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

Кафедра комп'ютерних наук та інформаційних технологій (№ 302)

ЗАТВЕРДЖУЮ

Гарант освітньої програми

_____ _Мирослав МОМОТ
(підпис) (ініціали та прізвище)

«____» _____ 2024 р.

РОБОЧА ПРОГРАМА ОБОВ'ЯЗКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Захист інформації в комп'ютерних системах

(назва навчальної дисципліни)

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

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

Освітня програма: «Комп'ютеризація обробки інформації та управління»
(найменування освітньої програми)

Форма навчання: денна

Рівень вищої освіти: перший (бакалаврський)

Харків 2024 рік

Розробник: Олексій ГУБКА, доцент, к.т.н., доцент 

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

Робочу програму розглянуто на засіданні кафедри комп'ютерних наук та інформаційних технологій

Протокол № _671/07_ від « _27_» _08_ 2024 р.

Завідувач кафедри _д.т.н., проф._ _____ Олег ФЕДОРОВИЧ

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

1. Опис навчальної дисципліни

<table>
<tr><td>Найменування показника</td><td>Галузь знань, спеціальність, освітня програма, рівень вищої освіти</td><td>Характеристика навчальної дисципліни (денна форма навчання)</td></tr>
<tr><td>Кількість кредитів – 5,5</td><td rowspan="10">Галузь знань
12 «Інформаційні технології»
(шифр та найменування)

Спеціальності:
122 «Комп’ютерні науки»

Освітні програми:
«Комп’ютеризація обробки інформації та управління»

Рівень вищої освіти:

перший (бакалаврський)</td><td>Обов'язкова</td></tr>
<tr><td>Кількість модулів – 2</td><td>Навчальний рік</td></tr>
<tr><td>Кількість змістових модулів – 2</td><td>2024/ 2025</td></tr>
<tr><td>Індивідуальне завдання: РР «Криптографічні методи захисту інформації».</td><td>Семестр</td></tr>
<tr><td rowspan="2">Загальна кількість годин – 60/165</td><td rowspan="2">8-й</td></tr>
<tr><td>Лекції</td></tr>
<tr><td rowspan="6">Кількість тижневих годин для денної форми навчання: аудиторних – 5 , самостійної роботи студента – 7</td><td rowspan="2">36 годин</td></tr>
<tr><td>Практичні, семінарські</td></tr>
<tr><td>–</td></tr>
<tr><td>Лабораторні</td></tr>
<tr><td>24 години</td></tr>
<tr><td>Самостійна робота</td></tr>
<tr><td>105 годин</td></tr>
<tr><td>Вид контролю</td></tr>
<tr><td>Модульний контроль, іспит</td></tr>
</table>

Співвідношення кількості годин аудиторних занять до самостійної роботи становить:
для денної форми навчання – 60/105

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

2. Мета та завдання навчальної дисципліни

Мета: надати студентам знань з методів та засобів забезпечення інформаційної безпеки, захисту інформаційних ресурсів та об’єктів критичної інфраструктури.

Завдання: вивчити основні методології захисту інформації для створення надійних комп'ютерних систем.

Загальні компетентності (ЗК):

- ЗК2. Здатність застосовувати знання у практичних ситуаціях.
- ЗК4. Здатність спілкуватися державною мовою як усно, так і письмово.
- ЗК5. Здатність спілкуватися іноземною мовою.
- ЗК11. Здатність приймати обґрунтовані рішення.

Спеціальні (фахові) компетентності:

- СК14. Здатність застосовувати методи та засоби забезпечення інформаційної безпеки, розробляти й експлуатувати спеціальне програмне забезпечення захисту інформаційних ресурсів об'єктів критичної інформаційної інфраструктури.
- СК18. Здатність розробляти й експлуатувати спеціальне програмне забезпечення для об'єктів та процесів аерокосмічної галузі.

Програмні результати навчання:

- ПР9. Розробляти програмні моделі предметних середовищ, вибирати парадигму програмування з позицій зручності та якості застосування для реалізації методів та алгоритмів розв'язання задач в галузі комп'ютерних наук.
- ПР19. Розуміти концепцію критичних інформаційних технологій для управління небезпечними системами та процесами.

