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

Кафедра інформаційних технологій проектування (№ 105)

ЗАТВЕРДЖУЮ

Гарант освітньої програми
_____ Олександр КАРАТАНОВ
(підпис) (ініціали та прізвище)

«28» серпня 2025 р.

СИЛАБУС
НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Технології захисту інформації
(назва навчальної дисципліни)

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

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

Освітня програма: «Інформаційні технології проектування»
(найменування освітньої програми)

Форма навчання: денна

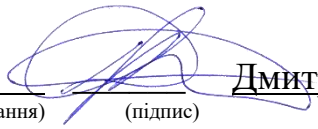
Рівень вищої освіти: перший (бакалаврський)

Харків 2025 рік

Розробник: доцент каф 105, к.т.н., доцент Аліна АРТЬОМОВА 
(прізвище та ініціали, посада, науковий ступінь і вчене звання) (підпис)

Силабус навчальної дисципліни розглянуто на засіданні кафедри № 105 «Інформаційних технологій проєктування»
(назва кафедри)

Протокол № 1 від « 28» серпня 2025 р.

Декан факультету № 1 к.т.н., доцент  Дмитро КРИЦЬКИЙ
(науковий ступінь і вчене звання) (підпис) (ім'я та прізвище)

1. Загальна інформація про викладача

Артьомова Аліна Вадимівна, доцент кафедри інформаційних технологій проєктування, кандидат технічних наук, доцент.

Перелік дисциплін, які викладає: чисельні методи, методи захисту інформації, інструменти автоматизованого проєктування

Напрями наукових досліджень:
методи і моделі автоматизації планування ланцюга маршрутів польотів БПЛА для підвищення ефективності пошуку об’єктів

2. Опис навчальної дисципліни

Форма здобуття освіти	Денна
Семестр	7
Мова викладання	Українська
Тип дисципліни	Обов’язкова
Обсяг дисципліни: кредити ЄКТС/ кількість годин	денна: 4,5 кредитів ЄКТС / 135 годин (64 аудиторних, з яких: лекції – 32, практичні – 32; СРЗ – 71)
Види навчальної діяльності	Лекції, лабораторні заняття, самостійна робота
Види контролю	Поточний контроль, модульний контроль, семестровий контроль – іспит
Пререквізити	Хмарні технології, Інструментальні засоби візуального проектування.
Кореквізити	Технології розподілених систем та паралельних обчислень, Комп’ютерні технології у виробництві.
Постреквізити	Наскрізне проектування.

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

Мета вивчення: вивчення сучасних методів, технологій та засобів захисту інформації в автоматизованих системах.
Завдання: вивчення комплексу організаційних (законодавча база, вимоги до персоналу та інше) та технологічних (алгоритми та протоколи, що застосовуються у криптографії) дій, що виконуються для забезпечення інформаційної безпеки автоматизованих систем.

Компетентності, які набуваються:
Інтегральна компетентність: Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі комп'ютерних наук або у процесі навчання, що передбачає застосування теорій та методів інформаційних технологій і характеризується комплексністю та невизначеністю умов.

Загальні компетентності:
ЗК2. Здатність застосовувати знання у практичних ситуаціях.
ЗК3. Знання та розуміння предметної області та розуміння професійної діяльності.
ЗК12.Здатність оцінювати та забезпечувати якість виконуваних робіт

Спеціальні компетентності:

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

Програмні результати навчання:
ПР16. Розуміти концепцію інформаційної безпеки, принципи безпечного проектування програмного забезпечення, забезпечувати безпеку комп'ютерних мереж в умовах неповноти та невизначеності вихідних даних.

4. Зміст навчальної дисципліни

Модуль 1.

Змістовний модуль 1. Безпека та захист даних.

Тема 1. Поняття інформаційної безпеки.

Анотація: У підрозділі розглянуто сутність інформаційної безпеки як стану захищеності даних від несанкціонованого доступу, модифікації чи знищення. Визначено основні цілі: конфіденційність, цілісність та доступність інформації.
Тема лекції: Поняття інформаційної безпеки.
Тема лабораторного заняття: -
Самостійна робота здобувача освіти: опрацювати матеріали лекції.

