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

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

ЗАТВЕРДЖУЮ

Гарант освітньої програми


_____Мирослав МОМОТ
(підпис) (ім’я та прізвище)

«_29_» ____08_____ 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: 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)

Вводиться в дію з «01» вересня 2025 р.

Харків 2025

Розробник: Олексій Губка, доцент, к.т.н., доцент _____
(ім’я та прізвище, посада, науковий ступінь і вчене звання) (підпис)

Силабус навчальної дисципліни розглянуто на засіданні кафедри комп’ютерних наук та інформаційних технологій (№ 302)

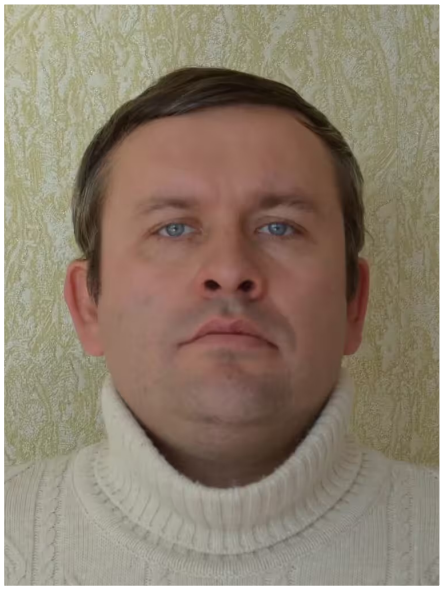
Протокол № _682/07_ від «_26_» __06___ 2025 р.

В. о. завідувача кафедри _д.т.н., проф.__ _____ Олег ФЕДОРОВИЧ
(науковий ступінь та вчене звання) (підпис) (ім’я та прізвище)

Погоджено з представником здобувачів

здобувач вищої освіти групи 356 _____Єгор РАДЧЕНКО_
(ім’я та прізвище)

1.Загальна інформація про викладача



ПІБ: Губка Олексій Сергійович
Посада: доцент кафедри комп'ютерних наук та інформаційних технологій
Науковий ступінь: кандидат техн. наук
Вчене звання: доцент
Перелік дисциплін, які викладає:
- Операційні системи,
- Основи програмування,
- Тестування програмних систем,
- Тестування інформаційних систем,
- Захист інформації в комп'ютерних системах
- Технології захисту інформації.

Напрями наукових досліджень:
- Захист інформації та шифрування даних,
- Розробка та тестування програмного забезпечення,
- Операційні системи.

Контактна інформація: s.gubka@khai.edu

2. Опис навчальної дисципліни

Форми навчання – денна, дистанційна.
Семестр – 8 семестр.
Мова викладання – українська.
Тип дисципліни – обов'язкова.
Обсяг дисципліни – 5,5 кредитів ЄКТС/ 165 годин (60 годин аудиторних, з яких: лекції – 36, лабораторні роботи – 24, самостійна робота здобувача освіти - 105).
Види навчальної діяльності – лекції, лабораторні (практичні) роботи, самостійна робота здобувача.
Види контролю – поточний, захисти лабораторних (практичних) робіт, захист розрахункової роботи, модульний та підсумковий (семестровий) контроль (іспит).

Пререквізити:
- Структури даних та їх віртуалізація (ОК11)
- Технології комп'ютерного проєктування та віртуалізації IT-інфраструктури (ОК18)
- Тестування програмних систем (ОК19)
- Статистичні та імовірнісні методи дата-аналізу (ОК20)
- Мобільні та хмарні технології (КР) (ОК21)
- Операційні системи (ОК23)
- Бази даних та знань, сховища даних та Big Data (ОК29)
- Технології розробки програмного забезпечення та DevOps (ОК30)

- Комп’ютерні мережі (ОК32)

Кореквізити:

- Промислова автоматизація, вбудовані системи реального часу та Інтернету-речей (ОК38)
- Проєктування та програмування розподілених інформаційних систем (КР) (ОК39)

Постреквізити:

- Кваліфікаційна робота (ОК40)

3. Мета та завдання навчальної дисципліни

Мета вивчення: надати здобувача вищої освітим 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.

Компетентності, які набуваються:

Загальні компетентності:

- 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, предметні) 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.

4. Зміст навчальної дисципліни

Модуль 1.

Змістовний модуль 1.

ТЕМА 1. Вступ до навчальної дисципліни.

- Тема та питання лекції:

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.

- Самостійна робота здобувача освіти:

Опрацювання матеріалу лекцій. Формування запитань до викладача. Підготовка до модульного контролю.

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

- Тема та питання лекції:

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).

- Самостійна робота здобувача освіти:

Опрацювання матеріалу лекцій. Формування запитань до викладача. Підготовка до модульного контролю.

ТЕМА 3. Загальні поняття криптографічного захисту інформації.

- Тема та питання лекції:

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

*Лабораторна робота 1: «*Електронні ключі для захисту інформації (eToken)*».*

- Самостійна робота здобувача освіти:

Підготовка до виконання лабораторної роботи. Формування запитань до викладача. Оформлення лабораторної роботи та підготовка до її захисту. Виконання індивідуального завдання. Підготовка до модульного контролю.

ТЕМА 4. Системи відкритого шифрування.

- Теми та питання лекції:

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.

- *Лабораторна робота 2: «*Електронний цифровий підпис та печатка*».*

- Самостійна робота здобувача освіти:

Підготовка до виконання лабораторної роботи. Формування запитань до викладача. Оформлення лабораторної роботи та підготовка до її захисту. Виконання індивідуального завдання. Підготовка до модульного контролю.

ТЕМА 5. Загальні відомості про алгоритм шифрування "Калина" ДСТУ 7624:2014.

