечення конфіденційності на рівні носіїв інформації.**

Комплекс мір по запобіганню доступності носіїв інформації. Вимоги до користувачів автоматизованої системи для забезпечення зберігання носіїв.

### **Тема 4. Забезпечення конфіденційності на рівні доступу до носіїв інформації.**

Поняття о аутентифікації та ідентифікації. Методи аутентифікації. Поняття о паролі та логіни. Вимоги про вибір паролів. Зберігання та обмін паролями. Кількісна оцінка стійкості систем з паролями.

### **Тема 5. Забезпечення конфіденційності на рівні представлення та зміст інформації.**

Захист інформації криптографічними методами. Принципи побудови криптосистем. Порушення безпеки при роботі з криптосистемами. Стенографія.

### **Тема 6. Побудова систем захисту від погроз порушення цілісності інформації.**

Поняття цілісності даних в автоматизованій системі. Принципи Кларка-Вильсона. Захист цілісності на рівні носіїв інформації. Захист цілісності на рівні змісту та представлення інформації.

### **Тема 7. Побудова систем захисту від погроз відмов в доступі та розкритті параметрів системи.**

Принципи побудови системи захисту від погроз відмови в доступі. Забезпечення відмовостійкості ПЗ АС. Запобігання відмов у ПЗ АС. Тимчасова, програмна та інформаційна збитковість.

## **Модульний контроль**

### **Модуль 2.**

#### **Змістовний модуль 2. Мережева безпека.**

### **Тема 8. Основи побудови систем секретного зв'язку.**

Поняття системи секретного зв'язку. Шифрування та дешифрування. Алгоритми шифрування.

### **Тема 9. Алгоритми шифрування.**

Типи алгоритмів шифрування. Реалізація алгоритмів шифрування. Основні вимоги до реалізації алгоритмів шифрування. Алгоритми блочного шифрування. Основні симетричні алгоритми шифрування. Основні асиметричні алгоритми шифрування.

### **Тема 10. Основи побудови криптографічних протоколів.**

Поняття криптографічного протоколу. Задачі, які вирішуються завдяки криптографічними протоколами. Безпека криптографічних протоколів. Протоколи аутентифікації. Специфічні протоколи.

## **Модульний контроль**

#### 4. Структура навчальної дисципліни

Назва змістовного модуля і тем	Кількість годин				
	Усього	У тому числі			
		л	п	лаб.	с. р.
1	2	3	4	5	6
<b>Модуль 1</b>					
<b>Змістовний модуль 1.</b>					
Тема 1.	6	2	-	-	4
Тема 2.	12	2	-	6	4
Тема 3.	12	2	-	6	4
Тема 4.	8	4	-	-	4
Тема 5.	6	2	-	-	4
Тема 6.	11	2	-	4	5
Тема 7.	11	2	-	4	5
<b>Модульний контроль</b>	2	-	-	-	2
Разом за змістовним модулем 1	68	16	-	20	32
<b>Модуль 2</b>					
<b>Змістовний модуль 2.</b>					
Тема 8.	12	4	-	4	4
Тема 9.	14	6	-	4	4
Тема 10.	14	6	-	4	4
<b>Модульний контроль</b>	2	-	-	-	2
Разом за змістовним модулем 2	42	16	-	12	14
<b>Усього годин</b>	110	32	-	32	46
<b>Індивідуальне завдання</b>	20	-	-	-	20
<b>Контрольний захід</b>	5	-	-	-	5
<b>Усього годин</b>	135	32	-	32	71

#### 5. Теми семінарських занять

Семінарські заняття навчальним планом не передбачені.

#### 6. Теми практичних занять

Практичні заняття навчальним планом не передбачені.

#### 7. Теми лабораторних занять

№ п/п	Назва теми	Кількість годин
1	Реалізація режимів роботи ECB, SM, CBC, OFB, CFB блочних шифрів	6
2	Реалізація теоретико-кількісних алгоритмів	6
3	Реалізація симетричного алгоритму шифрування DES	4
4	Модульна контрольна робота № 1	4
5	Реалізація асиметричного алгоритму шифрування RSA	4
6	Реалізація однонаправленої хеш-функції SHA	4
7	Реалізація алгоритму електронно-цифрового підпису (ЕЦП)	4
	<b>Разом</b>	32

