Міністерство освіти і науки України
Національний аерокосмічний університет
«Харківський авіаційний інститут»

Кафедра Інформаційно-комунікаційних технологій ім. О.О. Зеленського (№ 504)

ЗАТВЕРДЖУЮ

Гарант освітньої програми

_____ Олег ЄРЕМЕЄВ
(підпис) (ім'я та ПРІЗВИЩЕ)

28 серпня 2025 р.

СИЛАБУС 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 та технології»
(код і найменування спеціальності)

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

Рівень вищої освіти: перший (бакалаврський)

Силабус введено в дію з 01.09.2025

Харків – 2025 р.

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

Силабус навчальної дисципліни розглянуто на засіданні кафедри

Інформаційно-комунікаційних технологій ім. О.О. Зеленського
(назва кафедри)

Протокол № 1 від « 28» серпня 2025 р.

Завідувач кафедри д.т.н., професор _____ Володимир ЛУКІН
(науковий ступінь і вчене звання) (підпис) (ім'я та ПРІЗВИЩЕ)

Погоджено з представником здобувачів освіти:

_____ _____ Віолетта ІЛЬЇНА __
(підпис) (ім'я та ПРІЗВИЩЕ)

1. Загальна інформація про викладача

ПІБ: Єремеєв Олег Ігорович

Посада: доцент

Науковий ступінь: к.т.н.

Вчене звання: доцент

Перелік дисциплін, які викладає:
Алгоритми і структури даних
Бази даних
Захист інформації в інфокомунікаціях
Автоматизація та безпека корпоративних мереж

Напрями наукових досліджень:
Обробка зображень, цифрова обробка зображень, аналіз зображень, оцінка візуальної якості зображень, стиснення зображень, класифікація, штучні нейронні мережі, машинне навчання, навчання без учителя, глибинне навчання

Контактна інформація:
o.ieremeiev@khai.edu

2. Опис навчальної дисципліни

Форма здобуття освіти	Денна
Семестр	5 - й
Мова викладання	Українська
Тип дисципліни	Обов’язкова
Обсяг дисципліни: кредити ЄКТС/ кількість годин	4,5 кредитів ЄКТС / 135 годин (56 аудиторних, з яких: лекції – 32, практичні – 24; СРЗ – 79)
Види навчальної діяльності	Лекції, практичні заняття, самостійна робота
Види контролю	Поточний контроль, модульний контроль, семестровий контроль – модульний контроль, іспит
Пререквізити	«Дискретна математика», «Алгоритми і структури даних»

3. Мета та завдання навчальної дисципліни, переліки компетентностей та очікуваних результатів навчання

Мета – 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:

Інтегральна компетентність:

Здатність розв’язувати складні спеціалізовані задачі та практичні проблеми в області інформаційних систем та технологій, або в процесі навчання, що характеризуються комплексністю та невизначеністю умов, які потребують застосування теорій та методів інформаційних технологій.

Загальні компетентності (ЗК)

Після закінчення цієї програми здобувач освіти буде здатен:

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

Спеціальні компетентності

Після закінчення цієї програми здобувач освіти буде здатен:

застосовувати стандарти в області інформаційних систем та технологій при розробці функціональних профілів, побудові та інтеграції систем, продуктів, сервісів і елементів інфраструктури організації; проектувати, розробляти та використовувати засоби реалізації інформаційних систем, технологій та інфокомунікацій (методичні, інформаційні, алгоритмічні, технічні, програмні та інші); оцінювати та враховувати економічні, соціальні, технологічні та екологічні фактори на всіх етапах життєвого циклу інфокомунікаційних систем; 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; до аналізу, синтезу і оптимізації інформаційних систем та технологій з використанням математичних моделей і методів; управляти та користуватися сучасними інформаційно-комунікаційними системами та технологіями (у тому числі такими, що базуються на використанні Інтернет)

Програмні результати навчання:

У результаті вивчення навчальної дисципліни студент повинен:

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; 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.

4. Зміст навчальної дисципліни

МОДУЛЬ 1

Змістовний модуль 1. Захист інформації і забезпечення конфіденційності

Тема 1. Проблема захисту інформації та типові загрози

Мета: ознайомити студентів з основними проблемами захисту інформації і дотичних до неї активами (люди, обладнання, ресурси, дані), а також розглянути найбільш поширені загрози для мереж і кінцевих пристроїв, соціальної інженерії.

Теми лекцій:

1. Проблема захисту інформації.
2. Типові загрози та злочинці.
3. Основи мереж і управління пакетами в Scapy.
4. Атаки на мережі і кінцеві пристрої

Теми практичних робіт:

1. Злом моноалфавітного підставного шифру методом частотної атаки.
2. Оцінка стійкості пароля до зламу.
3. Пошук мережевих вразливостей кінцевого пристрою.

Самостійна робота здобувачів освіти: опрацювання матеріалу лекцій, підготовка до захисту практичних робіт.

Тема 2. Конфіденційність інформації та основи криптографії

Мета: ознайомити студентів з методами та засобами забезпечення конфіденційності інформації, надати теоретичні відомості щодо криптографії

в цілому та основних алгоритмів шифрування і навчити застосовувати їх на практиці.

Теми лекцій:
1. Управління доступом і методи приховування інформації.
2. Основи криптографії.
3. Симетричні алгоритми шифрування.
4. Алгоритми шифрування з відкритим ключем.

