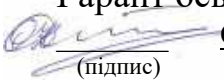
Міністерство освіти і науки України
Національний аерокосмічний університет
«Харківський авіаційний інститут»

**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

Інформаційно-комунікаційні системи
(назва навчальної дисципліни)

**Галузь знань:** 12 «Інформаційні технології»
(шифр і найменування галузі знань)
**Спеціальність:** 125 «Кібербезпека та захист інформації»
(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**

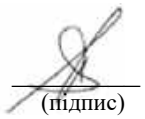
**Харків – 2025 р.**

Розробник (и): Тецький А. Г., доцент, к.т.н.
(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:


(підпис) Ілля МІЦИК
(ім'я та ПРІЗВИЩЕ)

## 1. Загальна інформація про викладача

**ПІБ:** Тецький Артем Григорович

**Посада:** Доцент

**Науковий ступінь:** Кандидат технічних наук

**Вчене звання: -**

**Перелік дисциплін, які викладає:**

Операційні системи;
Інформаційно-комунікаційні системи;
Безпека вебсистем (вибіркова);
Засоби тестування на проникнення (пентестингу, білого хакінгу) (вибіркова);
Технології захисту хмарних та вебсистем (вибіркова).

**Напрями наукових досліджень:**

Кібербезпека вебзастосунків.

**Контактна інформація:**

a.tetskiy@csn.khai.edu

## 2. Опис навчальної дисципліни

| | |
|---|---|
| Форма здобуття освіти | Денна |
| Семестр | 5 |
| Мова викладання | Українська |
| Тип дисципліни | Обов'язкова |
| Обсяг дисципліни: кредити ЄКТС/ кількість годин | 4 кредити ЄКТС / 120 годин (64 аудиторних, з яких: лекції – 32, лабораторні – 32; СРЗ – 56) |
| Види навчальної діяльності | Лекції, лабораторні заняття, самостійна робота |
| Види контролю | Поточний контроль, модульний контроль, семестровий контроль – іспит |
| Пререквізити | ОК12 «Системи технічного захисту інформації» |

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

**Мета** – набуття знань про структуру та принципи функціонування інформаційно-комунікаційних систем, а також формування практичних навичок застосування інструментальних засобів для аналізу, тестування й забезпечення їх кібербезпеки.

**Завдання** – знайомство з архітектурою ІКС та типами мережевої взаємодії, аналіз типових вразливостей протоколів та сервісів, отримання практичних навичок роботи з інструментами Kali Linux для тестування безпеки, впровадження базових засоби захисту від атак у тестовому середовищі.

**Компетентності, які набуваються:**

**Загальні компетентності (ЗК):**

– КЗ 1. Здатність застосовувати знання у практичних ситуаціях.

– КЗ 2. Знання та розуміння предметної області та розуміння професії.

– КЗ 3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово.

– КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.

– КЗ 5. Здатність до пошуку, оброблення та аналізу інформації.

**Фахові компетентності спеціальності (ФК):**

– КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.

– КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.

**Результати навчання (РН):**

– ПРН 1. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації.

– ПРН 2. Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність.

– ПРН 3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності.

– ПРН 4. Аналізувати, аргументувати, приймати рішення при розв’язанні складних спеціалізованих задач та практичних проблем у

професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.

– ПРН 8. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та/або кібербезпеки.

– ПРН 10. Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем.

– ПРН 11. Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах.

– ПРН 13. Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних.

– ПРН 14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень.

– ПРН 15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.

– ПРН 17. Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент.

– ПРН 22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки.

– ПРН 23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.

– ПРН 24. Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових).

– ПРН 26. Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем.

– ПРН 27. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах.

– ПРН 28. Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-

телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки.

– ПРН 29. Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів.

– ПРН 31. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем.

– ПРН 38. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації.

– ПРН 40. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації.

– ПРН 46. Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах.

– ПРН 47. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації.

– ПРН 48. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах.

– ПРН 52. Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах.

## 4. Зміст навчальної дисципліни

### МОДУЛЬ 1
### Змістовний модуль 1. Архітектура і протоколи ІКС

**Тема 1. Підготовка безпечного тестового середовища. Віртуалізація, топологія ІКС, ролі вузлів**

Стисла анотація: Поняття тестового середовища для аналізу безпеки. Основи віртуалізації, налаштування взаємодії між вузлами (Kali Linux, Metasploitable). Структура інформаційно-комунікаційних систем.

**Тема 2. Перехоплення, візуалізація та аналіз мережевого трафіку як основа виявлення аномалій в ІКС**

Стисла анотація: Основи функціонування протоколів канального та транспортного рівнів. Перехоплення та декодування трафіку. Інструменти аналізу (Wireshark, Burpsuite). Виявлення ознак вторгнення, небезпечних протоколів та аномальної поведінки в мережевому трафіку.

