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

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

ЗАТВЕРДЖУЮ

Гарант освітньої програми

_____ О. О. Ілляшенко
(підпис) (ініціали та прізвище)

«31» серпня 2021 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)

Форма навчання: денна

Рівень вищої освіти: перший (бакалаврський)

Харків 2021 рік

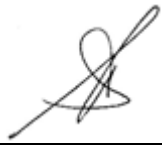
Розробник: Пєвнєв В. Я., доцент, д.т.н., доцент 

(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 2021 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>Характеристика навчальної дисципліни (денна форма навчання)</td></tr>
<tr><td>Кількість кредитів – 12</td><td rowspan="11">Галузь знань
12 «Інформаційні технології"
(шифр та найменування)

Спеціальність
125 «Кібербезпека"
(код та найменування)

Освітня програма
«Безпека інформаційних і комунікаційних систем»
(найменування)

Рівень вищої освіти:
перший (бакалаврський)</td><td>Обов’язкова</td></tr>
<tr><td>Кількість модулів – 4</td><td>Навчальний рік</td></tr>
<tr><td>Кількість змістовних модулів – 4</td><td>2021/ 2022</td></tr>
<tr><td>Індивідуальне завдання - РР, РГР
(назва)</td><td>Семестр</td></tr>
<tr><td rowspan="2">Загальна кількість годин – 128*/232</td><td>5, 6-й</td></tr>
<tr><td>Лекції *</td></tr>
<tr><td rowspan="3">Тижневих годин для денної форми навчання:
аудиторних – 4
самостійної роботи студента – 7,25</td><td>64 годин</td></tr>
<tr><td>Практичні, семінарські*</td></tr>
<tr><td>64 годин</td></tr>
<tr><td></td><td>Лабораторні *</td></tr>
<tr><td></td><td>0 годин</td></tr>
<tr><td></td><td>Самостійна робота</td></tr>
<tr><td></td><td>232 годин</td></tr>
<tr><td></td><td>Вид контролю</td></tr>
<tr><td></td><td>іспит</td></tr>
</table>

Співвідношення кількості годин аудиторних занять до самостійної роботи становить: *48/72*.

* Аудиторне навантаження може бути зменшене або збільшене на одну годину в залежності від розкладу занять.

2. Мета та завдання навчальної дисципліни

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

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.

Компетентності, які набуваються:

- здатність застосовувати знання у практичних ситуаціях;
- знання та розуміння предметної області та розуміння професії;
- здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово;
- вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням;
- здатність до пошуку, оброблення та аналізу інформації;
- 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;
- здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки;
- здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз , здійснення кібератак, збоїв та відмов різних класів та походження;
- здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності;
- здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

Очікувані результати навчання:

- організовувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність;
- використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів;

- вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;
- застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем;
- впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки;
- здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах;
- вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації.

Пререквізити – дисципліна є обов'язковим компонентом освітній програми і базується на знаннях, отриманих під час вивчення дисциплін із циклу загальної підготовки, зокрема "Вища математика", "Фізика", "Теорія електричних кіл і мікроелектроніка", " Дискретна математика " "Іноземна мова".

Кореквізити – 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. «Науково-педагогічне стажування».

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.).

Модульний контроль.

4. 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

5. Теми семінарських занять

№ з/п	Назва теми	Кількість годин
		Денна форма навчання
1		
2		
	Разом	

6. Теми практичних занять

№ з/п	Назва теми	Кількість годин
1	Алгоритми, що реалізують шифри простої заміни та підстановки	4
2	Алгоритми багато абеткового шифру	4
3	Режими блокового шифрування	4
4	Алгоритм блокового шифрування DES	4
5	Функції та схеми шифрування алгоритму AES	4
6	Функції та схеми шифрування алгоритму ДСТУ 7624:2014 «Калина»	4
7	Конгруентних алгоритмів генерації гама шифру	4
8	Алгоритми генерації гама шифру побудований на регістрах зсуву	4
9	Алгоритми генерації простих чисел	4
10	Алгоритми RSA та Ель Гаммаля	4
11	Алгоритми факторизації	4
12	Алгоритми крипто аналізу систем дискретного логарифмування	4
13	Код виявлення маніпуляцій та геш функції	4
14	Алгоритми формування цифрового підпису	4
15	Цифрій підпис на основі протоколу Шнорра	4