Міждисциплінарні зв'язки:

Дана дисципліна базується на дисциплінах, які були вивчені студентами на попередніх курсах:

- Алгоритмізація та мови програмування (ОК7)
- Програмування ІУС (ОК12)
- Основи тестування інформаційних систем (ОК16)
- Технологія створення програмних продуктів (ОК28)
- Методи та системи штучного інтелекту (ОК30)
- Організація БД та знань (ОК32)

Дана дисципліна зв'язана з наступними дисциплінами, які вивчаються студентами пізніше:

- Дипломна робота (проект) бакалавра (ОК37)

3. Програма навчальної дисципліни

Модуль 1.

Змістовий модуль 1

Тема 1. Вступ до навчальної дисципліни.

Предмет, об'єкт, мета і задачі вивчення дисципліни. Місце і роль курсу в системі дисциплін. Основні тенденції розвитку методів захисту ПК і криптографічних систем. Історія розвитку криптографії.

Тема 2. Класифікація небезпек для програмного забезпечення інформаційних систем (ПЗ ІС).

Визначення програмного забезпечення ІС. Класифікація ПЗ. Вимоги до ПЗ. Антивірусний захист ПК. Фізичний захист ПК. Антишпигунський захист ПК. Криптографічний захист даних ПЗ інформаційних управляючих систем (ІУС) та об'єктів критичної інформаційної інфраструктури. Авторизація доступу в операційних системах (FreeBSD, Mac OS, Linux).

Тема 3. Загальні поняття криптографічного захисту інформації.

Поняття шифру. Оцінка якості шифрів. Різновиди задач криптографічного аналізу. Абсолютна стійкість та стійкість у операціях. Термінологія з захисту інформації.

Тема 4. Системи відкритого шифрування.

Синтез якісних шифрів. Системи відкритого розподілення ключів та системи відкритого шифрування. Системи Диффи-Хеллмана и RSA. Алгоритми шифрування DSA, MD4, MD5. Аналіз криптографічної стійкості алгоритмів шифрування. Електронний цифровий підпис та печатка (ЕЦП).

Компоненти ЕЦП. Поняття та свойства хеш-функції. Протокол ЕЦП Ель-Гамаля.

Тема 5. Загальні відомості про алгоритм шифрування "Калина" ДСТУ 7624:2014. Реалізація алгоритму. Базові цикли криптографічних перетворень. Базові режими шифрування. Оптимізація алгоритму на мові високого рівня.

Тема 6. Антивірусний захист даних.

Методи боротьби з комп'ютерними вірусами. Класифікація комп'ютерних вірусів. Віруси-трояни. Віруси-черв'яки. Програми-монітори. Програми-сканери.

Модульний контроль.

Модуль 2.

Змістовий модуль 2

Тема 7. Алгоритми генерації випадкових чисел.

Поняття програмного датчику випадкових чисел (ПДВЧ). Модель функціонування ПДВЧ. Вибір алгоритму ПДВЧ. Вибір алгоритму ПДВЧ.

Тема 8. Криптографічні інтерфейси.

Термінологія. Поняття зовнішнього сервісу безпеки. Огляд функцій інтерфейсу CryptoAPI. Системні питання реалізації засобів криптографічного захисту інформації (ЗКЗІ). Засоби та особливості реалізації криптографічних систем. Криптографічний захист транспортного рівня. Криптографічний захист прикладного рівня.

Тема 9. Забезпечення надійності криптографічних алгоритмів.

Основні підходи забезпечення відмовостійкості. Специфічні питання забезпечення надійності програмної реалізації криптографічних алгоритмів захисту даних. Методологія побудови надійних ЗКЗІ.

Тема 10. Особливості криптографічних засобів (КЗ).

Ліцензування КЗ. Сертифікація КЗ. Стандартизація КЗ. Законодавча база України стосовно захисту інформації.

Тема 11. Заключна лекція.

Перспективи розвитку технологій захисту інформації.

Модульний контроль.

Індивідуальне завдання – виконання РР на тематику «Криптографічні методи захисту інформації».

