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

Кафедра «Комп'ютерних систем, мереж і кібербезпеки» (№ 503)

ЗАТВЕРДЖУЮ

Гарант освітньої програми

_____ Анатолій Шостак
(підпис) (ім'я та ПРІЗВИЩЕ)

«29» серпня 2025 р.

СИЛАБУС ОБОВ'ЯЗКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Захист інформації в комп'ютерних системах
(назва навчальної дисципліни)

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

Спеціальність: 123 «Комп'ютерна інженерія»
(код і найменування спеціальності)

Освітня програма: «Системне програмування»
(найменування освітньої програми)

Рівень вищої освіти: перший (бакалаврський)

Силабус введено в дію з 01.09.2025

Харків – 2025 р.

Розробник (и): __Андрій Карпенко, ст. викладач, д-р філософії_ _____
(прізвище та ініціали, посада, науковий ступінь і вчене звання) (підпис)

Силабус навчальної дисципліни розглянуто на засіданні кафедри _____

_____
(назва кафедри)

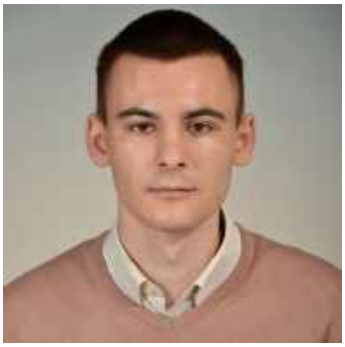
Протокол № 1 від « 29» серпня 2025 р.

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

Погоджено з представником здобувачів освіти:

_____ _____ __Поліна Огарко_____
(підпис) (ім'я та ПРІЗВИЩЕ)

1. Загальна інформація про викладача



ПІБ: Карпенко Андрій Сергійович
Посада: старший викладач
Науковий ступінь: Ph.D.
Вчене звання: відсутнє
Перелік дисциплін, які викладає: захист інформації в комп'ютерних мережах, теоретичні основи криптології, управління інформаційною безпекою, теорія та технології розробки безпечних розподілених систем.
Напрями наукових досліджень: хмарні технології, кібербезпека, тестування програмного забезпечення.
Контактна інформація: *a.karpenko@csn.khai.edu, +380507095250*

2. Опис навчальної дисципліни

Форма здобуття освіти	*Денна, заочна*
Семестр	7-й
Мова викладання	Українська
Тип дисципліни	Обов'язкова
Обсяг дисципліни: кредити ЄКТС/ кількість годин	*денна*: 4 кредитів ЄКТС / 120 годин (64 аудиторних, з яких: лекції – 32, практичні – 32; СРЗ – 56); *заочна*: 4 кредитів ЄКТС / 120 годин (8 аудиторних, з яких: лекції – 4, практичні – 4; СРЗ – 112)
Види навчальної діяльності	Лекції, лабораторні заняття, самостійна робота та розрахункова робота
Види контролю	Поточний контроль, модульний контроль, семестровий контроль – іспит.
Пререквізити	«Теорія інформації і кодування», «Комп'ютерні мережі»

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

Мета – ознайомлення тих, хто навчається, з методологією, основними напрямами, методами і алгоритмами реалізації функцій захисту інформації в комп'ютерних системах та мережах, а також придбанні навичок розрахунку параметрів сучасних криптографічних алгоритмів забезпечення захисту інформації, використанню стеганографічних методів захисту інформації та методам антивірусного захисту.

Завдання – вивчення принципів побудови криптографічних та стеганографічних алгоритмів забезпечення захисту інформації, антивірусного захисту, а також базових положень щодо реалізації комплексної системи захисту інформації в установі (підприємстві).

Компетентності, які набуваються:

Інтегральна компетентність:

Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми під час професійної діяльності в комп'ютерній галузі або навчання, що передбачає застосування теорій та методів комп'ютерної інженерії і характеризується комплексністю та невизначеністю умов.

Загальні компетентності

Після закінчення цієї програми здобувач освіти буде здатен:

(ЗК1) здатність до абстрактного мислення, аналізу і синтезу.

(ЗК2) здатність вчитися і оволодівати сучасними знаннями.

(ЗК9) здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.

(ЗК10) здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.

Спеціальні компетентності

Після закінчення цієї програми здобувач освіти буде здатен:

(ФК1) Здатність застосовувати законодавчу та нормативноправову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі комп'ютерної інженерії.

(ФК4) здатність забезпечувати захист інформації, що обробляється в комп'ютерних та кіберфізичних системах та мережах з метою реалізації встановленої політики інформаційної безпеки.