Теми практичних робіт:
1. Мережа Фейстеля
2. Симетричне шифрування засобами Python
3. Шифрування з відкритим ключем засобами Python

Самостійна робота здобувачів освіти: опрацювання матеріалу лекцій, підготовка до захисту практичних робіт.

Модульний контроль 1

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

Тема 1. Забезпечення цілісності та доступності даних

Мета: ознайомити студентів з принципами забезпечення цілісності і доступності даних та основними методами і засобами їх реалізації.

Теми лекцій:
1. Забезпечення цілісності даних.
2. Управління ключами. Створення, накопичення, розподіл.
3. Криптоаналіз. Прості числа в криптосистемах.
4. Забезпечення доступності даних.

Теми практичних робіт:
1. Перевірка цілісності засобами Python

Самостійна робота здобувачів освіти: опрацювання матеріалу лекцій, підготовка до захисту практичних робіт.

Тема 2. Забезпечення безпеки інформації.

Мета: ознайомити студентів з основними організаційними заходами та технічними засобами захисту інформації, комплексним захистом на прикладі хмарних сховищ, а також надати основні принципи та методи проектування систем захисту.

Теми лекцій:
1. Організаційні заходи захисту інформації.

2. Технічні засоби захисту інформації.
3. Хмари та датацентри.
4. Проектування системи захисту.

Теми практичних робіт:
1. Перевірка надійності захисту робочої станції

Самостійна робота здобувачів освіти: опрацювання матеріалу лекцій, підготовка до захисту практичних робіт.
Модульний контроль 2

5. Індивідуальні завдання

Не передбачено навчальним планом.

6. Методи навчання

При викладанні курсу використовуються наступні навчальні методи:

- демонстрація;
- ілюстрація;
- розповідь;
- спостереження;
- дослідження;
- практична робота;
- виконання завдань.

7. Методи контролю

1) поточний контроль (оцінювання роботи студентів на практичних заняттях);
2) модульний контроль за змістовними модулями;
3) семестровий контроль у вигляді іспиту.

8. Критерії оцінювання та розподіл балів, які отримують здобувачі освіти

Таблиця 8.1 – Розподіл балів, які отримують здобувачі освіти

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...7	6	0...42
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...7	2	0...14
Модульний контроль	0…18	1	0…18
Усього за семестр			**0…100**

Семестровий контроль (іспит) проводиться у разі відмови здобувача освіти від балів підсумкового контролю й за наявності допуску до іспиту. Під час складання семестрового іспиту здобувач освіти має можливість отримати максимум 100 балів.

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

Таблиця 8.2 – Шкали оцінювання: бальна і традиційна

Сума балів	Оцінка за традиційною шкалою	
	Іспит, диференційний залік	Залік
90 – 100	Відмінно	Зараховано
75 – 89	Добре	
60 – 74	Задовільно	
0 – 59	Незадовільно	Не зараховано

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.

9. Політика навчального курсу

Відвідування занять та відпрацювання пропусків.

Курс має інтерактивний характер, тому обов'язковою є присутність на лекційних, практичних заняттях. У разі пропуску занять з поважних причин (лікарняний, академічна мобільність, інші підтверджені обставини) здобувач освіти зобов'язаний протягом тижня узгодити з викладачем індивідуальний графік відпрацювання. Пропущені заняття відпрацьовуються на консультаціях шляхом усної співбесіди за темами заняття або у вигляді індивідуального письмового завдання.

Виконання завдань та контрольні заходи.

Невиконані завдання повинні бути здані в строки, визначені викладачем. Прострочені завдання можуть бути прийняті з пониженням оцінки або у формі додаткового індивідуального завдання.

Академічна доброчесність.

Усі учасники освітнього процесу мають дотримуватися вимог Положення про академічну доброчесність Національного аерокосмічного університету «Харківський авіаційний інститут» (https://khai.edu/assets/files/polozhennya/polozhennya-pro-akademichnu-dobrochesnist.pdf). Очікується, що письмові роботи здобувачів будуть оригінальними та матимуть належні посилання на використані джерела. Використання чужих ідей без цитування, фабрикація чи фальсифікація даних, списування, втручання в роботу інших студентів розцінюються як академічна недоброчесність. Виявлення плагіату є підставою для незарахування роботи незалежно від його обсягу.

Вирішення конфліктів та етична поведінка.

Усі спірні ситуації, пов'язані з корупційними діями, конфліктом інтересів, проявами дискримінації, сексуальними домаганнями чи іншими формами порушення етики, вирішуються відповідно до положень Кодексу етичної поведінки Національного аерокосмічного університету «Харківський авіаційний інститут» (https://khai.edu/ua/university/normativna-baza/ustanovchi-dokumenti/kodeks-etichnoi-povedinki/).

10. Методичне забезпечення

1. Сайт кафедри 504, http://k504.khai.edu, на якому розміщено НМКД вибіркової навчальної дисципліни "Захист інформації в інфокомунікаціях": робоча програма; конспект лекцій; навчальний

посібник з лабораторного практикуму; питання та тести контрольних заходів; електронні презентації лекцій.

2. 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.-301с.
http://library.khai.edu/library/fulltexts/doc/_A_A_Zahist_Informaciyi11.pdf

11. Рекомендована література

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

12. Інформаційні ресурси

1. Науково-технічна бібліотека ХАІ [Електронний ресурс] - Режим доступу: https://library.khai.edu - 20.06.2025.
2. https://netacad.com