МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АЕРОКОСМІЧНИЙ УНІВЕРСИТЕТ
ІМ. М. Є. ЖУКОВСЬКОГО
«ХАРКІВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»

КАФЕДРА ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
ІМ. О.О. ЗЕЛЕНСЬКОГО (№ 504)

«ЗАТВЕРДЖУЮ»
Гарант освітньої програми

(підпис) Олексій РУБЕЛЬ
(ініціали та прізвище)

31 серпня 2023 р.

РОБОЧА ПРОГРАМА ОБОВ'ЯЗКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Захист інформації в інфокомунікаціях
(назва навчальної дисципліни)

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

Спеціальність: 126 «Інформаційні системи і технології»
(код і найменування спеціальності)

Освітня програма: «Штучний інтелект та інформаційні системи»
(найменування освітньої програми)

Форма навчання: денна

Рівень вищої освіти: перший (бакалаврський)

Харків 2023 рік

Розробник: Єремеєв О.І., доцент каф. 504, к.т.н.
(прізвище та ініціали, посада, науковий ступінь і вчене звання) (підпис)

Робочу програму розглянуто на засіданні кафедри
інформаційно-комунікаційних технологій ім. О.О. Зеленського
(назва кафедри)

Протокол № 1 від 31 серпня 2023 р.

Завідувач кафедри д.т.н., професор (підпис) Володимир ЛУКІН
(науковий ступінь і вчене звання) (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 – 4,5</td><td rowspan="11">Галузь знань
12 «Інформаційні технології»
(шифр і найменування)

Спеціальність
126 «Інформаційні системи і технології»
(код і найменування)

Освітня програма
«Штучний інтелект та інформаційні системи»
(найменування)

Рівень вищої освіти:
перший (бакалаврський)</td><td>Обов’язкова</td></tr>
<tr><td>Кількість модулів – 1</td><td>Навчальний рік</td></tr>
<tr><td>Кількість змістовних модулів – 2</td><td>2023/2024</td></tr>
<tr><td>Індивідуальне завдання не передбачено навчальним планом
(назва)</td><td>Семестр</td></tr>
<tr><td rowspan="2">Загальна кількість годин – 56/135</td><td>5-й / 3-й**</td></tr>
<tr><td>Лекції*</td></tr>
<tr><td rowspan="6">Кількість тижневих годин для денної форми навчання:
аудиторних – 3,5
самостійної роботи здобувача– 4,9</td><td>32 години</td></tr>
<tr><td>Практичні*</td></tr>
<tr><td>24 години</td></tr>
<tr><td>Лабораторні*</td></tr>
<tr><td>0 годин</td></tr>
<tr><td>Самостійна робота</td></tr>
<tr><td>79 годин</td><td>Вид контролю</td></tr>
<tr><td>модульний контроль, іспит</td></tr>
</table>

Співвідношення кількості годин аудиторних занять до самостійної роботи становить: **56 / 79**.

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

** Скорочений термін навчання (3 роки)

2. Мета та завдання навчальної дисципліни

Мета вивчення: набуття студентами знань і вмінь, використання їх у своїй практичній роботі, пов'язаній з шифруванням симетричними шифрами, шифруванням з відкритим ключем, шифруванням одноразовими блокнотами та скремблерами, використанням цифрових електронних підписів, схем розподілення секрету, технічними засобами захисту інформації, протоколами аутентифікації, захистом інформації у обчислювальних мережах.

Завдання: вивчення сучасних програмно-алгоритмічних та апаратних методів захисту інформації.

Компетентності, які набуваються:

загальні компетентності: здатність застосовувати знання у практичних ситуаціях; здатність до розуміння предметної області та професійної діяльності; здатність до пошуку, оброблення та узагальнення інформації з різних джерел.

