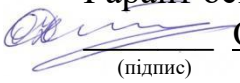
Міністерство освіти і науки України
Національний аерокосмічний університет ім. М. Є. Жуковського
«Харківський авіаційний інститут»

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

ЗАТВЕРДЖУЮ

Гарант освітньої програми

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

" 31" серпня 2024 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»
(шифр і назва галузі знань)

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

Освітня програма «Кібербезпека»
(найменування освітньої програми)

Форма навчання: денна

Рівень вищої освіти: перший (бакалаврський)

Харків 2024 рік

Розробник: Пєвнєв В.Я., професор, 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 2024 р.

Завідувач кафедри д.т.н., професор (підпис) В. С. Харченко
(науковий ступінь та вчене звання) (ініціали та прізвище)

1. Опис навчальної дисципліни

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, спеціальність, освітня програма, рівень вищої освіти</td><td colspan="2">Характеристика навчальної дисципліни</td></tr>
<tr><td>Денна форма навчання</td><td>Заочна форма навчання</td></tr>
<tr><td>Кількість кредитів – 4(4,5)</td><td rowspan="11">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 –2</td><td colspan="2">Навчальний рік</td></tr>
<tr><td>Кількість змістових модулів – 4</td><td colspan="2">2024/ 2025</td></tr>
<tr><td>Індивідуальне завдання РР(РГР)</td><td colspan="2">Семестр</td></tr>
<tr><td rowspan="2">Загальна кількість годин
денна – 112 / 255</td><td>5-й</td><td>6-й</td></tr>
<tr><td colspan="2">Лекції 1)</td></tr>
<tr><td rowspan="6">Кількість тижневих годин для денної форми навчання:
аудиторних – 3(4)
самостійної роботи студента – 4,5(4,5)</td><td>32 годин</td><td>32 годин</td></tr>
<tr><td colspan="2">Практичні, семінарські</td></tr>
<tr><td></td><td></td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>16 годин</td><td>32 годин</td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>72 годин</td><td>71 годин</td></tr>
<tr><td colspan="2">Вид контролю</td></tr>
<tr><td>іспит</td><td>іспит</td></tr>
</table>

Співвідношення кількості годин аудиторних занять до самостійної роботи становить: для денної форми навчання – 112/143

.

2. Мета та завдання навчальної дисципліни

Мета – володіння науковими методами обґрунтування, вибору та аналізу криптографічних алгоритмів і протоколів, їх використання для вирішення задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах.

Завдання:

– вивчити основні поняття, критерії та показники надійності та криптостійкості криптографічних алгоритмів і протоколів;

– вивчити основні методи та засоби шифрування, що використаються в симетричних та асиметричних криптосистемах;

– вивчити методи і засоби забезпечення конфіденційності та контроля цілісності інформації , що використаються в інформаційно-телекомунікаційних системах;

– оволодіти практичними навичками використання систем шифрування під час передавання та збереження інформації в інформаційно-телекомунікаційних системах.

Компетентності, які набуваються.

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 впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.).

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, вразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

Очікувані 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 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 інформації.

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

Пререквізити –"Апаратні та програмні засоби захисту інформації", "Теоретичні основи криптології", "Операційні системи".

Кореквізити – "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.).

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	12	4			8
Тема 2. Класичні алгоритми шифрування	22	6		4	12
Тема 3. Алгоритми симетричного шифрування. Модульний контроль	22	6		4	12
Разом за змістовим модулем 1	56	16		8	32
Змістовий модуль 2					
Тема4. Сучасні симетричні блокові алгоритми	28	8		4	16
Тема 5. Потокові алгоритми шифрування. Модульний контроль	30	8		4	18
Разом за змістовим модулем 2	58	16		8	34

Разом за модулем 1	114	32		16	66
Модуль 2					
Індивідуальне завдання	6				6
Усього годин за семестр	120	32		16	72
Модуль 3					
Змістовий модуль 3					
Тема 6. Криптосистеми із відкритим ключем	32	8		8	16
Тема 7**.** Криптоаналіз асиметричних систем. Модульний контроль	32	8		8	16
Разом за змістовим модулем 4	64	16		16	32
Змістовий модуль 5					
Тема 8. Автентифікация та цифровий підпис	32	8		8	16
Тема 9. Реалізація алгоритмів автентифікації і цифрового підпису. Модульний контроль	33	8		8	17
Разом за змістовим модулем 5	65	16		16	33
Разом за модулем 3	129	32		32	65
Модуль 4					
Індивідуальне завдання	6				6
Усього годин за семестр	135	32		32	71
Усього годин за дисципліною	255	64		48	143

5. Теми семінарських занять

№ з/п	Назва теми	Кількість годин	
		Денна форма навчання	Заочна форма навчання
1	*Не передбачено*		
	Разом		

6. Теми практичних занять

№ з/п	Назва теми	Кількість годин	
		Денна форма навчання	Заочна форма навчання
1	*Не передбачено*		
	Разом		

7. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
		Денна форма навчання
1	Дослідження алгоритму багато абеткового шифру	4
2	Дослідження алгоритму блокового шифрування DES	4
3	Дослідження функції та схеми шифрування алгоритму *ДСТУ* 7624:2014 «Калина»	4

