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

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

**ЗАТВЕРДЖУЮ**

Гарант освітньої програми
_____ Олег ІЛЛЯШЕНКО
(підпис) (ім'я та ПРІЗВИЩЕ)

« 29 » серпня 2025 р.

# СИЛАБУС ОБОВ'ЯЗКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Захист інформації в інформаційно-комунікаційних системах (КП)
(назва навчальної дисципліни)

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

**Спеціальність:** 125 «Кібербезпека»
(код і найменування спеціальності)

**Освітня програма**: «Безпека інформаційних і комунікаційних систем»
(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 _____
__комп’ютерних систем, мереж і кібербезпеки_____
(назва кафедри)

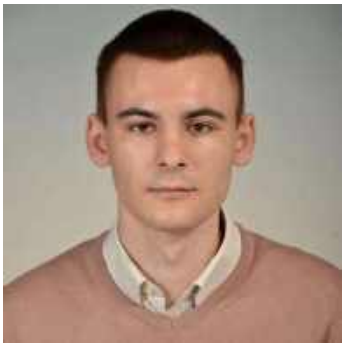
Протокол № 1 від « 29» серпня 2025 р.

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

Погоджено з представником здобувачів освіти:

_____ __Ілля МІЦИК_____
(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* |
| Семестр | 7-й |
| Мова викладання | Українська |
| Тип дисципліни | Обов'язкова |
| Обсяг дисципліни: кредити ЄКТС/ кількість годин | *денна*: 2 кредитів ЄКТС / 60 годин (16 аудиторних, з яких: практичні заняття – 16; СРЗ – 44); |
| Види навчальної діяльності | Практичні заняття, курсовий проєкт, самостійна робота. |
| Види контролю | диф. залік. |
| Пререквізити | Прикладна криптологія, Захист інформації в інформаційно-комунікаційних системах, Інформаційно-комунікаційні системи |

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

**Мета** – визначення рівня підготовленості студента до розв'язання комплексу сучасних наукових і прикладних завдань відповідно до захисту інформації в інформаційно-комунікаційних системах.

**Завдання** – систематизація, закріплення і розширення теоретичних знань; розвиток навичок самостійної роботи, оволодіння методикою досліджень і експериментування використання сучасних інформаційних технологій у процесі розв'язання задач, які передбачені завданням на курсове проектування.

**Компетентності, які набуваються:**

***Інтегральна компетентність***:

Здатність розв’язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки і або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.

***Загальні компетентності***

***Після закінчення цієї програми здобувач освіти буде здатен:***

(ЗК1) здатність застосовувати знання у практичних ситуаціях.

(ЗК2) знання та розуміння предметної області та розуміння професії.

(ЗК3) здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово.

(ЗК4) вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.

(ЗК5) здатність до пошуку, оброблення та аналізу інформації.

***Спеціальні компетентності***

***Після закінчення цієї програми здобувач освіти буде здатен:***

(КФ1) здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.

(КФ3) здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.

(КФ12) здатність аналізувати, виявляти та оцінювати можливі загрози, вразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

***Результати навчання:***

(ПРН1) застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації.

(ПРН8) готувати пропозиції до нормативних актів щодо забезпечення інформаційної та/або кібербезпеки.

(ПРН14) вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-

апаратними засобами та давати оцінку результативності якості прийнятих рішень.

(ПРН19) застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.

(ПРН30) здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем.

(ПРН31) застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем.

(ПРН34) приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації.

(ПРН50) забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних).

(ПРН51) підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах.

## 4. Зміст навчальної дисципліни

## МОДУЛЬ 1
## Змістовний модуль 1. Розроблення програми досліджень

### Тема 1. Постановка задачі на курсове проектування

*Анотація:* Розглядаються основні поняття та термінологія в галузі захисту інформації в інформаційно-комунікаційних системах. Визначається об'єкт та предмет дослідження курсового проекту. Аналізуються актуальні загрози інформаційної безпеки ІКС.

*Тема практичного заняття 1:* Предмет, мета вивчення і задачі дисципліни. Структура та зміст дисципліни і методичні рекомендації щодо її вивчення. Місце дисципліни у навчальному процесі. Вимоги до знань та вмінь тих, хто навчається. Аналіз предметної області. Визначення об'єкта та предмета дослідження курсового проекту.

*Самостійна робота здобувачів:* Вивчення нормативно-правової бази захисту інформації в ІКС. Аналіз актуальних загроз інформаційної безпеки. Формулювання актуальності теми курсового проекту.

