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

Кафедра комп'ютерних систем, мереж і кібербезпеки(№ 503)

ЗАТВЕРДЖУЮ

Голова НМК

_____ Д .М. Крицький
(підпис) (ініціали та прізвище)

« 31 » серпня 2023 р.

РОБОЧА ПРОГРАМА ОБОВ'ЯЗКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Прикладна криптологія
(назва навчальної дисципліни)

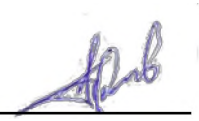
Галузь знань: 12 "Інформаційні технології"
(шифр і найменування галузі знань)

Спеціальність: 125 "Кібербезпека"
(код та найменування спеціальності)

Освітня програма: Безпека інформаційних і комунікаційних систем
(найменування освітньої програми)

Рівень вищої освіти: перший (бакалаврський)

Харків 2023 р.

Розробник: Пєвнєв В.Я., доцент кафедри 503, к.т.н., доцент 

(прізвище та ініціали, посада, науковий ступінь та вчене звання) (підпис)

Робочу програму розглянуто на засіданні кафедри _____
_ комп'ютерних систем, мереж і кібербезпеки_____

(назва кафедри)

Протокол №_____1_____від «_30___»____08___2023 р.

Завідувач кафедри_____д.т.н., професор _____ В. С. Харченко

(науковий ступінь та вчене звання) (підпис) (ініціали та прізвище)

1. Опис навчальної дисципліни

<table>
<tr><td>Найменування показників</td><td>Галузь знань, спеціальність, освітня програма, рівень вищої освіти</td><td colspan="2">Характеристика навчальної дисципліни
денна форма навчання)</td></tr>
<tr><td>Кількість кредитів – 8,5</td><td rowspan="15">Галузь знань
12 "Інформаційні технології"
(шифр та найменування)

Спеціальність
125 - Кібербезпека
(код та найменування)

Освітня програма
" Безпека інформаційних та комунікаційних систем"
(найменування)

Рівень вищої освіти:
перший (бакалаврський)</td><td colspan="2">Обов’язкова</td></tr>
<tr><td>Кількість модулів – 4</td><td colspan="2">Навчальний рік</td></tr>
<tr><td>Кількість змістових модулів – 4</td><td colspan="2">2023/ 2024</td></tr>
<tr><td rowspan="2">Індивідуальне завдання: розрахункова робота, розрахунково-графічні роботи</td><td colspan="2">Семестр</td></tr>
<tr><td>5</td><td>6</td></tr>
<tr><td rowspan="2">Загальна кількість годин
денна – 128 /255</td><td colspan="2">Лекції</td></tr>
<tr><td colspan="2">64 годин</td></tr>
<tr><td rowspan="8">Кількість тижневих годин для денної форми навчання: аудиторних – 4/4; самостійної – 7,25/7,25.</td><td colspan="2">Практичні, семінарські</td></tr>
<tr><td colspan="2"></td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td colspan="2">64 годин</td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td colspan="2">127 годин</td></tr>
<tr><td colspan="2">Вид контролю</td></tr>
<tr><td colspan="2">іспит</td></tr>
</table>

Співвідношення кількості годин аудиторних занять до самостійної роботи становить для денної форми навчання – 128/*127*.

[1)] Аудиторне навантаження може бути зменшене або збільшене на одну годину в залежності від розкладу занять.

2. Мета та завдання навчальної дисципліни

1. Мета вивчення: володіння науковими методами обґрунтування, вибору та аналізу криптографічних алгоритмів і протоколів.

2. Завдання: здійснювати порівняльний аналіз криптографічних алгоритмів та оцінку їх криптографічної стійкості; здійснювати розрахунок та вибір конкретних параметрів криптографічних алгоритмів і протоколів; використовувати спеціалізоване програмне забезпечення та розробляти на базі мов програмування високого рівня програмне забезпечення для вирішення задач криптозахисту даних

3. Програмні компетентності. Дисципліна має допомогти сформувати у студентів такі компетентності:

– (КЗ 1) здатність застосовувати знання у практичних ситуаціях;

– (КЗ 2) знання та розуміння предметної області та розуміння професії;

– (КЗ 3) здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово;

– (КЗ 4) вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням;

– (КЗ 5) здатність до пошуку, оброблення та аналізу інформації;

– (КФ 1) здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки;

– (КФ 4) здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки;

– (КФ 7) здатність відновлювати штатне функціонування інформаційних інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз , здійснення кібератак, збоїв та відмов різних класів та походження;

– (КФ 10) здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності;

– (КФ 12) здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

4. Програмні результати навчання. В результаті вивчення дисципліни студенти мають досягти такі програмні результати навчання:

– ПРН 1 Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації.