фахові компетентності: здатність застосовувати стандарти в області інформаційних систем та технологій при розробці функціональних профілів, побудові та інтеграції систем, продуктів, сервісів і елементів інфраструктури організації; здатність проектувати, розробляти та використовувати засоби реалізації інформаційних систем, технологій та інфокомунікацій (методичні, інформаційні, алгоритмічні, технічні, програмні та інші); здатність оцінювати та враховувати економічні, соціальні, технологічні та екологічні фактори на всіх етапах життєвого циклу інфокомунікаційних систем; здатність використовувати сучасні інформаційні системи та технології (виробничі, підтримки прийняття рішень, інтелектуального аналізу даних та інші), методики й техніки кібербезпеки під час виконання функціональних завдань та обов'язків; здатність до аналізу, синтезу і оптимізації інформаційних систем та технологій з використанням математичних моделей і методів; здатність управляти та користуватися сучасними інформаційно-комунікаційними системами та технологіями (у тому числі такими, що базуються на використанні Інтернет)

Очікувані результати навчання: вміння застосовувати знання фундаментальних і природничих наук, системного аналізу та технологій моделювання, стандартних алгоритмів та дискретного аналізу при розв'язанні задач проектування і використання інформаційних систем та технологій; вміння використовувати базові знання інформатики й сучасних інформаційних систем та технологій, навички програмування, технології безпечної роботи в комп'ютерних мережах, методи створення баз даних та інтернет-ресурсів, технології розроблення алгоритмів і комп'ютерних програм мовами високого рівня із застосуванням об'єктно-орієнтованого програмування для розв'язання задач проектування і використання інформаційних систем та технологій; застосовувати правила оформлення проектних матеріалів інформаційних систем та технологій, знати склад та послідовність виконання проектних робіт з урахуванням вимог відповідних нормативно-правових документів для запровадження у професійній діяльності.

Пререквізити - "Дискретна математика", "Алгоритми і структури даних"

Кореквізити - "Адміністрування інформаційних систем", "Технології неперервної інтеграції і розгортання інформаційних систем"

3. Зміст навчальної дисципліни

Модуль 1.

Змістовний модуль 1. Захист інформації і забезпечення конфіденційності

Тема 1. Проблема захисту інформації. Предмет вивчення і задачі дисципліни. Інформація та проблема її захисту в інформаційно-комунікаційних системах. Домени і комплексний захист. Куб кібербезпеки. Основні відомості про три виміри куба кібербезпеки. Захист інформації з давніх часів - класичні алгоритми шифрування.

Тема 2. Типові загрози та злочинці. Базові визначення. Джерела загроз. Злочинці. Загрози та їх класифікація. Вразливості. Загрози підвищеної складності. Призначення і методологія атак. Інструменти атак.

Тема 3. Основи мереж. Моделі мереж. Еталонна модель OSI та її рівні. Основні мережні протоколи. Функції і заголовки транспортного рівня. Функції і заголовки мережного рівня. Функції і заголовки канального рівня. Мережне обладнання. Інструменти практичної частини. Jupyter Notebook. Основи формування та управління пакетами в Scapy.

Тема 4. Мережні атаки. Атаки та загрози мережі. Розвідувальні атаки. Атаки доступу. Атаки "відмова в обслуговуванні". Методи приховування. Атаки на фізичному та канальному рівні. Атаки на мережному рівні. Атак на транспортному рівні. Атаки на бездротові мережі. Атаки на рівні додатків. Атаки на віддалені служби. Вразливості ПК. Атаки у віртуальному середовищі. Типи шкідливого програмного забезпечення. Обман та методи обману. Соціальна інженерія.

Тема 5. Управління доступом і методи приховування інформації. Конфіденційність. Контроль доступу. Аутентифікація, авторизація та аудит. Методи аутентифікації. Авторизація та списки контролю доступу. Звітність та моніторинг. Типи, системи та засоби контролю доступу. Стратегії контролю доступу. Приховування даних. Маскування даних. Стеганографія. Обфускація даних.

Тема 6. Основи криптографії. Криптографія і вимоги до алгоритмів шифрування. Складність криптографічних алгоритмів. Класифікація алгоритмів шифрування, їх особливості. Математичні основи криптографії і базові операції. Одноразові блокноти. Скремблери.