### Тема 2. Основні вимоги до курсового проекту

*Анотація:* Визначаються зміст та структура курсового проекту з захисту інформації в ІКС. Розглядаються вимоги до основної частини, технічного завдання, аналізу загроз та вразливостей, проектування системи захисту.

*Тема практичного заняття 2:* Зміст та структура курсового проекту. Загальні положення. Основна частина: аналіз предметної області, модель загроз та порушника, проектування системи захисту, програмна реалізація. Список використаних джерел.

*Самостійна робота здобувачів:* Розробка структури курсового проекту. Складання плану дослідження. Визначення переліку джерел за темою проекту.

### Тема 3. Аналіз існуючих методів захисту інформації в ІКС

*Анотація:* Проводиться порівняльний аналіз існуючих методів та засобів захисту інформації в інформаційно-комунікаційних системах.

Вивчаються криптографічні методи захисту, механізми контролю доступу, засоби мережевої безпеки.

*Тема практичного заняття 3:* Проведення аналітичного огляду існуючих методів захисту інформації за темою курсового проекту. Огляд літературних джерел та патентний пошук. Аналіз нормативних документів (НД ТЗІ, ISO/IEC 27001).

*Самостійна робота здобувачів:* Пошук та аналіз наукових публікацій за темою проекту. Складання бібліографічного списку. Порівняльний аналіз існуючих рішень та визначення їх недоліків.

### Тема 4. Постановка завдання на дослідження

*Анотація:* Формулюється мета та завдання дослідження. Визначаються вхідні дані, обмеження та вимоги до результатів. Розробляється модель загроз та порушника. Обґрунтовується актуальність та наукова новизна дослідження.

*Тема практичного заняття 4:* Формулювання мети, завдань та вимог до курсового проекту. Розробка моделі загроз та порушника. Визначення критеріїв оцінки результатів. Розробка технічного завдання на систему захисту інформації.

*Самостійна робота здобувачів***:** Деталізація завдань дослідження. Визначення очікуваних результатів та критеріїв їх оцінки. Обґрунтування наукової новизни та практичної цінності.

## Змістовний модуль 2. Розроблення та захист курсового проекту

### Тема 5. Проектування системи захисту інформації

*Анотація:* Розробляється архітектура системи захисту інформації в ІКС. Обираються методи та засоби захисту. Проектуються механізми криптографічного захисту, контролю доступу, моніторингу та аудиту.

*Тема практичного заняття 5:* Проектування архітектури системи захисту. Вибір криптографічних алгоритмів та протоколів. Проектування підсистем контролю доступу та моніторингу.

*Самостійна робота здобувачів:* Розробка структурних схем системи захисту. Обґрунтування вибору методів та засобів захисту. Проектування алгоритмів роботи системи.

**Тема 6. Програмна реалізація системи захисту**

*Анотація:* Здійснюється програмна реалізація системи захисту інформації. Розробляється програмний код відповідно до спроектованої архітектури. Реалізуються криптографічні алгоритми та механізми захисту.

*Тема практичного заняття 6:* Програмна реалізація системи захисту інформації. Розробка програмного коду. Реалізація криптографічних модулів та механізмів контролю доступу.

*Самостійна робота здобувачів:* Розробка та налагодження програмного забезпечення. Документування програмного коду. Підготовка інструкції користувача.

**Тема 7. Тестування та верифікація**

*Анотація:* Проводиться верифікація та тестування розробленого рішення. Аналізуються результати тестування та оцінюється ефективність захисту. Виявляються та усуваються недоліки.

*Тема практичного заняття 7:* Тестування та верифікація системи захисту. Підготовка тестових сценаріїв. Аналіз результатів тестування. Оцінка ефективності захисту.

*Самостійна робота здобувачів:* Підготовка тестових сценаріїв. Документування результатів тестування. Аналіз відповідності результатів технічному завданню.

**Тема 8. Оформлення курсового проекту**

*Анотація:* Розглядаються вимоги до оформлення пояснювальної записки курсового проекту. Вивчаються правила оформлення ілюстрацій, таблиць, формул, програмного коду та списку використаних джерел.

*Тема практичного заняття 8:* Оформлення курсового проекту. Загальні вимоги до оформлення пояснювальної записки. Ілюстрації, таблиці, формули. Оформлення програмного коду. Оформлення списку використаних джерел за ДСТУ 8302:2015.

*Самостійна робота здобувачів:* Оформлення пояснювальної записки відповідно до вимог. Підготовка графічного матеріалу. Форматування списку джерел.

**Тема 9. Підготовка до захисту курсового проекту**

*Анотація:* Розглядається порядок підготовки до захисту курсового проекту. Формуються вимоги до презентації та доповіді. Визначаються критерії оцінювання курсового проекту.