Тема 2. Традиційні криптографічні системи.

Анотація: У підрозділі розглянуто принципи традиційних криптографічних систем на основі симетричного шифрування. Проаналізовано класичні алгоритми заміни й перестановки, їх переваги та обмеження, а також проблеми криптостійкості в сучасних умовах.
Тема лекції: Традиційні криптографічні системи.
Тема лабораторного заняття: Класичний шифр простої заміни та його криптоаналіз на прикладі біграмного шифру.
Самостійна робота здобувача освіти: опрацювати матеріали лекції, виконання індивідуальних завдань, підготовка до захисту лабораторних робіт.

Тема 3. Симетричні алгоритми шифрування

Анотація: У підрозділі подано загальну характеристику симетричних алгоритмів шифрування, що використовують єдиний секретний ключ. Розглянуто основні типи (потокові та блочні шифри), їхні переваги у швидкодії та недоліки, пов'язані з розповсюдженням ключів.
Тема лекції: Симетричні алгоритми шифрування
Тема лабораторного заняття: -
Самостійна робота здобувача освіти: опрацювати матеріали лекції.

Тема 4. Мережа Фейстеля

Анотація: Подано структуру мережі Фейстеля як базової моделі побудови блочних шифрів. Описано принципи поділу даних на підблоки, виконання раундів та значення цієї архітектури для сучасних криптоалгоритмів.
Тема лекції: Мережа Фейстеля.
Тема лабораторного заняття: -
Самостійна робота здобувача освіти: опрацювати матеріали лекції.

Тема 5. Алгоритм DES
Анотація: Висвітлено основні характеристики алгоритму симетричного блочного шифрування DES. Розглянуто його структуру, ключові параметри та причини зниження криптостійкості з часом.
Тема лекції: Алгоритм DES
Тема лабораторного заняття: Реалізація симетричного алгоритму шифрування DES.
Самостійна робота здобувача освіти: опрацювати матеріали лекції, виконання індивідуальних завдань, підготовка до захисту лабораторних робіт.

Тема 6. Модифікація DES (3DES).
Анотація: Описано триразове застосування алгоритму DES як метод підвищення його стійкості. Проаналізовано переваги та недоліки 3DES у порівнянні з класичним DES і сучасними алгоритмами шифрування.
Тема лекції: Модифікація DES (3DES).
Тема лабораторного заняття: -
Самостійна робота здобувача освіти: опрацювати матеріали лекції, підготовка до модульної роботи.

Тема 7. Загальний опис криптоалгоритму AES.
Анотація: Описано алгоритм симетричного шифрування AES, його параметри, основні криптографічні перетворення та переваги застосування у сучасних протоколах безпеки.
Тема лекції: Загальний опис криптоалгоритму AES.
Тема лабораторного заняття: Дослідження криптографічних властивостей блокового симетричного шифру AES.
Самостійна робота здобувача освіти: опрацювати матеріали лекції, виконання індивідуальних завдань, підготовка до захисту лабораторних робіт.

Модульний контроль 1

Змістовний модуль 2. Мережева безпека.
Тема 8. Асиметричні криптосистеми. Алгоритм RSA
Анотація: У підрозділі розглянуто принципи роботи асиметричних криптосистем на основі відкритого та закритого ключів, зокрема алгоритм RSA. Наведено його математичні основи, включно з конгруентностями, алгоритмом Евкліда, функцією Ейлера та модульною арифметикою, а також

проаналізовано процеси генерації ключів, шифрування і дешифрування та визначено сфери практичного застосування.
Тема лекції: Асиметричні криптосистеми. Алгоритм RSA
Тема лабораторного заняття: Реалізація асиметричного алгоритму шифрування RSA.
Самостійна робота здобувача освіти: опрацювати матеріали лекції, виконання індивідуальних завдань, підготовка до захисту лабораторних робіт.