Тема 7. Симетричні алгоритми шифрування. Блокові і потокові симетричні шифри. Мережа Фейстеля. Режими роботи ECB, CBC, CFB та OFB. Стандарти симетричного шифрування DES, AES, TEA, "Калина" та інші. Шифрування засобами Python.

Тема 8. Алгоритми шифрування з відкритим ключем. Принципи та особливості алгоритмів з відкритим ключем. Математичні основи цілочисленної арифметики великих чисел. Метод обміну секретним ключем Діффі-Геллмана. Вимоги до шифрування з відкритим ключем. Асиметричний криптоалгоритм RSA. Асиметричний криптоалгоритм Ель-Гамаля. Асиметричне шифрування засобами Python.

Модульний контроль

Модуль 2.

Змістовний модуль 2. Забезпечення цілісності та доступності даних. Рекомендації щодо забезпечення безпеки інформації.

Тема 1. Забезпечення цілісності даних. Засоби контролю цілісності даних. Функція хешування, її властивості. Додавання солі та запобігання атак. Криптографічні алгоритми хешування. Електронний цифровий підпис та законодавство. Як працює технологія цифрового підпису. Алгоритми цифрового підпису. Кваліфікований електронний підпис в Україні. Створення КЕП ("Дія.Підпис" та інші), їх застосування. Атака днів народження. Цифрові сертифікати та їх валідація. Цілісність баз даних. Вимоги до цілісності баз даних

Тема 2. Управління ключами. Створення, накопичення, розподіл. Рандомізація повідомлень. Псевдовипадкові послідовності. Метод лінійного конгруенту. Лінійна рекурентна послідовність. Метод Фібоначчі з запізненнями. Метод XorShift. Криптостійкі генератори на основі односторонніх функцій. Генератор ANSI X9.17. Комбінування алгоритмів генерації методом Макларена-Марсал'ї. Системи керування ключами. Сертифікація при розподілі ключів.

Тема 3. Криптоаналіз. Прості числа в криптосистемах.

Прості числа в криптосистемах. Решето Ератосфена. Генерація простих чисел. Точна перевірка простоти чисел. Теорема Вільсона. Тест Міллера-Рабіна. Метод факторизації Ферма. Факторизація методом двійкового решета.

Тема 4. Забезпечення доступності даних. Концепція п'яти дев'яток. Заходи для поліпшення доступності. Керування активами. Захист в глибину. Надмірність. Системна стійкість. Реагування на інциденти. Технології реагування на інциденти. Відновлення після катастроф. Планування відновлення та безперервності бізнесу.

Тема 5. Організаційні заходи захисту інформації. Засоби протидії кіберзлочинності. Стандарти, рекомендації, закони. Політики та процедури кібербезпеки. Модель кібербезпеки ISO та її використання. Навчання персоналу. Захист від користувачів та витоку інформації.

Тема 6. Технічні засоби захисту інформації. Засоби захисту: програмні, апаратні, мережеві та хмарні. Мережеві технології захисту (MAC, VLAN, ACL). Міжмережеві екрани. Сиситеми спостереження та реагування IDS/IPS. Віртуальні приватні мережі VPN. Укріплення захисту мережі. Захист систем та пристроїв. Захист бездротових та мобільних пристроїв. Захист додатків та даних. Керування вмістом і образами. Фізичний захист робочих станцій. Безпечний віддалений доступ. Укріплення захисту серверів. Фізичний захист серверів. Фізичний контроль доступу. Засоби безпеки. Комплексний захист на при

Тема 7. Хмара. Комплексний захист хмарних сховищ. Класифікація: tier та вимоги. Приклади організації центрів обробки даних. Критична інфраструктура. Резервування на всіх рввнях. Автоматихзація та віртуалізація. Заходи безпеки.