– ПРН 2 організовувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність;

– ПРН 3 Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності.

– ПРН 6 Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.

– ПРН 7 Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки.

– ПРН 8 Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки.

– ПРН 9 Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки.

– ПРН 10 Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем.

– ПРН 13 Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних.

– ПРН 19 Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.

– ПРН 22 Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки.

– ПРН 47 Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформац

– ПРН 48 Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах.

Міждисциплінарні зв'язки. Дисципліна базується на знаннях, отриманих під час вивчення дисциплін у циклі загальної і професійної підготовки, передбачених навчальним планом спеціальності.

Матеріал дисципліни базується на знаннях, отриманих під час вивчення дисциплін із циклу загальної підготовки, зокрема "Вища математика", "Фізика", "Дискретна математика" "Іноземна мова".

Матеріал дисципліни базується на знаннях, отриманих під час вивчення дисциплін із циклу професійної підготовки, а саме " Операційні системи", "Теоретичні основи криптології".

Матеріал, засвоєний під час вивчення цієї дисципліни, є базою для дисциплін із циклу професійної підготовки, а саме "Захист інформації в інформаційно-комунікаційних системах", "Системи технічного захисту інформації", "Комплексні системи захисту інформації: проектування, впровадження, супровід", "Безпека операційних систем", для курсового та дипломного проектування.

3. Програма навчальної дисципліни

Модуль 1.
Змістовий модуль 1

Тема 1. Основи захисту інформації в інфокомунікаційних системах

Місце криптографії в забезпеченні інформаційної безпеки. Основні визначення. Термінологія. Загрози інформаційній безпеці. Етапи розвітку криптографічних систем. Класифікація криптографічних систем. Загальна схема криптографічних систем. Критерії і показники ефективності криптосистем за Шеноном.

Тема 2. Класичні алгоритми шифрування

Основні класи симетричних криптосистем. Шифри перестановки. Таблиці, що шифрують. Система омофонів. Біграмні шифри. Шифр Плейфера. Шифри складної заміни. Шифр Цезаря. Багатоалфавітний шифр. Шифр Вижинера. ШифрХілла. Принципи побудови абсолютно стійких криптосистем. Одноразовий блокнот.

.

Тема 3. Алгоритми симетричного шифрування

Алгоритми блокового шифрування та їх характеристика. Мережа Фейстеля. Модифікація мережі Фейстеля. Режими блокового шифрування. Алгоритм блокового шифрування DES. Схема шифрування. Функції алгоритму DES. Алгоритми формування ключів. Криптоаналіз DES. ДСТУ ГОСТ 28147:2009

Модульний контроль

Змістовий модуль 2.

Тема4. Сучасні симетричні блокові алгоритми

Алгоритм AES. Функції алгоритму AES. Схема шифрування. Алгоритм ДСТУ 7624:2014 «Калина» Схема шифрування.

Тема 5. Потокові алгоритми шифрування.

Шифрування методом гамування. Процес гамування. Генератори двійкових псевдовипадкових послідовностей. Принципи побудови потокових шифрів. Сучасні потокові алгоритми шифрування. Криптоаналіз потокових шифрів. Методика тестування якості псевдовипадкових послідовностей. Стандарт FIPS-140-1.

Модульний контроль.

Модуль 2.

Розрахункова робота на тему «Визначення якості гами» (6 год.).

Модуль 3.

Змістовий модуль 3.

Тема 6. Криптосистеми із відкритим ключем

Теоретичні основи побудови криптосистем із відкритим ключем. Концепція криптосистем із відкритим ключем. Односпрямовані функції. Криптосистема RSA. Алгоритми генерації простих чисел. Криптосистема Ель Гамаля. Криптосистеми на еліптичних кривих.

Тема 7. Криптоаналіз асиметричних систем

Криптоаналіз систем із відкритим ключем. Класифікація алгоритмів факторизації. Алгоритм Полларда. Алгоритм Ленстра. Алгоритм факторизації на основі рішення нерівності. Алгоритм дискретного логарифмирования COS Алгоритм решета числового поля. Криптоанализ систем на эллептических кривых Алгоритм дискретного логарифмування COS.

Модульний контроль.

Змістовий модуль 4.