(ФК10) здатність здійснювати організацію робочих місць, їхнє технічне оснащення, розміщення комп'ютерного устаткування, використання

організаційних, технічних, алгоритмічних та інших методів і засобів захисту інформації.

(ФК11) Здатність оформляти отримані робочі результати у вигляді презентацій, науково-технічних звітів.

(ФК13) Здатність вирішувати проблеми у галузі комп'ютерних та інформаційних технологій, визначати обмеження цих технологій.

(ФК15) Здатність аргументувати вибір методів розв'язування спеціалізованих задач, критично оцінювати отримані результати, обгрунтовувати та захищати прийняті рішення.

(ФК17) Здатність розробляти, налагоджувати та адмініструвати системи управління контентом (CMS) для веб-застосунків.

Програмні результати навчання:

(ПРН1) Знати і розуміти наукові положення, що лежать в основі функціонування комп'ютерних засобів, систем та мереж.

(ПРН4) Знати та розуміти вплив технічнихих рішень в суспільному, економічному, соціальному екологічному контексті.

(ПРН7) Вміти розв'язувати задачі аналізу та синтезу засобів, характерних для спеціальності.

(ПРН8) Вміти системно мислити та застосовувати творчі здібності до формування нових ідей.

(ПРН9) Вміти застосовувати знання технічних характеристик, конструктивних особливостей, призначення і правил експлуатації програмно-технічних засобів комп'ютерних систем та мереж для вирішення технічних задач спеціальності.

4. Зміст навчальної дисципліни

МОДУЛЬ 1
Змістовний модуль 1. Захист інформації

Тема 1. Основи захисту інформації в комп'ютерних системах

Анотація: Розглядаються основні визначення та термінологія в галузі захисту інформації, загрози інформаційної безпеки, нормативно-правова база та технічні засоби захисту інформації.

Тема лекції 1: Основні визначення, термінологія та загрози інформаційної безпеки

Тема лекції 2: Нормативно-правова база та технічні засоби захисту інформації

Самостійна робота здобувачів: Опрацювання матеріалу лекцій, підготовка до модульного контролю, виконання індивідуальних завдань, проходження тестування за результатами роботи на лекційних заняттях, формування питань до викладача.

Тема 2. Симетричні криптологічні системи

Анотація: Вивчаються основні класи симетричних криптосистем, включаючи шифри перестановки, таблиці що шифрують, систему омофонів, біграмні шифри, шифри складної заміни, багатоалфавітний шифр, систему Віженера та одноразовий блокнот.

Тема лекції 1: Основні класи симетричних криптосистем: шифри перестановки, таблиці що шифрують, система омофонів, біграмні шифри

Тема лекції 2: Шифри складної заміни: багатоалфавітний шифр, система Віженера, одноразовий блокнот

Тема лабораторного заняття 1: Дослідження алгоритму багатоалфавітного шифру

Самостійна робота здобувачів: Опрацювання матеріалу лекцій, підготовка до лабораторного заняття, формування звіту з індивідуальної лабораторної роботи 1, підготовка до захисту лабораторної роботи, проходження тестування за результатами роботи на лекційних та лабораторних заняттях, виконання індивідуальних завдань, підготовка до модульного контролю, формування питань до викладача.

Тема 3. Сучасні алгоритми симетричного шифрування

Анотація: Розглядаються алгоритми блокового шифрування (DES, ДСТУ ГОСТ 28147-2009, AES, ДСТУ 7624:2014), їх характеристики, мережа Фейстела, режими блокового шифрування, а також шифрування методом гамування та побудова потокових шифрів.

Тема лекції 1: Алгоритми блокового шифрування: характеристика, мережа Фейстела, режими блокового шифрування, алгоритми DES, ДСТУ ГОСТ 28147-2009, AES, ДСТУ 7624:2014.

Тема лекції 2: Шифрування методом гамування: процес гамування, конгруентний генератор, генератор на регістрах зсуву, побудова потокових шифрів.

Тема лабораторного заняття 1: Дослідження та порівняльний аналіз алгоритмів DES та AES

Самостійна робота здобувачів: Опрацювання матеріалу лекцій, підготовка до лабораторного заняття, формування звіту з індивідуальної лабораторної роботи 2, підготовка до захисту лабораторної роботи, проходження тестування за результатами роботи на лекційних та лабораторних заняттях, виконання індивідуальних завдань, підготовка до модульного контролю, формування питань до викладача.