- Теми та питання лекції:

Реалізація алгоритму. Базові цикли криптографічних перетворень. Базові режими шифрування. Оптимізація алгоритму на мові високого рівня.

- *Лабораторна робота 2: «*Симетричний алгоритм шифрування "Калина" ДСТУ 7624:2014*».*

- Самостійна робота здобувача освіти:

Підготовка до виконання лабораторної роботи. Формування запитань до викладача. Оформлення лабораторної роботи та підготовка до її захисту. Виконання індивідуального завдання. Підготовка до модульного контролю.

ТЕМА 6. Антивірусний захист даних.

- Теми та питання лекції:

Поняття процедур та функцій в мові C#. Поняття методу в мові C#. Відмінність понять методу та функції.

- *Лабораторна робота 3: «*Антивірусні та антишпигунські програми та пакети (Avira Free Antivirus, NOD 32)*».*
- *Самостійна робота здобувача освіти:*

Підготовка до виконання лабораторної роботи. Формування запитань до викладача. Оформлення лабораторної роботи та підготовка до її захисту. Виконання індивідуального завдання. Підготовка до модульного контролю.

Модульний контроль 1.

Модуль 2.

Змістовний модуль 2.

ТЕМА 7. Алгоритми генерації випадкових чисел.

- Теми та питання лекцій:

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

- *Лабораторна робота 4: «*Захист інформації у операційній системі Windows. Протокол Kerberos*».*
- *Самостійна робота здобувача освіти:*

Підготовка до виконання лабораторної роботи. Формування запитань до викладача. Оформлення лабораторної роботи та підготовка до її захисту. Виконання індивідуального завдання. Підготовка до модульного контролю.

ТЕМА 8. Криптографічні інтерфейси.

- Теми та питання лекцій:

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.

- *Лабораторна робота 5: «*Шифруюча файлова система EFS (Windows 11)*».*
- *Самостійна робота здобувача освіти:*

Підготовка до виконання лабораторної роботи. Формування запитань до викладача. Оформлення лабораторної роботи та підготовка до її захисту. Виконання індивідуального завдання. Підготовка до модульного контролю.

ТЕМА 9. Забезпечення надійності криптографічних алгоритмів.

- Теми та питання лекцій:

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

- *Лабораторна робота 7: «*Асиметричний алгоритм шифрування RSA*».*
- *Самостійна робота здобувача освіти:*

Підготовка до виконання лабораторної роботи. Формування запитань до викладача. Оформлення лабораторної роботи та підготовка до її захисту. Виконання індивідуального завдання. Підготовка до модульного контролю.

ТЕМА 10. Особливості криптографічних засобів (КЗ).

- *Теми та питання лекцій:*

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

- *Самостійна робота здобувача освіти:*

Опрацювання матеріалу лекцій. Формування запитань до викладача. Підготовка до модульного контролю.

ТЕМА 11. Заключна лекція.

- *Тема та питання лекції:*

Перспективи розвитку технологій захисту інформації.

- *Самостійна робота здобувача освіти:*

Опрацювання матеріалу лекцій. Формування запитань до викладача. Підготовка до модульного контролю.

Модульний контроль 2.

5. Індивідуальні завдання

Виконання розрахункової роботи на тему «Криптографічні методи захисту інформації». Метою роботи є закріплення знань та навичок, отриманих на протязі курсу щодо розв’язання задач у сфері побудови та використання мови програмування C#.

6. Методи навчання

Словесні, наочні, практичні. Проведення аудиторних занять, індивідуальні консультації (при необхідності), самостійна робота здобувачів за матеріалами, опублікованими кафедрою (методичні посібники) та іншими матеріалами, в тому числі електронними.

7. Методи контролю

Поточний контроль (теоретичне опитування й розв’язання практичних завдань), захист практичних робіт, захист розрахункової роботи, модульний контроль (тестування за розділами курсу) та підсумковий (семестровий) контроль (іспит).

8. Критерії оцінювання та розподіл балів, які отримують здобувачі

Таблиця 8.1 – Розподіл балів, які отримують здобувачі освіти

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 здобувача вищої освіти 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 двох теоретичних та одного практичного запитань. За повну правильну відповідь на два перших запитання студент отримує по 33 бали. За повну правильну відповідь на останнє запитання – 34 бали.

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

Критерії оцінювання роботи здобувача 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.

9. Політика навчального курсу

Відвідування занять. Здобувачі освіти, які за певних обставин не можуть відвідувати практичні заняття регулярно, повинні протягом тижня узгодити із викладачем графік індивідуального відпрацювання пропущених занять. Окремі пропущені заняття мають бути відпрацьовані на найближчій консультації протягом тижня після їх пропуску.

Дотримання вимог академічної доброчесності здобувачами освіти під час вивчення навчальної дисципліни. Під час вивчення навчальної дисципліни здобувачі освіти мають дотримуватися загальноприйнятих морально-етичних норм і правил поведінки, вимог академічної доброчесності, передбачених Положенням про академічну доброчесність Національного аерокосмічного університету «Харківський авіаційний інститут» (https://khai.edu/assets/files/polozhennya/polozhennya-pro-akademichnu-dobrochesnist.pdf).

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://khai.edu/ua/university/normativna-baza/ustanovchi-dokumenti/kodeks-etichnoi-povedinki/).

10. Методичне забезпечення

1. Комплекс навчально-методичного забезпечення дисципліни: сайт дистанційного навчання університету «Ментор» [Електронний ресурс]. – Режим доступу: https://mentor.khai.edu/course/view.php?id=1306

11. 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.

12. Інформаційні ресурси

Сайт науково-технічної бібліотеки університету [Електронний ресурс]. – Режим доступу: http://library.khai.edu.

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