## 8. Самостійна робота

№ п/п	Назва теми	Кількість годин
1	Побудова систем захисту від загроз розкриття параметрів інформаційної системи. Ієрархічний метод розробки ПЗ АС. Дослідження коректності реалізації та верифікації АС. Теорія безпечних систем.	15
2	Захист мереж. Міжмережеві фільтри. Основні компоненти та схеми міжмережевого захисту на базі мережевих фільтрів. Програмні засоби захисту. Електронні картки.	15
3	Підготовка до модульної контрольної роботи №1	2
4	Стійкість алгоритмів шифрування. Концепція стійкості алгоритму шифрування. Критерії стійкості. Основні види та причини атак на криптографічні алгоритми. Ключова інформація. Типи ключів. Генерація ключової інформації. Зберігання ключів.	4
5	Алгоритми шифрування. Типи алгоритмів шифрування. Реалізація алгоритмів шифрування. Основні вимоги щодо реалізації алгоритмів шифрування. Алгоритми блокового шифрування.	4
6	Хеш-функції. Електронно-цифровий підпис. Основні типи хеш-функцій. Алгоритм побудови хеш-функцій. Цілі та властивості електронно-цифрового підпису (ЕЦП). Схеми побудови ЕЦП. Види атак на ЕЦП.	4
7	Підготовка до модульної контрольної роботи №2	2
8	Контрольний захід	5
	<b>Разом</b>	<b>51</b>

## 9. Індивідуальні завдання

Зміст: Побудова ПЗ з використанням алгоритмів симетричного шифрування.

Варіанти завдань (перелік алгоритмів) – алгоритми завдяки яким можливо шифрувати інформацію.

Тижні 3 – 16. Трудомісткість: 20 годин самостійної роботи.

План-графіка виконання ІДЗ:

№	Найменування розділу	Обсяг, %	Тиждень здачі	Кількість сторінок ПЗ	Трудомісткість	
					аудиторн.	самостійн.
1	Поставлення задачі	10	3	2 – 3	—	2
2	Розроблення фізичної діаграми	20	5	2 – 3	-	4
3	Описання алгоритмів	20	6	5 – 7	-	4
4	Написання програмного забезпечення	20	7	6 – 8	-	4
5	Тестування ПЗ	20	8	3 – 5	-	4
6	Оформлення ПЗ	10	13 – 16	2	—	2
<b>Разом</b>		<b>100</b>		<b>20 – 28</b>	<b>-</b>	<b>20</b>

## 10. Методи навчання

При проведенні лекцій, лабораторних робіт та самостійної роботи використовуються такі методи навчання як словесні (пояснення, розповідь, бесіда, навчальна дискусія та ін.); наочні (ілюстрування, демонстрування, самостійне спостереження) та практичні (лабораторні роботи), а саме лекції проводяться з використанням основних розділів конспекту лекцій в електронній формі, елементів мультимедійної підтримки курсу (відеофрагментів), демонстрацій окремих прийомів роботи з інструментальним середовищем та/або роздатковий матеріалу у вигляді схем та діаграм.

Лабораторні роботи виконуються з використанням навчальних (демонстраційних) та ліцензованих програмних засобів.

Самостійна робота включає підготовку до лабораторних робіт, модульного контролю та іспиту, виконання поза аудиторної частини індивідуального завдання і вивчення вказаних вище тем за конспектом, літературними джерелами та програмною документацією.

## 11. Методи контролю

Контроль здійснюється згідно з “Положенням про модульно-рейтингову систему оцінювання знань студентів”.

Поточний контроль – відповідно до повноти, якості та своєчасності виконання лабораторних робіт та розділів домашнього завдання;

проміжний (модульний) контроль – письмові контрольні роботи на 8-му та 16-му тижнях;

підсумковий контроль – письмовий іспит.

## 12. Критерії оцінювання та розподіл балів, які отримують студенти

### 12.1. Розподіл балів, які отримують студенти (кількісні критерії оцінювання)

Складові навчальної роботи	Бали за одне заняття (завдання)	Кількість занять (завдань)	Сумарна кількість балів
<b>Змістовний модуль 1</b>			
Виконання і захист лабораторних робіт	6	4	24
Модульний контроль	20	1	20
<b>Змістовний модуль 2</b>			
Виконання і захист лабораторних (практичних) робіт	6	3	18
Модульний контроль	20	1	20
Виконання РГР	18	1	18
<b>Усього за семестр</b>			<b>100</b>

Семестровий контроль (іспит) проводиться у разі відмови студента від балів поточного тестування й за наявності допуску до іспиту. Під час складання семестрового іспиту студент має можливість отримати максимум 100 балів.

Білет для іспиту складається з 4 питань кожне питання оцінюється в 25 балів, 2 питання теоретичні, 2 питання практичні – сума 100 балів.