Тема 4. Криптосистеми із відкритим ключем

Анотація: Вивчаються теоретичні основи побудови криптосистем із відкритим ключем, концепція таких систем, односпрямовані функції, криптосистеми RSA, Ель Гамаля та на еліптичних кривих.

Тема лекції 1: Теоретичні основи та концепція криптосистем із відкритим ключем, односпрямовані функції.

Тема лекції 2: Криптосистеми із відкритим ключем: RSA, Ель Гамаля, на еліптичних кривих.

Тема лабораторного заняття 1: Дослідження алгоритму RSA

Самостійна робота здобувачів: Опрацювання матеріалу лекцій, підготовка до лабораторного заняття, формування звіту з індивідуальної лабораторної роботи 3, підготовка до захисту лабораторної роботи, проходження тестування за результатами роботи на лекційних та лабораторних заняттях, виконання індивідуальних завдань, підготовка до модульного контролю, формування питань до викладача.

Тема 5. Автентифікація та цифровий підпис

Анотація: Розглядаються задачі автентифікації та автентифікації даних, контроль незмінності масивів даних, виробіток коду виявлення маніпуляцій, цифровий підпис на основі різних криптосистем, функції хешування, багатоадресна автентифікація та обмін ключами.

Тема лекції 1: Задачі автентифікації та автентифікації даних, контроль незмінності масивів даних, виробіток коду виявлення маніпуляцій.

Тема лекції 2: Цифровий підпис.

Тема лабораторного заняття 1: Дослідження алгоритму цифрового підпису

Тема лабораторного заняття 2: Дослідження алгоритму обміну ключами

Самостійна робота здобувачів: Опрацювання матеріалу лекцій, підготовка до лабораторних занять, формування звітів з індивідуальних лабораторних робіт 4 та 5, підготовка до захисту лабораторних робіт, проходження тестування за результатами роботи на лекційних та

лабораторних заняттях, виконання індивідуальних завдань, підготовка до модульного контролю, формування питань до викладача.

Модульний контроль 1

Змістовний модуль 2. Системи захисту інформації

Тема 6. Антивірусний захист

Анотація: Вивчаються загальна характеристика та класифікація комп'ютерних вірусів, їх фізична структура, механізми зараження, різні типи вірусів (файлові, бутові, stealth, поліморфні, макровіруси, мережеві), засоби нейтралізації вірусів, методи захисту та технології виявлення шкідливого коду.

Тема лекції 1: Загальна характеристика, класифікація та типи комп'ютерних вірусів: фізична структура, зараження програми, файлові, бутові, stealth, поліморфні, макровіруси, мережеві віруси

Тема лекції 2: Засоби нейтралізації та методи захисту від комп'ютерних вірусів: антивіруси, детектори, фаги, вакцини, технології виявлення шкідливого коду, модель системи захисту від шкідливих програм

Тема лабораторного заняття 1: Дослідження можливості використання описаних вразливостей для вбудовування у вірусний код

Самостійна робота здобувачів: Опрацювання матеріалу лекцій, підготовка до лабораторного заняття, формування звіту з індивідуальної лабораторної роботи 6, підготовка до захисту лабораторної роботи, проходження тестування за результатами роботи на лекційних та лабораторних заняттях, виконання індивідуальних завдань, підготовка до модульного контролю, формування питань до викладача.

Тема 7. Стеганографія

Анотація: Розглядаються узагальнена модель стегосистеми, основні програми стеганографії, приховування даних, цифрові водяні знаки, стеганографія з відкритим ключем, різні алгоритми вбудовування інформації в зображення, аудіо та відео сигнали, включаючи методи на основі квантування, фрактального перетворення та стандарту MPEG.

Тема лекції 1: Узагальнена модель стегосистеми, основні програми стеганографії, приховування даних, цифрові водяні знаки, стеганографія з відкритим ключем.

Тема лекції 2: Алгоритми вбудовування інформації в зображення: адитивні алгоритми, алгоритми на основі лінійного вбудовування даних, алгоритми на основі квантування та фрактального перетворення.

Тема лабораторного заняття 1: Дослідження алгоритмів прихованої передачі інформації в текстовому файлі.

Тема лабораторного заняття 2: Дослідження алгоритмів прихованої передачі інформації в нерухомому зображенні.

Самостійна робота здобувачів: Опрацювання матеріалу лекцій, підготовка до лабораторних занять, формування звітів з індивідуальних лабораторних робіт 7 та 8, підготовка до захисту лабораторних робіт, проходження тестування за результатами роботи на лекційних та лабораторних заняттях, виконання індивідуальних завдань, підготовка до модульного контролю, формування питань до викладача.