Тема 8. Проектування системи захисту. Проектування системи захисту. Визначення цілей та завдань захисту інформації. Визначення вимог та обмежень щодо інформації. Власні сервера чи хмара. Забезпечення організаційних заходів безпеки. Контроль доступу. Планування відмовостійкості. Налаштування захисту. Постійний моніторинг.

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
Модуль 1					
Змістовний модуль 1. Захист інформації і забезпечення конфіденційності					
Тема 1. Проблема захисту інформації	9	2	2	-	5
Тема 2. Типові загрози та злочинці	15	2	4	-	9
Тема 3. Основи мереж	4	2	-		2
Тема 4. Мережні атаки	18	4	4	-	10
Тема 5. Управління доступом і методи приховування інформації.	4	2	-	-	2
Тема 6. Основи криптографії	4	2	-	-	2
Тема 7. Симетричні криптоалгоритми	15	2	4	-	9
Тема 8. Алгоритми шифрування з відкритим ключем	9	1	2	-	6
Модульний контроль	1	1	-	-	-
Разом за змістовним модулем 1	79	18	16	-	45
Змістовний модуль 2. Забезпечення цілісності та доступності даних. Рекомендації щодо забезпечення безпеки інформації.					
Тема 1. Забезпечення цілісності даних	20	4	4	-	12
Тема 2. Управління ключами. Створення, накопичення, розподіл.	3	1	-	-	2
Тема 3. Криптоаналіз. Прості числа в криптосистемах.	3	1	-	-	2
Тема 4. Забезпечення доступності даних.	4	2	-		2
Тема 5. Організаційні заходи захисту інформації	4	2	-	-	2

Тема 6. Технічні засоби захисту інформації	3	1	-	-	2
Тема 7. Хмара	3	1	-	-	2
Тема 8. Проектування системи захисту	15	1	4	-	10
Модульний контроль	1	1	-	-	-
Разом за змістовним модулем 2	56	14	8	-	34
Усього годин	**135**	**32**	**24**	**-**	**79**

5. Теми семінарських занять

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

6. Теми практичних занять

№ п/п	Назва теми	Кількість годин
1	Злом моноалфавітного підставного шифру методом частотної атаки	2
2	Оцінка стійкості пароля до зламу	4
3	Пошук мережевих вразливостей кінцевого пристрою	4
4	Мережа Фейстеля	2
5	Симетричне шифрування засобами Python	2
6	Шифрування з відкритим ключем засобами Python	2
7	Перевірка цілісності засобами Python	4
8	Перевірка надійності захисту робочої станції	4
	Разом	24

7. Теми лабораторних занять

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

8. Самостійна робота

№ п/п	Назва теми	Кількість годин
1	Опрацювання матеріалу лекцій	24
2	Підготовка до практичних робіт	24
3	Опрацювання матеріалів та результатів отриманих на практичних заняттях	27
4	Підготовка до модульного контролю	4
	Разом	79

9. Індивідуальні завдання

Не передбачено навчальним планом

10. Методи навчання

При викладанні курсу використовуються наступні навчальні методи:
– демонстрація;
– ілюстрація;
– розповідь;
– спостереження;
– дослідження;
– лабораторна робота.

11. Методи контролю

Для контролю успішності в даному курсі використано:
- поточний контроль (на практичних заняттях);
- модульний контроль за змістовними модулями;
- семестровий 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…0,5	8	0…4
Виконання і захист практичних робіт	0...8	6	0...48
Модульний контроль	0…18	1	0…18
Змістовний модуль 2			
Робота на лекціях	0…0,5	8	0…4
Виконання і захист практичних робіт	0...8	1	0...8
Модульний контроль	0…18	1	0…18
Усього за семестр			**0…100**

Білет для іспиту складається з з двадцяти тестових теоретичних та чотирьох практичних питань. Максимальна сума балів за за теоретичні питанні - 60 балів, за практичні - 40 балів.

Критерії оцінювання роботи здобувача протягом семестру

Задовільно (60-74). Показати мінімум знань та умінь. Захистити всі індивідуальні завдання та здати тестування. Знати синтаксис мови програмування Python. Мати уявлення про типові загрози безпеці інформації та міри протидії. Вміти застосовувати наведені рекомендації.