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. Вступ до навчальної дисципліни	12	4	-	-	8
Тема 2. Класифікація небезпек для ПЗ ІС	12	4	-	-	8
Тема 3. Загальні поняття криптографічного захисту інформації	16	4	-	4	8
Тема 4. Системи відкритого шифрування	16	4	-	4	8
Тема 5. Загальні відомості про алгоритм шифрування “Калина” ДСТУ 7624:2014	16	4	-	4	8
Тема 6. Антивірусний захист даних	13	4	-	4	5
Усього годин	**85**	**24**	**-**	**16**	**45**
Модуль 2					
Змістовий модуль 2					
Тема 7. Алгоритми генерації випадкових чисел	14	2	-	2	10
Тема 8. Криптографічні інтерфейси	14	2	-	2	10
Тема 9. Забезпечення надійності криптографічних алгоритмів	16	2	-	4	10
Тема 10. Особливості криптографічних засобів	12	2	-	-	10
Тема 11. Заключна лекція	4	4	-	-	-
Усього годин	**60**	**12**	**-**	**8**	**40**
Індивідуальне завдання	20				20
Усього	**165**	**36**	**-**	**24**	**105**

5. Теми семінарських занять

№ з/п	Назва теми	Кількість годин
1	Не передбачено навчальним планом	

6. Теми практичних занять

№ з/п	Назва теми	Кількість годин
1	Не передбачено навчальним планом	

7. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
		Денна форма навчання
1	Електронні ключі для захисту інформації (eToken)	4
2	Антивірусні та антишпигунські програми та пакети (Avira Free Antivirus, NOD 32)	4
3	Електронний цифровий підпис та печатка	4
4	Симетричний алгоритм шифрування “Калина” ДСТУ 7624:2014	4
5	Шифруюча файлова система EFS (Windows 11)	2
6	Захист інформації у операційній системі Windows. Протокол Kerberos	2
7	Асиметричний алгоритм шифрування RSA	4
	Разом	24

8. Самостійна робота

№ з/п	Назва теми	Кількість годин
		Денна форма навчання
1	Історія розвитку криптографії	8
2	Фізичний захист ПК. Термінологія з захисту інформації	8
3	Алгоритми шифрування DSA, MD4, MD5. Аналіз криптографічної стійкості алгоритмів шифрування. Протокол ЕЦП Ель-Гамаля	8
4	Оптимізація ДСТУ 7624:2014 на мові високого рівня	8
5	Локальна аутентифікація користувача у операційній системі Windows	8
6	Класифікація комп’ютерних вірусів	5
7	Вибір алгоритму ПДВЧ	10
8	Огляд функцій інтерфейсу CryptoAPI	10
9	Криптографічний захист прикладного рівня	10
10	Методологія побудови надійних ЗКЗІ	10
11	Індивідуальне завдання	20
	Разом	105

9. Індивідуальні завдання

Виконання РР на тематику «Криптографічні методи захисту інформації».

10. Методи навчання

Проведення аудиторних лекцій, лабораторних занять, індивідуальні консультації (при необхідності), самостійна робота студентів за матеріалами, опублікованими кафедрою (методичні посібники) та іншими матеріалами, в тому числі електронними.

11. Методи контролю

Проведення поточного контролю, контроль лабораторних робіт, модульний контроль, 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	Кількість занять	Сумарна кількість балів
Змістовний модуль 1			
Робота на лекціях	0	12	0
Виконання і захист лабораторних робіт	0...5	4	0...20
Модульний контроль	0…20	1	0…20
Змістовний модуль 2			
Робота на лекціях	0	6	0
Виконання і захист лабораторних робіт	0...5	3	0...15
Модульний контроль	0…20	1	0…20
Виконання і захист РР	0…25		0…25
Усього за семестр			**0…100**

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 3 теоретичних запитань. За повну правильну відповідь на два перших запитання студент отримує по 33 бали. За повну правильну відповідь на останнє запитання –34 бали.

12.2. Якісні критерії оцінювання

Необхідний обсяг знань для одержання позитивної оцінки:

- місце і роль захисту інформації у програмному забезпеченні ІУС;
- структура, принципи організації та функціонування сучасних систем захисту інформації;
- симетричні та асиметричні алгоритми шифрування;
- інструменти захисту інформації;
- історію розвитку криптографії;

- класифікацію вірусів.

Необхідний обсяг вмінь для отримання позитивної оцінки:
- використовувати принципи захисту інформації при проектуванні ІУС;
- застосовувати сучасні алгоритми шифрування у захисті даних в ІУС;
- будувати модель загроз технологічної безпеки.