Модульний контроль 2

5. Індивідуальні завдання

Виконання розрахункової роботи «Розрахунок та аналіз параметрів комплексної системи захисту інформації з використанням криптографічних алгоритмів та стеганографічних методів»

6. Методи навчання

Лекції з елементами інтерактиву (пояснення з використанням презентацій, демонстрація роботи криптографічних алгоритмів, аналіз прикладів застосування методів захисту інформації, міні-опитування для перевірки розуміння матеріалу). Лабораторні заняття – дослідження та реалізація криптографічних алгоритмів (симетричне та асиметричне шифрування, цифровий підпис, стеганографічні методи), порівняльний аналіз алгоритмів, експериментальна перевірка властивостей систем захисту, робота з програмними засобами криптографії та стеганографії. Проєктно-орієнтоване навчання – виконання практичних завдань з розробки та аналізу систем захисту інформації, інтеграція криптографічних та стеганографічних методів у комплексні рішення. Робота в малих групах – колективний аналіз алгоритмів шифрування, обговорення методів захисту від вірусів, спільне вирішення задач з криптоаналізу, обмін досвідом щодо використання стеганографічних технологій. Використання системи онлайн-тестування для перевірки знань з теоретичних основ криптографії, алгоритмів шифрування, методів автентифікації та стеганографії. Самостійна робота – опрацювання матеріалу лекцій, підготовка до лабораторних занять, формування звітів з лабораторних робіт, виконання індивідуальних завдань з розрахунку параметрів криптографічних систем, робота з електронними матеріалами та онлайн-курсами з криптографії та захисту інформації, підготовка до модульних контрольних робіт. Консультації – індивідуальні та групові (очно або онлайн) для підтримки та корекції навчального процесу, допомога у виконанні лабораторних робіт та розрахункових завдань, роз'яснення складних питань криптографії та стеганографії.

7. Методи контролю

Поточний контроль: опитування на лекційних та лабораторних заняттях з основних понять криптографії та захисту інформації; аналіз та порівняння криптографічних алгоритмів; виконання письмових контрольних робіт з окремих розділів курсу (симетричні та асиметричні криптосистеми, алгоритми шифрування, автентифікація та цифровий підпис, антивірусний захист, стеганографія); програмований контроль (тестування, онлайн-тести) з

теоретичних основ та практичних аспектів захисту інформації; оцінювання виконання індивідуальних лабораторних робіт з дослідження алгоритмів шифрування, цифрового підпису, стеганографічних методів; перевірка звітів з лабораторних робіт та їх захист; оцінювання виконання індивідуальних розрахункових завдань з визначення параметрів криптографічних систем.

Модульний контроль: складання модульного контролю з змістового модуля 1 "Криптографія" та змістового модуля 2 "Системи захисту інформації"; перевірка знань з теоретичних основ криптографії, алгоритмів шифрування, методів автентифікації, антивірусного захисту та стеганографії; оцінювання практичних навичок роботи з криптографічними алгоритмами та системами захисту.

Підсумковий контроль: іспит, що включає теоретичні питання з усіх розділів курсу та практичні завдання з аналізу та застосування методів захисту інформації.

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
Модуль 1 Змістовий модуль 1			
Робота на лекціях	0...1	10	0...10
Лабораторні заняття	0...5	5	0...25
Модульний контроль	0…24	1	0…12
Змістовий модуль 2			
Робота на лекціях	0...1	6	0...6
Лабораторні заняття	0...5	3	0...15
Модульний контроль	0…20	1	0…12
Модуль 2			
Розрахункова робота	0…20	1	0…20
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 двох теоретичних і одного практичного запитання. За теоретичні запитання студент отримує до 60 балів (до 30 балів за кожне) , за практичне – до 40 балів. Під час складання семестрового іспиту здобувач має можливість отримати максимум 100 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 освіти протягом семестру