Тема 8. Автентифікация та цифровий підпис

Задача автентифікації. Задача автентифікації даних. Контроль незмінності масивів даних. Виробітку коду виявлення маніпуляцій. Цифровий підпис. Цифровий підпис на основі традиційних блокових шифрів. Цифрові підписи, засновані на асиметричних криптосистемах. Функція хешування.

Тема 9. Реалізація алгоритмів автентифікації і цифрового підпису

ДСТУ 4145-2002. Зображення і перетворення даних. Обчислювальні алгоритми. Обчислення і перевіряння параметрів цифрового підпису. Обчислення і перевіряння цифрового підпису. Багатоадресна автентіфікація. Багатоадресна автентіфікація без забезпечення невідмовлення. Багатоадресна автентіфікація з забезпеченням невідмовлення.

Модульний контроль.

Модуль 4.

Розрахунково-графічна робота на тему «Побудова простих чисел» (6 год.).

3. Структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин				
	Денна форма				
	Усього	У тому числі			
		л	п	лаб.	с. р.
Модуль 1					
Змістовий модуль 1					
Тема 1. Основи захисту інформації в інфокомунікаційних системах	16	4		2	10
Тема 2. Класичні алгоритми шифрування	32	6		6	20
Тема 3. Алгоритми симетричного шифрування. Модульний контроль	38	6		8	24
Разом за змістовим модулем 1	86	16		16	54
Змістовий модуль 2					
Тема4. Сучасні симетричні блокові алгоритми	44	8		8	28
Тема 5. Потокові алгоритми шифрування. Модульний контроль	44	8		8	28
Разом за змістовим модулем 2	88	16		16	56
Разом за модулем 1	174	32		32	110
Модуль 2					
Індивідуальне завдання	6				6
Усього годин за семестр	180	32		32	116
Модуль 3					
Змістовий модуль 3					
Тема 6. Криптосистеми із відкритим ключем	44	8		8	28
Тема 7**.** Криптоаналіз асиметричних систем. Модульний контроль	44	8		8	28
Разом за змістовим модулем 3	88	16		16	56
Змістовий модуль 4					
Тема 8. Автентифікация та цифровий підпис	42	8		8	26
Тема 9. Реалізація алгоритмів автентифікації і цифрового підпису. Модульний контроль	44	8		8	28
Разом за змістовим модулем 4	86	16		16	54
Разом за модулем 4	174	32		32	110
Модуль 4					
Індивідуальне завдання	6				6
Усього годин за семестр	180	32		32	116
Усього годин за дисципліною	360	64		64	232

4. Теми семінарських занять

№ з/п	Назва теми	Кількість годин
1		
	Разом	

5. Теми практичних занять

№ з/п	Назва теми	Кількість годин	
1			
	Разом		

6. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1	Дослідження алгоритмів, що реалізують шифри простої заміни та підстановки	4
2	Дослідження алгоритму багато абеткового шифру	4
3	Дослідження режимів блокового шифрування	4
4	Дослідження алгоритму блокового шифрування DES	4
5	Дослідження функції та схеми шифрування алгоритму AES	4
6	Дослідження функції та схеми шифрування алгоритму ДСТУ 7624:2014 «Калина»	4
7	Дослідження конгруентних алгоритмів генерації гама шифру	4
8	Дослідження алгоритмів генерації гама шифру побудований на регістрах зсуву	4
9	Дослідження алгоритмів генерації простих чисел	4
10	Дослідження алгоритмів RSA та Ель Гаммаля	4
11	Дослідження алгоритмів факторизації	4
12	Дослідження алгоритмів крипто аналізу систем дискретного логарифмування	4
13	Дослідження коду виявлення маніпуляцій та геш функції	4
14	Дослідження алгоритмів формування цифрового підпису	4
15	Дослідження цифрового підпису на основі протоколу Шнорра	4
16	Дослідження протоколу Фейге – Фиата – Шамира	4
	Разом	**64**

7. Самостійна робота

№ з/п	Назва теми	Кількість годин
1	Тема 1. Основи захисту інформації в інфокомунікаційних системах	10
2	Тема 2. Класичні алгоритми шифрування	20
3	Тема 3. Алгоритми симетричного шифрування	24
4	Тема4. Сучасні симетричні блокові алгоритми	28
5	Тема 5. Потокові алгоритми шифрування.	28
6	Виконання розрахункової роботи.	6
7	Тема 6. Криптосистеми із відкритим ключем	28
8	Тема 7. Криптоаналіз асиметричних систем	28
9	Тема 8. Автентифікация та цифровий підпис	26
10	Тема 9. Реалізація алгоритмів автентифікації і цифрового підпису	28
11	Виконання розрахункової роботи.	6
	Разом	**232**

8. Індивідуальні завдання

№ з/п	Назва теми	Кількість годин
1	Розрахункова робота на тему «Визначення якості гами»	6
2	Розрахунково-графічна робота на тему «Побудова простих чисел»	6
	Разом	**12**

9. Методи навчання

Проведення аудиторних лекцій, практичних занять, консультацій, а також самостійна робота студентів за матеріалами, опублікованими кафедрою.