12.3 Критерії оцінювання роботи студента протягом семестру
Задовільно (60-74). Мати мінімум знань та умінь. Відпрацювати та захистити всі лабораторні роботи та домашні завдання (РР). Вміти самостійно давати характеристику та описувати засоби захисту інформації. Знати класифікацію вірусів. Виявляти в структурі ПЗ програмні закладки.
Добре (75-89). Твердо мати мінімум знань, виконати усі завдання. Показати вміння виконувати та захищати всі лабораторні роботи в обумовлений викладачем строк з обґрунтуванням рішень та заходів, які запропоновано у роботах. Вміти використовувати принципи захисту інформації при проектуванні ІУС. Застосовувати сучасні алгоритми шифрування у захисті даних в ІУС.
Відмінно (90-100). Повно знати основний та додатковий матеріал. Знати усі теми. Орієнтуватися у підручниках та посібниках. Вміти використовувати принципи захисту інформації при проектуванні ІУС. Застосовувати сучасні алгоритми шифрування у захисті даних в ІУС. Будувати модель загроз технологічної безпеки. Безпомилково виконувати та захищати всі лабораторні роботи в обумовлений викладачем строк з докладним обґрунтуванням рішень та заходів, які запропоновано у роботах.

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

Сайт дистанційного навчання університету «Ментор» [Електронний ресурс]. – Режим доступу: https://mentor.khai.edu/course/view.php?id=1306

14. Рекомендована література

Базова

1. Захист інформації в комп’ютерних системах: підручник / В.Д. Козюра, В.О. Хорошко, М.Є. Шелест, Ю.М. Ткач, О.О. Балюнов. – Ніжин: ФОП Лук'яненко В.В., ТПК «Орхідея», 2020. -236 с.
2. Захист систем електронних комунікацій : навч. посіб. / В.О. Хорошко, О.В. Криворучко, М.М. Браіловський та ін. – Київ : Київ. нац. торг.-екон. ун-т, 2019. - 164 с.
3. Інформаційна безпека. Підручник / В. В. Остроухов, М. М. Присяжнюк, О. І. Фармагей, М. М. Чеховська та ін.; під ред. В. В. Остроухова – К.: Видавництво Ліра-К, 2021. – 412 с.
4. Кібербезпека : сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. / С. Е. Остапов, С. П. Євсеєв, О.Г. Король. – Львів: «Новий Світ 2000», 2020 . – 678 с.

Допоміжна

1. Tanenbaum, E. S., Boss, H. J. Modern Operating Systems, 4th Edition. - Pearson Higher Education, 2015. – 1120p.
2. Шеховцов В.А. Операційні системи. – К.: Видавнича група BHV, 2005. – 576 с.
3. ДСТУ 7564:2014. Інформаційні технології. Криптографічний захист інформації. Функція хешування. – Чинний з 29.12.2014 р. – ПАТ «Інститут інформаційних технологій» Мінекономрозвитку України, 2016. – 228 с.
4. Горбенко І.Д., Гріненко Т.О. Захист інформації в інформаційно-телекомунікаційних системах: Навч. посібник. Ч.1. Криптографічний захист інформації – Харків: ХНУРЕ, 2004. – 368 с.
5. Тарнавський Ю. А. Технології захисту інформації: підручник / Ю.А. Тарнавський. – Київ: КПІ ім. Ігоря Сікорського, 2018. – 162 с.
6. Остапов С.Е. Технології захисту інформації: навчальний посібник / С.Е. Остапов, С.П. Євсеєв, О.Г. Король. – Х.: ХНЕУ, 2013. – 476 с.
7. ДСТУ 7624:2014. Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення. – Чинний з 29.12.2014 р. ПАТ «Інститут інформаційних технологій» Мінекономрозвитку України, 2016. – 228 с.
8. Кузнецов О. О. Захист інформації в інформаційних системах: навч. посіб. / О.О. Кузнецов, С.П. Євсеєв, О.Г. Король. – Харків: ХНЕУ, 2011. – 510 с.

15. Інформаційні ресурси

1. Сайт науково-технічної бібліотеки університету [Електронний ресурс]. – Режим доступу: http://library.khai.edu.
2. Сайт Державної служби спеціального зв'язку та захисту інформації України [Електронний ресурс]. – Режим доступу: https://cip.gov.ua/ua