Тема 9. Геш-функції. Особливості. Алгоритми. SHA.
Анотація: Визначення геш-функції. Властивості криптографічних геш-функцій. Популярні алгоритми гешування. Практичне застосування геш-функцій. Порядок і структура гешування. Гешування в blockchain та Merkle tree. Процедури створення та перевірки підпису. Схеми цифрового підпису RSA та Ель-Гамаля. Стандарт цифрового підпису DSS.
Тема лекції: Геш-функції. Особливості. Алгоритми. SHA.
Тема лабораторного заняття: Реалізація однонаправленої хэш-функції SHA.
Самостійна робота здобувача освіти: опрацювати матеріали лекції, виконання індивідуальних завдань, підготовка до захисту лабораторних робіт.

Тема 10. Основи побудови криптографічних протоколів.
Анотація: Поняття криптографічного протоколу. Задачі, які вирішуються завдяки криптографічними протоколами. Безпека криптографічних протоколів. Протоколи аутентифікації. Специфічні протоколи.
Тема лекції: Основи побудови криптографічних протоколів.
Тема лабораторного заняття: Реалізація алгоритму електронно-цифрового підпису (ЭЦП).
Самостійна робота здобувача освіти: опрацювати матеріали лекції, виконання індивідуальних завдань, підготовка до захисту лабораторних робіт, підготовка до модульної робіти.

Модульний контроль 2

5. Індивідуальні завдання

Індивідуальне завдання (РГР) передбачені навчальним планом.

6. Методи навчання

Проблемні лекції спрямовані на розвиток логічного мислення здобувачів освіти. Коло питань теми лекції обмежується двома-трьома ключовими моментами, увага здобувачів освіти концентрується на матеріалі, що не знайшов відображення в підручниках, використовується передовий досвід. Під час лекцій

використовується друкований опорний конспект у якому виділені головні висновки з питань, що розглядаються. При викладанні лекційного матеріалу здобувачам освіти пропонуються питання для самостійного розмірковування. При цьому лектор задає запитання, які спонукають здобувача освіти шукати розв'язання проблемної ситуації. Така система примушує здобувачів освіти сконцентруватися і почати активно мислити в пошуках правильної відповіді.

Семінари-дискусії передбачають обмін думками та поглядами учасників з приводу даної теми (питання), а також розвивають мислення, допомагають формувати погляди і переконання, виробляють вміння формулювати думки й висловлювати їх, вчать оцінювати пропозиції інших людей, критично підходити до власних поглядів.

Кейс-метод – метод аналізу конкретних ситуацій, який дає змогу наблизити процес навчання до реальної практичної діяльності спеціалістів і передбачає розгляд проблемних ситуацій у процесі вивчення навчального матеріалу

Презентації – виступи перед аудиторією, що використовуються для представлення певних результатів роботи з виконання індивідуальних завдань.

7. Методи контролю

Поточний контроль (теоретичне опитування й виконання та захист лабораторних робіт), модульний контроль (тестування за розділами курсу) та підсумковий (семестровий) контроль (іспит).

Під час вивчення дисципліни застосовується поточний і підсумковий контроль знань. Усі ці види контролю тісно взаємозв'язані й організуються так, щоб стимулювати ефективну самостійну роботу здобувача освіти протягом семестру і забезпечити об'єктивне оцінювання рівня їхніх знань.

Поточний контроль здійснюється під час лабораторних занять, у процесі розгляду й оцінювання виконаних завдань, спілкування викладача зі здобувачем освіти на індивідуальних консультаціях. Він має на меті перевірку рівня підготовленості здобувача освіти до виконання конкретної роботи. Засоби проведення поточного контролю включають тести для виявлення ступеня оволодіння здобувачами освіти необхідними теоретичними положеннями.

Підсумковий контроль проводиться у формі контрольних робіт за окремими частинами (модулями) дисципліни. Для проміжного контролю дисципліна поділена на дві частини (модулі): 1 модуль – теми 1-7; 2 – теми 8-10.