*Тема практичного заняття 9:* Порядок захисту курсового проекту. Оформлення презентації. Структура та зміст доповіді. Підготовка відповідей на типові запитання.

*Самостійна робота здобувачів:* Підготовка презентації результатів дослідження. Підготовка тез доповіді. Репетиція захисту.

**Тема 10. Захист курсового проекту**

*Анотація:* Проводиться публічний захист курсового проекту. Демонструється працездатність розробленої системи захисту інформації. Оцінюються результати виконання курсового проекту.

*Тема практичного заняття 10:* Публічний захист курсового проекту. Доповідь з презентацією. Демонстрація програмного продукту. Відповіді на запитання комісії.

*Самостійна робота здобувачів:* Фінальна підготовка до захисту. Перевірка працездатності програмного продукту. Підготовка демонстраційних матеріалів.

## 5. Індивідуальні завдання

Виконання курсового проекту.

## 6. Методи навчання

Проведення аудиторних практичних робіт, консультацій, а також самостійна робота здобувачів з використанням відповідних матеріалів (п.11, 12).

## 7. Методи контролю

*Поточний контроль*: опитування на практичних заняттях з основних понять захисту інформації в ІКС, криптографічних алгоритмів та методів захисту; аналіз та порівняння існуючих методів та рішень за темою курсового проекту; перевірка виконання етапів курсового проекту (аналіз предметної області, постановка завдання, розробка моделі загроз та порушника, проектування системи захисту, програмна реалізація, тестування); оцінювання виконання індивідуальних завдань з аналізу криптографічних алгоритмів, розробки архітектури системи захисту, програмної реалізації та тестування; перевірка проміжних результатів виконання курсового проекту та їх відповідності технічному завданню; оцінювання якості оформлення пояснювальної записки, доповіді та презентації.

*Підсумковий контроль*: захист курсового проекту, що включає перевірку пояснювальної записки на відповідність вимогам стандартів, демонстрацію працездатності розробленої системи захисту інформації, доповідь з презентацією основних результатів дослідження, відповіді на запитання комісії щодо теоретичних основ, архітектурних рішень, особливостей програмної реалізації та отриманих результатів.

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

Поточний контроль передбачає контроль за роботою студента протягом семестру над курсовим проектом, надання йому допомоги та надання консультацій під час роботи над відповідними пунктами курсового проекту.

Підсумкова оцінка виставляється виходячи з якості пояснювальної записки, повноти викладеного матеріалу, відповідності ЄСКД та ЄСПД, якості та повноти доповіді, відповідей на питання членів комісії.

Таблиця 8.1 – Розподіл балів, які отримують здобувачі освіти

| № з/п | Показчик | Кількість балів |
|---|---|---|
| 1 | Якість пояснювальної записки | 0 - 10 |
| 2 | Повнота викладеного матеріалу | 0 - 10 |
| 3 | Відповідність ЄСКД та ЄСПД | 0 - 10 |
| 4 | Якість та повнота доповіді | 0 - 30 |
| 5 | Якість відповідей на питання | 0 - 40 |
| 6 | Разом | 0 - 100 |

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 усі етапи курсового проекту на базовому рівні. Знає основні визначення та термінологію в галузі захисту інформації в ІКС. Розуміє класифікацію загроз та вразливостей інформаційно-комунікаційних систем. Знає основні криптографічні алгоритми та методи захисту інформації. Описує базові принципи проектування системи захисту інформації. Виконав програмну реалізацію системи захисту з базовою функціональністю. Провів тестування з обмеженим набором тестових сценаріїв. Оформив пояснювальну записку з незначними відхиленнями від вимог. Підготував презентацію та доповідь на базовому рівні. Відповідає на базові запитання комісії щодо виконаного проекту.

***Добре (75-89)*** – здобувач має знання, навички та вміння для досягнення результатів навчання за програмою. Виконав усі етапи курсового проекту на достатньому рівні. Додатково до вимог на оцінку "задовільно": Проводить порівняльний аналіз методів захисту інформації, порівнює їх ефективність та область застосування. Самостійно розробляє детальну модель загроз та порушника для конкретної ІКС. Обґрунтовує вибір криптографічних алгоритмів та методів захисту для конкретного завдання. Проектує архітектуру системи захисту з урахуванням вимог безпеки та продуктивності. Виконав програмну реалізацію з повною функціональністю відповідно до технічного завдання. Провів комплексне тестування з детальним аналізом результатів. Оформив пояснювальну записку відповідно до вимог стандартів.

Підготував якісну презентацію та структуровану доповідь. Впевнено відповідає на більшість запитань комісії.