10. Методи контролю

Проведення поточного контролю, письмового модульного контролю, підсумковий контроль у вигляді іспиту.

11. 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
Змістовний модуль 1			
Робота на лекціях	0…1	8	0…8
Виконання і захист лабораторних (практичних) робіт	0...6	4	0...24
Модульний контроль	0…25	1	0…25
Змістовний модуль 2			
Робота на лекціях	0…1	8	0…8
Виконання і захист лабораторних (практичних) робіт	0...6	4	0...24
Модульний контроль	0…25	1	0…25
Виконання і захист РР	0…10	1	0…10
Усього за семестр			**0…100**
Змістовний модуль 3			
Робота на лекціях	0…1	8	0…8
Виконання і захист лабораторних (практичних) робіт	0...6	4	0...24
Модульний контроль	0…25	1	0…25
Змістовний модуль 4			
Робота на лекціях	0…1	8	0…8
Виконання і захист лабораторних (практичних) робіт	0...6	4	0...24
Модульний контроль	0…25	1	0…25
Виконання і захист РГР	0…10	1	0…10
Усього за семестр			**0…100**

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

Білет для іспиту/заліку складається з двох теоретичних питання (0…30 балів за кожне питання) та одно практичне завдання (0…40 балів).

12.2. Якісні критерії оцінювання

Необхідний обсяг знань для одержання позитивної оцінки.
Студент повинен знати:

- загальні аспекти проблематики в галузі інформаційної безпеки (сучасний стан задач та проблем, загрози та види вірусних атак на інформаційні та комунікаційні системи, вимоги до їх захищеності), а також тенденції і перспективи створення механізмів захисту інформації за допомогою систем криптографічного захисту;
- характеристику методів і засобів криптографічного перетворення інформації, а також основних методів крипто аналізу;
- принципи побудови симетричних (блочних і потокових) та асиметричних криптографічних алгоритмів та протоколів, що використовуються для забезпечення конфіденційності та автентичності і цілісності повідомлень, а також показники ефективності криптографічних систем;
- методи забезпечення автентичності користувачів комп'ютерної мережі;
- характеристику методів реалізації основних функцій системи управління ключовими структурами.

Необхідний обсяг вмінь для одержання позитивної оцінки.

Студент повинен вміти:

- виконувати криптографічні перетворення у відповідності зі схемами симетричного (блочного та потокового) і несиметричного шифрування, а також проводити порівняльний аналіз крипостійкості симетричних та несиметричних криптографічних систем;
- розраховувати параметри асиметричних алгоритмів цифрового підпису, протоколів автентифікації користувачів та схем формування ключів;
- здійснювати оцінку криптографічної стійкісті криптографічних алгоритмів та схем хешування 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

12. Методичне забезпечення

1. Презентації лекцій
2. Керівництво до лабораторних робіт

14. Рекомендована література

Базова

1. Горбенко І.Д., Гриненко Т.О. Захист інформації в інформаційно-комунікаційних системах. Част.1. Криптографічний захист інформації. Харків: ХНУРЕ, 2004. 367 с.
2. Задірака В., Олесик О. Комп'ютерна криптологія. К.: «Політехніка», 2002. 502 с.

Допоміжна

1. Барич С.Г., Гончаров В.В., Сєров Р.Є. Основи сучасної криптографії.-М.: Гаряча лінія-Телеком, 2001.-120 с.
2. Романець Ю.І., Тимофєєв П.А., Шаньгін В.Ф. Захист інформації в комп'ютерних системах та мережах.-М.: Радіо та зв'язок, 1999.-328 с.
3. Ельтанов Б.А. Розвиток методу решета. М.: Статистика, 1986. - 157с.
4. Василенко О. Н. Теоретико-числові алгоритми у криптографії. М: МЦНМО. 2003. 328 с.

15. Інформаційні ресурси

1. http://www.kernel.org
2. http://fedoraproject.org
3. http://www.ubuntu.com
4. http://www.csn.khai.edu