Добре (75-89). Твердо знати мінімум, захистити всі індивідуальні завдання, виконати всі КР, здати тестування та поза аудиторну самостійну роботу. Уміти окрім наведених базових знань реалізувати базові задачі аналізу мережевої безпеки та шифрування даних, коректно застосовувати відповідно до поставлених задач алгоритми шифрування та хешування, що забезпечать необхідний рівень стійкості.

Відмінно (90-100). Здати всі контрольні точки з оцінкою «відмінно». Досконально знати всі теми та вміти застосовувати їх.

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. Пономаренко Н. Н. Защита информации в телекоммуникационных системах : учеб. пособие по решению задач / Н. Н. Пономаренко ; М-во образования и науки Украины, Нац. аэрокосм. ун-т им. Н.Е. Жуковского "Харьк. авиац. ин-т". - Х. : Нац. аэрокосм. ун-т им. Н. Е. Жуковского "Харьк. авиац. ин-т", 2015. - 40 с.

2. Криптология и защита информации : учеб. пособие / Л. И. Курпа, Ю. А. Щербакова, Н. В. Драшпуль, Н. А. Украинец [и др.] ; М-во образования и науки, молодежи и спорта Украины, Нац. аэрокосм. ун-т им. Н. Е. Жуковского "Харьк. авиац. ин-т". - Х. : Нац. аэрокосм. ун-т им. Н. Е. Жуковского "Харьк. авиац. ин-т", 2012. - 84 с. – электронное издание.

3. Лысенко И. В. Математика эллиптических кривых и криптография : учеб. пособие / И. В. Лысенко ; М-во образования и науки Украины, Нац. аэрокосм. ун-т им. Н. Е. Жуковского "Харьк. авиац. ин-т". - Харьков : Нац. аэрокосм. ун-т им. Н. Е. Жуковского "Харьк. авиац. ин-т", 2016. - 52 с.

4. Сайт кафедри 504, http://k504.khai.edu, на якому розміщено НМКД вибіркової навчальної дисципліни “Телекомунікаційні т інформаційні мережі”: робоча програма; конспект лекцій; навчальний посібник з лабораторного практикуму; питання та тести контрольних заходів; електронні презентації лекцій.

Навчально-методичне забезпечення дисципліни "Захист інформації в телекомунікаційних системах" для бакалаврів / Нац. аерокосм. ун-т ім. М. Є. Жуковського "Харків. авіац. ін-т" ; розроб. О. І. Єремеєв. - Харків, 2020. - 301 с . - http://library.khai.edu/library/fulltexts/doc/_A_A_Zahist_Informaciyi11.pdf

14. Рекомендована література

Базова

1. Інформаційна безпека: навч. посібник / Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник, А. П. Бондарєв, С. С. Войтусік та ін. - Львів: Видавництво Львівської політехніки, 2019. - 580 с.
2. Остапов С. Е., Євсеєв С. П., Король О. Г. Технології захисту інформації. Посібник. – К.: Родовід, 2014. – 428 с
3. Криптологія у прикладах, тестах і задачах : навч. посіб. / Т. В. Бабенко [та ін.] ; Держ. ВНЗ "Нац. гірн. ун-т". - Дніпропетровськ : НГУ, 2013. - 318 с.
4. Основи захисту інформації в телекомунікаційних та комп’ютерних мережах / Л. Л. Гончарова, А. Д. Возненко, О. І. Стасюк, Ю. О. Коваль. – К., 2013. – 435 с.

Допоміжна

1. Євсеєв С. П., Шматко О. В., Король О. Г. Кібербезпека: криптографія з Python: навч. посібник. - Львів: Видавництво “Новий світ - 2000”, 2021 - 120 с.

15. Інформаційні ресурси

1.Науково-технічна бібліотека ХАІ [Електронний ресурс] - Режим доступу: http://library.khai.edu - 20.06.2017.

2. https://netacad.com