***Відмінно (90-100)*** – здобувач має глибокі знання, навички та вміння для досягнення результатів навчання за програмою на високому рівні. Виконав усі етапи курсового проекту на високому рівні. Додатково до вимог на оцінку "добре": Вільно оперує термінологією захисту інформації та криптографії. Самостійно аналізує сучасні загрози та вразливості ІКС, пропонує інноваційні рішення для їх нейтралізації. Обґрунтовує вибір архітектурних рішень з урахуванням криптографічної стійкості, продуктивності та масштабованості. Виконав програмну реалізацію з розширеною функціональністю, оптимізованим кодом та зручним інтерфейсом. Провів всебічне тестування включаючи тестування на проникнення та оцінку криптографічної стійкості. Оформив пояснювальну записку бездоганно з високою якістю графічних матеріалів. Підготував професійну презентацію та переконливу доповідь. Демонструє глибоке розуміння теоретичних основ та практичних аспектів захисту інформації. Впевнено та вичерпно відповідає на всі запитання комісії, демонструє здатність до наукової дискусії.

## 9. Політика навчального курсу

***Відвідування занять.*** Обов'язкове відвідування практичних занять з навчальної дисципліни "Захист інформації в інформаційно-комунікаційних системах (КП)" через їх інтерактивний характер та необхідність практичного освоєння методів аналізу предметної області, розробки моделі загроз та порушника, проектування архітектури системи захисту, програмної реалізації та тестування для забезпечення захисту інформації в ІКС. Здобувачі освіти, які не можуть регулярно відвідувати заняття, зобов'язані узгодити з керівником курсового проекту протягом тижня графік відпрацювання пропущених занять та консультацій. Пропущені заняття необхідно відпрацювати під час найближчої консультації протягом тижня з моменту пропуску, як правило, у формі звіту про виконання відповідного етапу курсового проекту. У деяких випадках допускається відпрацювання пропущених практичних занять у формі виконання письмових завдань з аналізу методів захисту інформації, розробки елементів моделі загроз, оформлення розділів пояснювальної записки або демонстрації проміжних результатів програмної реалізації. Пропуск захисту курсового проекту 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. Навчально-методичний комплекс дисципліни розміщений у системі дистанційного навчання «Ментор»: [Ел. ресурс]. https://mentor.khai.edu/course/view.php?id=4835

## 11. Рекомендована література

**Базова**


1. Важинський С. Е., Щербак Т. І. Методика та організація наукових досліджень навч. пос. Суми: СумДПУ ім. А. С. Макаренка, 2016. – 260 с.
2. Рассоха І. М. «Методологія та організація наукових досліджень» Харк. нац. акад. міськ. госп-ва. – Х.: ХНАМГ, 2011. – 76 с.
3. Грайворонський М. В., Новіков О. М. Безпека інформаційно-комунікаційних систем._ К.: Вид.група BHV, 2009.-608 с.
4. Технології захисту інформації. Мультимедійне інтерактивне електронне видання комбінованого використання / уклад. Євсеєв С. П., Король О. Г., Остапов С. Е., Коц Г. П. – Х.: ХНЕУ ім. С.Кузнеця, 2016. – 1013 Мб.
5. С. П. Євсеєв. Технології захисту інформації / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Чернівці. – Видавничий дом “Родовід”, 2014. – 428 с.

6. Захист інформації в автоматизованих системах управління: навч. посіб. /Уклад. І.А. Пількевич, Н.М. Лобанчикова, К.В. Молодецька. – Житомир: Вид-во ЖДУ ім. І. Франка, 2015. 226 с.
7. Кібербезпека: сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. / С. Е. Остапов, С. П. Євсеєв, О.Г. Король. – Львів: «Новий Світ2000», 2020. – 678 с

**Допоміжна**

1. Jeremiah Grossman. XSS Attacks CROSS SITE SCRIPTING EXPLOITS AND DEFENSE. – USA.: Amazon DS, 2018 – 630 с.
2. Holistic Info-Sec for Web Developers. [Electronic resource]. – Access mode: https://holisticinfosecforwebdevelopers.com/ 4
3. OWASP Web Security Testing Guide. [Electronic resource]. – Access mode : https://owasp.org/www-project-web-security-testing-guide/
4. Open Web Application Security Project [Електронний ресурс]. Режим доступу: a. www.owasp.org 6. Когут Ю.І. Кібербезпека

## 12. Інформаційні ресурси

1. http://www.dsszzi.gov.ua Державна служба спеціального зв'язку та захисту інформації України.
2. http://www.csn.khai.edu Кафедральний сайт
3. http://www.bezpeka.com/ru/lib/spec/cript.html Криптографічний захист інформації.