Задовільно (60-74) – здобувач має знання, навички та вміння для досягнення результатів навчання за програмою. Виконав та захистив розрахункову роботу. Написав дві модульні контрольні роботи. Знає основні визначення та термінологію в галузі захисту інформації, загрози інформаційної безпеки, нормативно-правову базу. Розуміє принципи роботи симетричних криптологічних систем (шифри перестановки, таблиці що шифрують, система Віженера, одноразовий блокнот). Описує структуру та принципи роботи алгоритмів блокового шифрування (DES, AES, ДСТУ ГОСТ 28147-2009, ДСТУ 7624:2014). Розрізняє симетричні та асиметричні криптосистеми, знає основи криптосистем із відкритим ключем (RSA, Ель Гамаля). Пояснює задачі автентифікації та автентифікації даних, принципи роботи цифрового підпису та функцій хешування. Знає загальну характеристику та класифікацію комп'ютерних вірусів, основні типи вірусів (файлові, бутові, stealth, поліморфні, макровіруси, мережеві). Описує засоби нейтралізації та методи захисту від комп'ютерних вірусів. Розуміє основні принципи стеганографії, узагальнену модель стегосистеми, основні програми стеганографії. Виконує лабораторні роботи з дослідження криптографічних алгоритмів та стеганографічних методів. Використовує стандартні алгоритми шифрування та методи захисту інформації для розв'язання базових задач. Розраховує основні параметри криптографічних систем за наданими формулами та алгоритмами.

Добре (75-89) – здобувач має знання, навички та вміння для досягнення результатів навчання за програмою. Виконав та захистив розрахункову роботу. Написав дві модульні контрольні роботи. Додатково до вимог на оцінку "задовільно": Проводить глибокий аналіз криптографічних алгоритмів, порівнює їх характеристики, переваги та недоліки. Самостійно аналізує та порівнює алгоритми симетричного шифрування (DES, AES, ДСТУ), оцінює їх криптостійкість та продуктивність. Розраховує параметри криптосистем із відкритим ключем (довжину ключів, оцінку криптостійкості) для конкретних завдань. Самостійно проектує та реалізує системи автентифікації та цифрового підпису з урахуванням специфіки застосування. Знає структуру допоміжних систем захисту інформації, виконує базові

розрахунки для систем антивірусного захисту. Аналізує стеганографічні алгоритми вбудовування інформації в різні типи медіа (текст, зображення, аудіо, відео), оцінює їх стійкість до атак. Порівнює різні методи захисту інформації та обґрунтовує вибір оптимального рішення для конкретного сценарію. Виконує комплексний аналіз безпеки системи захисту інформації, визначає основні вразливості та ризики.

Відмінно (90-100) – здобувач має знання, навички та вміння, що дозволяють самостійно, вільно та обґрунтовано відповідати на будь-які питання щодо захисту інформації в комп'ютерних системах, враховуючи технічні, правові, економічні та соціальні аспекти. Виконав та захистив розрахункову роботу. Написав дві модульні контрольні роботи. Самостійно пропонує комплекс проектних та технологічних рішень, що можуть підвищити ефективність систем захисту інформації порівняно зі стандартними рішеннями для криптографічних алгоритмів, систем автентифікації, антивірусного захисту та стеганографічних методів. Проводить аналіз складеної комплексної системи захисту інформації, що поєднує криптографічні методи, автентифікацію, антивірусний захист та стеганографію. Формулює завдання для додаткових досліджень у галузі захисту інформації. Організовує професійні комунікації з потенційними замовниками та експертами для обговорення технічних рішень та оптимізації систем захисту. Самостійно розробляє та оптимізує параметри криптографічних систем з урахуванням балансу між безпекою та продуктивністю. Створює інноваційні підходи до комбінації різних методів захисту інформації для досягнення максимальної ефективності. Проводить дослідження нових загроз інформаційної безпеки та розробляє методи захисту від них.

9. Політика навчального курсу

Відвідування занять. Обов'язкове відвідування лекційних та лабораторних занять з навчальної дисципліни "Захист інформації" через їх інтерактивний характер та необхідність практичного освоєння криптографічних алгоритмів, методів автентифікації, антивірусного захисту та стеганографії. Здобувачі освіти, які не можуть регулярно відвідувати заняття, зобов'язані узгодити з викладачем протягом тижня графік відпрацювання пропущених занять. Пропущені заняття необхідно відпрацювати під час найближчої консультації протягом тижня з моменту пропуску, як правило, у формі усного опитування за попередньо визначеними питаннями з відповідних тем курсу. У деяких випадках допускається відпрацювання пропущених лабораторних занять у формі виконання письмових завдань з дослідження криптографічних алгоритмів або стеганографічних методів. Пропуск модульних контрольних робіт та захисту розрахункової роботи без поважної причини не допускається.