16	Протокол Фейге – Фиата – Шамира	4
	Разом	**64**

7. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1		
2		
	Разом	

8. 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**

9. 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**

10. Методи навчання

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

11. Методи контролю

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

12. Критерії оцінювання та розподіл балів, які отримують здобувачі

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 практичних робіт	0...5	4	0...20
Модульний контроль	0…17	1	0…17
Змістовний модуль 2			
Робота на лекціях	0…1	8	0…8
Виконання і захист практичних робіт	0...5	4	0...20
Модульний контроль	0…17	1	0…17
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 практичних робіт	0...5	4	0...20
Модульний контроль	0…17	1	0…17
Змістовний модуль 4			
Робота на лекціях	0…1	8	0…8
Виконання і захист практичних робіт	0...5	4	0...20
Модульний контроль	0…17	1	0…17
Виконання і захист РГР	0…10	1	0…10
Усього за семестр			**0…100**

Контроль знань при проведенні занять оцінюється за такими шкалами:
<u>активність на лекції</u> під час відповідей на питання:
- активна робота на лекції - 1 бал;

<u>виконання і захист практичних робіт:</u>
- при виконанні всіх вимог завдань методик на роботи - 5 бали;
- незначні недоліки при відповіді на питання при захисті результатів роботи за змістом досліджуваної теми - 4 бали;
- неповні відповіді на питання при захисті результатів роботи за змістом досліджуваної теми - 3 бали;
- неповні відповіді на питання за змістом і результатами роботи - 2 бала;
- недооформлені результати роботи і неповні відповіді на питання за змістом результатів роботи -1бал;
- якщо робота не виконана і не захищена - 0 балів.

На модульний контроль (всього 17 балів) виносяться всі пройдені за контрольований період теми, які включаються в варіанти завдань, що містять по 17 питання (по всім темам та видам занять). Максимальна кількість балів за кожне питання - 1.

Семестровий контроль у вигляді іспиту 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 двох теоретичних та одного практичного запитань, максимальна кількість за кожне із запитань, складає за теоретичними питаннями 30 балів, за практичнім - 40 балів.

Критерії оцінювання роботи студента протягом семестру

Задовільно (60-74). Показати мінімум знань та умінь. Захистити не менше 80% від усіх завдань практичних занять. Уміти використовувати правові та нормативні документи, вітчизняних та міжнародних стандартів для проведення наукових робіт та робіт щодо криптологічному захисту інформації.

Добре (75-89). Твердо знати необхідний обсяг знань для одержання позитивної оцінки, захистити не менше 90% завдань практичних занять. Уміти використовувати сучасні методи теоретичних та експериментальних досліджень для організації криптологічного захисту інформації. Мати необхідний обсяг вмінь для одержання позитивної оцінки.

Відмінно (90-100). Здати всі контрольні точки з оцінкою «відмінно». Досконально знати всі теми та уміти їх застосовувати. Уміти організувати й виконувати роботи з криптологічного захисту інформації..

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

1. Навчально-методичний комплекс дисципліни розміщений на кафедральному сервері у відповідному каталозі.

2. Дистанційний курс в системі дистанційного навчання Ментор, розташований за адресою: https://mentor.khai.edu/course/view.php?id=4835.

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. Баричев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии.-М.: Горячая линия-Телеком, 2001.-120 с.
2. Романец Ю.И., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях.-М.: Радио и связь, 1999.-328 с.
3. Эльтанов Б.А. Развитие метода решета. М.: Статистика, 1986. – 157с.
4. Василенко О. Н.Теоретико-числовые алгоритмы в криптографии. 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