4	Дослідження алгоритмів генерації гама шифру	4
5	Дослідження алгоритмів генерації простих чисел	4
6	Дослідження алгоритмів RSA та Ель Гаммаля	4
7	Дослідження алгоритмів факторизації	4
8	Дослідження алгоритмів крипто аналізу систем дискретного логарифмування	4
9	Дослідження коду виявлення маніпуляцій та геш функції	4
10	Дослідження алгоритмів формування цифрового підпису	4
11	Дослідження цифрового підпису на основі протоколу Шнорра	4
12	Дослідження протоколу Фейге – Фиата – Шамира	4
	Разом	**48**

8. Самостійна робота

№ з/п	Назва теми	Кількість годин
1	Тема 1. Основи захисту інформації в інфокомунікаційних системах	8
2	Тема 2. Класичні алгоритми шифрування	12
3	Тема 3. Алгоритми симетричного шифрування	12
4	Тема4. Сучасні симетричні блокові алгоритми	16
5	Тема 5. Потокові алгоритми шифрування.	18
6	Виконання розрахункової роботи.	6
7	Тема 6. Криптосистеми із відкритим ключем	16
8	Тема 7. Криптоаналіз асиметричних систем	16
9	Тема 8. Автентифікация та цифровий підпис	16
10	Тема 9. Реалізація алгоритмів автентифікації і цифрового підпису	17
11	Виконання розрахункової роботи.	6
	Разом	**143**

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, лабораторних занять, консультацій, а також самостійна робота студентів за матеріалами, опублікованими кафедрою.

11. Методи контролю

Проведення поточного контролю, модульного контролю (тести за кожним змістовим модулем), підсумковий контроль у вигляді іспиту.

12. Розподіл балів, які отримують студенти

Складові навчальної роботи	Бали за одне заняття (завдання)	Кількість занять (завдань)	Сумарна кількість балів
Модуль 1			
Робота на лекціях	0…1	16	0…16
Виконання і захист лабораторних робіт	0...5	4	0...20
Модульний контроль	0…32	2	0…64
Усього за семестр			**0 …100**
Модуль 2			
Робота на лекціях	0…1	16	0…16
Виконання і захист лабораторних робіт	0...5	8	0...40
Модульний контроль	0…22	2	0…44
Усього за семестр			**0…100**

Лабораторна робота має бути здана протягом двох тижнів. Для отримання максимальної оцінки повіни здати протягом трьох днів з моменту виконання за розкладом занять; 4 – 6; 3 – 9; 2 – 12; 1-14 днів

Участь у конференції -10 балів.

Стаття у фаховому журналі -20 балів

Критерії оцінювання знань студента під час іспиту

Задовільно (60-74). Мати уявлення про принципи побудови симетричних (блочних і потокових) та асиметричних криптографічних алгоритмів та протоколів, що використовуються для забезпечення конфіденційності та автентичності і цілісності повідомлень, криптографічні перетворення у відповідності зі схемами симетричного (блочного та потокового) і асиметричного шифрування, а також проводити порівняльний аналіз крипостійкості симетричних та асиметричних криптографічних систем.

Добре (75-89). Твердо знати характеристику методів і засобів криптографічного перетворення інформації, показники ефективності криптографічних систем, методи забезпечення автентичності користувачів комп’ютерної мережі, виконувати криптографічні перетворення у відповідності зі схемами симетричного (блочного та потокового) і асиметричного шифрування, розраховувати параметри асиметричних алгоритмів цифрового підпису, протоколів автентифікації користувачів та схем формування ключів.

Відмінно (90-100). Мати теоретичні знання та практичні навички щодо побудови та використання систем шифрування та обміну ключами.

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. Презентації лекцій
2. Керівництво до лабораторних робіт
3. Навчально-методичний комплекс дисципліни розміщений на кафедральному сервері у відповідному каталозі.
4. 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.
3. Горбенко Ю. І. Побудування та аналіз систем, протоколів и засобів криптографічного захисту інформації: монографія. Харків: Вид. «Форт»-
4. 2015. 900с.»

Допоміжна

1. Євсеєв С.П. , Король О.Г. , Шматко О.В Кібербезпека: криптографія з PYTHON. Вид. Новий світ-2000. 2021.- 120 с.
2. Клесов О.І., Елементарна теорія чисел та елементи криптографії, 2017, ТВіМС, Київ, 394 стор.
3. Прикладна криптологія : системи шифрування : підручник / О. Г. Корченко, В. П. Сіденко, Ю. О. Дрейс. – К. : ДУТ, 2014. – 448 с.

Інформаційні ресурси

1. Кваліфікаційний центр інформаційних технологій та кібербезпеки ДержНДІ технологій кібербезпеки [Електронний ресурс] – http://dstszi.gov.ua.
2. The Linux Kernel Archives [Електронний ресурс] – http://www.kernel.org
3. An innovative platform for hardware, clouds, and containers, Fedora [Електронний ресурс] – http://fedoraproject.org.
4. Canonical Ubuntu [Електронний ресурс] – http://www.ubuntu.com.
5. КАФЕДРА КОМП'ЮТЕРНИХ СИСТЕМ, МЕРЕЖ І КІБЕРБЕЗПЕКИ [Електронний ресурс] – http://www.csn.khai.edu.