Підсумковий контроль проводиться у формі письмового іспиту. Здобувачі освіти допускаються до іспиту, якщо вони виконали усі обов'язкові роботи і завдання з дисципліни протягом семестру. Перелік таких робіт і завдань доводиться до здобувача освіти на початку семестру. Своєчасність і якість їх виконання з'ясовуються в процесі поточного контролю.

Якщо здобувач освіти одержав незадовільну оцінку за контрольне оцінювання з певної теми курсу, або був відсутній на контрольному оцінюванні, то він зобов'язаний ліквідувати поточну заборгованість, що утворилася, під час

найближчої консультації у викладача, який проводить лабораторні заняття або лекції з даної дисципліни.
Здобувач освіти, який має заборгованості з контрольних оцінювань з окремих тем курсу «Технологія захисту інформації», вважається таким, що не виконав всі види робіт, передбачені навчальним планом на семестр з цієї навчальної дисципліни, і до іспиту не допускається.

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			
Активність під час аудиторної роботи	0…1	7	0…6
Виконання і захист лабораторних робіт	0...5	3	0...20
Модульний контроль	0…20	1	0…20
Змістовний модуль 2			
Активність під час аудиторної роботи	0…1	3	0…6
Виконання і захист лабораторних робіт	0...5	3	0...20
Модульний контроль	0…20	1	0…20
Виконання і захист РГР	0…8	1	0…8
Усього за семестр			**0…100**

Семестровий контроль (іспит) проводиться у разі допуску здобувача освіти, який набрав впродовж семестру не менше 50 балів і обов'язково виконав й захистив лабораторні роботи та здав модулі. При складанні семестрового іспиту здобувач освіти має можливість отримати максимум 100 балів.
Білет для іспиту складається з двох блоків теоретичних питань у вигляді тестів за кожним модулем та однієї практичної задачі. За кожне теоретичне питання максимальна кількість балів 25, за практичну задачу- 50 балів, загалом 100 балів.

Таблиця 8.2 – Шкали оцінювання: бальна і традиційна

Сума балів	Оцінка за традиційною шкалою	
	Іспит, диференційований залік	Іспит
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 лабораторні завдання та пройти тестування за двома модулями, виконати РГР. Здобувач має базові знання, розуміє основні поняття, але не завжди може глибоко пояснити деталі або зв'язки між поняттями, може ідентифікувати загрози та ризики, але пропонує поверхневий аналіз ситуацій і недостатньо критичний підхід, має загальне уявлення про те, як можна застосувати знання на практиці, але відповіді на практичні завдання обмежені та неповні, знає основи роботи з алгоритмами шифрування, але вимагає додаткової допомоги або часу для їх використання

Добре (75-89). Вміти все що вказано у попередньому пункті. Здобувач демонструє чітке розуміння теми, може вільно пояснювати ключові терміни та основні концепції, але іноді пропускає складніші деталі, проводить аналіз на прийнятному рівні, розуміє як працюють основні алгоритмами шифрування, але іноді не розкриває всі можливі аспекти проблеми, вільно працює з інструментами, однак у складних ситуаціях може виникати потреба в додатковій підтримці, обізнаний з основними новими загрозами та технологіями у сфері шифрування, але не завжди може їх застосувати на практиці

Відмінно (90-100). Здати всі контрольні точки з оцінкою «відмінно». Досконально знати всі теми та уміти застосовувати їх. Здобувач повинен мати глибоке і детальне розуміння теми, здатність не тільки пояснювати концепції, але й критично їх аналізувати, наводити приклади з практики, продемонстровано глибокий аналіз, здатність виявляти приховані загрози та пропонувати чіткі рішення з урахуванням різних факторів, демонструє впевнене володіння методами та інструментами, здатний критично аналізувати концепції, порівнювати алгоритми, пояснювати переваги та обмеження кожного, наводити приклади застосування у практичних сценаріях, виявляє приховані загрози та пропонує ефективні рішення для їх нейтралізації, демонструє впевнене володіння інструментами криптографії та захисту інформації, використовує знання для практичного забезпечення безпеки даних, роботи з різними системами шифрування, протоколами та геш-функціями, прогнозує можливі ризики та пропонує шляхи їх мінімізації, чітко орієнтується у сучасних загрозах, технологіях та тенденціях у шифрування, використовує ці знання для вирішення реальних проблем.