### 12.2. Якісні критерії оцінювання

Необхідний обсяг знань для одержання позитивної оцінки:

- класифікацію основних погроз інформаційної безпеки;



- основні принципи забезпечення інформаційної безпеки;
- принципи захисту інформації від погроз порушення конфіденційності;
- принципи захисту інформації від погроз порушення цілісності;
- принципи захисту інформації від погроз порушення доступу;
- принципи захисту інформації від погроз розкриття параметрів системи;
- методологію побудови захищених автоматизованих систем.

Необхідний обсяг вмінь для одержання позитивної оцінки:

- розробити інструкції персоналу автоматизованої системи;
- розробляти криптографічні системи з використанням симетричних алгоритмів шифрування;
- розробляти криптографічні системи з використанням асиметричних алгоритмів шифрування;
- реалізовувати алгоритми основних хеш функцій;
- реалізовувати алгоритми електронно-цифрового підпису та його контролю;
- реалізовувати процедуру встановлення безпечного з'єднання.

### 12.3 Критерії оцінювання роботи студента протягом семестру

**Задовільно (60-74).** Показати мінімум знань та умінь. Захистити всі індивідуальні завдання та здати тестування. Вміти використовувати афінні шифри, та шифри часу другої світової війни.

**Добре (75-89).** Твердо знати мінімум, захистити всі індивідуальні завдання, виконати всі КР, здати тестування та поза аудиторну самостійну роботу. Вміти все що вказано у попередньому пункті та вміти використовувати блочні шифри.

**Відмінно (90-100).** Здати всі контрольні точки з оцінкою «відмінно». Досконально знати всі теми та вміти застосовувати їх. Вміти все що вказано у попередніх пунктах та вміти використовувати шифри при потоці даних.

### Шкала оцінювання: бальна і традиційна

Сума балів	Оцінка за традиційною шкалою	
	Іспит, диференційований залік	Залік
90 – 100	Відмінно	Зараховано
75 – 89	Добре	
60 – 74	Задовільно	
0 – 59	Незадовільно	Не зараховано

### 13. Методичне забезпечення

Увесь науково методичний комплект з дисципліни розміщено на офіційному освітньому порталі Національного аерокосмічного університету ім. М.Є. Жуковського «Харківський авіаційний інститут».

### 14. Рекомендована література

#### 14.1. Базова

1. Юдін О.К. Захист інформації в мережах передачі даних / О.К. Юдін, О.Г. Корченко, Г.Ф. Конахович // Підручник — К. : Вид-во DIRECTLINE, 2019. — 714 с.

#### 14.2. Допоміжна

1. Сенів М. М. Безпека програм та даних: навч. посібник / М.М. Сенів, В.С. Яковина. — Львів : Видавництво Львівської політехніки, 2015. — 256 с.

2. Нормативно-правове забезпечення інформаційної безпеки: Збірник нормативно-правових документів / Уклад. О.Г. Корченко, Ю.О. Дрейс. — Житомир : ЖВІ НАУ, 2018. — 280 с.

3. Технології захисту інформації [Електронний ресурс] : підручник для студ. спеціальності 122 «Комп'ютерні науки», спеціалізацій «Інформаційні технології моніторингу довкілля», «Геометричне моделювання в інформаційних системах» / Ю. А. Тарнавський; КПІ ім. Ігоря

Сікорського. – Електронні текстові дані (1 файл: 2,04 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2018. – 162 с.

### **15. Інформаційні ресурси**

1. Концепція технічного захисту інформації в Україні. – [Електронний ресурс]. – Режим доступу : <http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=1126-97-%EF>.
2. Положення про проведення відкритого конкурсу криптографічних алгоритмів [Електронний ресурс] // Інститут кібернетики ім. В. М. Глушкова НАНУ; ДСТСЗІ [Електронний ресурс]. – Режим доступу : <http://www.dstszi.gov.ua/dstszi/control/gu/publish/article>
3. Комплексні системи захисту інформації [Електронний ресурс]. [Ю. Є. Яремчук, П. В. Павловський, В. С. Катаєв, В. В. Синюгін ] – Режим доступу: [https://web.posibnyky.vntu.edu.ua/fmib/41yaremchuk\\_kompleksni\\_systemy\\_za\\_hystu\\_informaciyi](https://web.posibnyky.vntu.edu.ua/fmib/41yaremchuk_kompleksni_systemy_za_hystu_informaciyi)
5. Основи програмування Режим доступу: <https://av.tib.eu/series/1500>
6. БД Режим доступу: <https://av.tib.eu/series/1487>
7. Онлайн курси міжнародного проекту кафедри. Режим доступу: [https://av.tib.eu/publisher/Projekt\\_Open\\_Education\\_Resources\\_with\\_Ukraine\\_](https://av.tib.eu/publisher/Projekt_Open_Education_Resources_with_Ukraine_)