Дотримання вимог академічної доброчесності Здобувачі освіти зобов'язані дотримуватися загальних морально-етичних норм, а також вимог академічної доброчесності, викладених у "Положенні про академічну доброчесність Національного аерокосмічного університету «Харківський авіаційний інститут»" (https://khal.edu/assets/files/polozhennya/polozhennya-pro-akademichnu-dobrochesnist.pdf). Роботи здобувачів освіти (звіти з лабораторних робіт, розрахункова робота, модульні контрольні роботи) повинні бути оригінальними. Прикладами порушення академічної доброчесності є відсутність посилань на джерела, вигадування джерел, плагіат, перешкоджання роботі інших здобувачів освіти. Виявлення ознак порушення академічної доброчесності в письмових роботах (звітах з лабораторних робіт, розрахунковій роботі, модульних контрольних роботах) призводить до оцінки "незадовільно" незалежно від масштабу плагіату або обману. Особлива увага приділяється оригінальності програмного коду, реалізованого під час лабораторних робіт з дослідження криптографічних алгоритмів та стеганографічних методів. Використання готових рішень без посилань на джерела та без власного аналізу та модифікації вважається порушенням академічної доброчесності.

Вирішення конфліктів. Порядок і процедури врегулювання конфліктів, пов'язаних із корупційними діями, зіткненням інтересів, різними формами дискримінації, сексуальними домаганнями, міжособистісними стосунками та іншими ситуаціями, що можуть виникнути під час навчання, а також правила етичної поведінки регламентуються Кодексом етичної поведінки в Національному аерокосмічному університеті «Харківський авіаційний інститут» (https://khal.edu/ua/university/normativna-baza/ustanovchi-dokumenti/kodeks-etichnoi-povedinki/).

10. Методичне забезпечення

1. Сторінка дисципліни у системі дистанційного навчання «Ментор» [Ел. ресурс]. URL: https://mentor.khai.edu/course/view.php?id=3737
2. Сторінка дисципліни у системі Classroom [Ел. ресурс]. URL: https://classroom.google.com/c/NjIwNjY2NjM1MTky?cjc=equsclq

11. Рекомендована література

Базова

1. Кузнецов О. О., Євсеєв С. П., Король О. Г. Стеганографія. Навчальний посібник. Харків: Вид. ХНЕУ, 2011. – 232 с.
2. Козіна Г.Л. Криптографія від історії до сучасних стандартів: навч.посібник / Запоріжжя : НУ «Запорізька політехніка», 2020. 192 с.

3. Дворецький М. Л., Нездолій Ю. О., Дворецька С. В., Кандиба І. О. Розробка мобільних застосунків для OS Android : навч. посіб. Миколаїв: Вид-во ЧНУ ім. Петра Могили, 2021. 140 с.
4. Радченко К. О. Розроблення мобільних застосунків. Конспект лекцій : навч. пос., К.: КПІ ім. Ігоря Сікорського, 2021. 546 с.
5. Програмування мобільних пристроїв: навчальний посібник для дистанційного навчання / К.Т. Кузьма. – Миколаїв: СПД Румянцева Г. В., 2021. 128 с.
6. D. Griffiths, D. Griffiths. Head First Android Development: A Learner's Guide to Building Android Apps with Kotlin. O'Reilly Media, 2021. 913 p.
7. N. Metzler. Kotlin Programming for Beginners: An Introduction to Learn the Kotlin Programming Language with Tutorials and Hands-On Examples, Lightbulb Publishing, 2021. 162c.
8. Гулак Г.М. Методологія захисту інформації. Аспекти кібербезпеки: підручник.– К.: Видавництво НА СБ України, 2022. – 256 с.
9. Остапов С.Е., Євсеєв С.П., Король О.Г. Технології захисту інформації: навчальний посібник. – Х.:Новий світ-2000, 2022. – 678 с

Допоміжна

1. A. Grant. Android for Absolute Beginners: Getting Started with Mobile Apps: Development Using the Android Java SDK, 2021. 204 p.
2. M. L. Murphy. Elements Of Android Room 0.5, Leanpub, 2021. 439 p.
3. J. DiMarzio Android Studio Game Development: Concepts and Design, 2021. 95c

12. Інформаційні ресурси

1.Тарнавський Ю. А. Технології захисту інформації URL: https://ela.kpi.ua/ bitstream/123456789/23896/1/TZI_book.pdf

2. Захист інформаційних ресурсів: криптографічні та стеганографічні методи захисту даних. URL: https://vfranchuk.fi.npu.edu.ua/ images/ files/ statty/32_ZIR_cript.pdf

3.Рейтинг найкращих антивірусів — ТОП-10 програм. https://itc.ua/ua/articles/reityng-antyvirusiv/