9. Політика навчального курсу

Відвідування занять. Регуляція пропусків. Інтерактивний характер курсу передбачає обов’язкове відвідування практичних 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. Відпрацювання занять здійснюється усно у формі співбесіди за питаннями, визначеними планом заняття. В окремих випадках дозволяється письмове відпрацювання пропущених занять шляхом виконання індивідуального письмового завдання.

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). Очікується, що роботи здобувачів освіти будуть їх оригінальними дослідженнями або міркуваннями. Відсутність посилань на використані джерела, фабрикування джерел, списування, втручання в роботу інших здобувачів освіти становлять, але не обмежують, приклади можливої академічної недоброчестності. Виявлення ознак академічної недоброчесності в письмовій роботі здобувача освіти є підставою для її незарахування викладачем незалежно від масштабів плагіату чи обману.

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

Посилання на курс у системі дистанційного навчання Ментор: https://mentor.khai.edu/course/view.php?id=9291

11. Рекомендована література

Базова

1. Юдін О.К. Захист інформації в мережах передачі даних / О.К. Юдін, О.Г. Корченко, Г.Ф. Конахович // Підручник — К. : Вид-во DIRECTLINE, 2019. — 714 с.

Допоміжна

1. Сенів М. М. Безпека програм та даних: навч. посібник / М.М. Сенів, В.С. Яковина. –Львів : Видавництво Львівської політехніки, 2015. –256 с.
2. Нормативно-правове забезпечення інформаційної безпеки: Збірник нормативно-правових документів / Уклад. О.Г. Корченко, Ю.О. Дрейс. — Житомир : ЖВІ НАУ, 2018. — 280 с.
3. НД ТЗІ 1.1-003-99: Термінологія в області захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБУ № 22 від 28.04.1999. ДСТСЗІ СБУ. – К., 1999. – 34 с.
4. НД ТЗІ 2.5-004-99: Критерії оцінки захищеності інформації у комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБУ № 22 від 28.04.1999. ДСТСЗІ СБУ. – К., 1999. – 34 с

5. НД ТЗІ 2.5-005-99: Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБУ № 22 від 28.04.1999. ДСТСЗІ СБУ. – К., 1999. – 34 с.
6. Технології захисту інформації [Електронний ресурс] : підручник для студ. спеціальності 122 «Комп'ютерні науки», спеціалізацій «Інформаційні технології моніторингу довкілля», «Геометричне моделювання в інформаційних системах» / Ю. А. Тарнавський; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 2,04 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2018. – 162 с.

11. Інформаційні ресурси

1. Концепція технічного захисту інформації в Україні. – [Електронний ресурс]. – Режим доступу : http://zakon1.rada.gov.ua/cgibin/laws /main.cgi?nreg=1126-97-%EF.
2. Положення про проведення відкритого конкурсу криптографічних алгоритмів // Інститут кібернетики ім. В. М. Глушкова НАНУ; ДСТСЗІ [Електронний ресурс]. – Режим доступу : http://www.dstszi.gov.ua /dstszi/ control /ru/publish/article
3. Український ресурс з безпеки [Електронний ресурс]. – Режим доступа : http://kiev-security.org.ua
4. Комплексні системи захисту інформації /[Електронний ресурс]. [Ю. Є. Яремчук, П. В. Павловський, В. С. Катаєв, В. В. Синюгін] – Режим доступу: https://web.posibnyky.vntu.edu.ua/fmib/41yaremchuk_kompleksni_systemy_za hystu_informaciyi
5. Основи програмування – Режим доступу: https://av.tib.eu/series/1500
6. БД Режим доступу: https://av.tib.eu/series/1487
7. Онлайн курси міжнародного проекту кафедри – Режим доступу: https: //av.tib.eu/publisher/Projekt__Open_Education_Resources_with_Ukraine_