Лабораторна робота №1. Налаштування тестового оточення.

Самостійна робота: Відпрацювання матеріалів лекції за темою 2.

**Тема 3. Методи автентифікації та пошук слабких місць через перебір паролів. Захист від brute-force атак**

Стисла анотація: Типові помилки конфігурації служб автентифікації. Перебір облікових даних. Огляд вразливостей при використанні облікових записів за замовчуванням. Аналіз загроз, пов’язаних з недостатнім контролем доступу в ІКС.

Лабораторна робота №2. Перехоплення та аналіз мережевого трафіку.

Самостійна робота: Відпрацювання матеріалів лекції за темою 3.

**Тема 4. Вразливості протоколу FTP та принципи безпечної передачі файлів у ІКС**

Стисла анотація: Огляд архітектури протоколу FTP та його недоліків у контексті кібербезпеки. Демонстрація анонімного доступу, витоку облікових даних через незашифровані з'єднання, типові експлойти. Основи переходу до безпечних альтернатив.

Лабораторна робота №3. Пошук даних за замовчуванням за допомогою перебору.

Самостійна робота: Відпрацювання матеріалів лекції за темою 4.

### МОДУЛЬ 2
### Змістовний модуль 2. Системи захисту в ІКС

**Тема 5. Збирання та аналіз журналів подій для виявлення кіберінцидентів. Основи розслідування подій безпеки**

Стисла анотація: Важливість логування в ІКС. Типи журналів. Методи виявлення слідів атак: підозріла активність, помилки входу, сканування. Основи створення звітів про інциденти.

Лабораторна робота №4. Протокол передачі файлів (FTP) і пов'язані вразливості.

Самостійна робота: Відпрацювання матеріалів лекції за темою 5.

**Тема 6. Протидія атакам перебору. Налаштування системи блокування підозрілих входів у ІКС**

Стисла анотація: Інструменти запобігання brute-force атакам. Принцип динамічного блокування IP-адрес. Практика побудови правил фільтрації. Вплив захисту від перебору на доступність систем та безпеку інформаційного середовища.

Лабораторна робота №5. Аналіз логів для виявлення інцидентів.

Самостійна робота: Відпрацювання матеріалів лекції за темою 6.

**Тема 7. Захист ІКС від аномальної активності. Фільтрація та виявлення підозрілих запитів**

Стисла анотація: Методи виявлення шкідливої активності в реальному часі. Аналіз запитів до вебсервісів. Побудова правил блокування для iptables. Практика виявлення та нейтралізації простих атак типу DoS, сканування або HTTP-флуду.

Лабораторна робота №6. Впровадження системи захисту від перебору.

Самостійна робота: Відпрацювання матеріалів лекції за темою 7.

**Тема 8. Використання штучного інтелекту в системах контроля мережевого трафіку**

Стисла анотація: Виявлення загроз, оптимізація роботи мережі та прогнозування можливих збоїв. Адаптивне управління та балансування навантаження.

Лабораторна робота №7. Впровадження системи захисту від підозрілих запитів.

Самостійна робота: Відпрацювання матеріалів лекції за темою 8.

## 5. Індивідуальні завдання

РГР на тему «Розроблення плану тестування на проникнення компонентів інформаційно-комунікаційної системи».

## 6. Методи навчання

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

## 7. Методи контролю

Проведення поточного контролю, електронного тестування, підсумковий 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 лабораторних робіт | 0...6 | 4 | 0…24 |
| Модульний контроль | 0…20 | 1 | 0…20 |
| **Змістовний модуль 2** | | | |
| Робота на лекціях | 0…0,5 | 8 | 0…4 |
| Виконання і захист лабораторних робіт | 0...6 | 3 | 0…18 |
| Модульний контроль | 0…20 | 1 | 0…20 |
| РГР | 0…10 | 1 | 0…10 |
| **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 запитань та двох практичних запитань (максимальна кількість балів за кожне – 25).

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).** Мати мінімум знань та умінь. Відпрацювати та захистити всі лабораторні роботи. Знати основні загрози безпеки операційних систем. Знати назви стандартів / спільнот, що описують вимоги до кібербезпеки різних систем та надають рекомендації з підвищення

кібербезпеки досліджуваних систем. Знати назви основних інструментальних засобів, що використовуються під час тестування на проникнення.

**Добре (75 - 89).** Твердо знати 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 пояснювати природу походження вразливостей. Вміти складати план тестування на проникнення. Вміти обирати інструментальні засоби тестування на проникнення. Знаходити вразливості за допомогою інструментальних засобів тестування на проникнення.

**Відмінно (90 - 100).** Повно знати основний та додатковий матеріал. Знати усі теми. Орієнтуватися у підручниках та посібниках. Вміти аналізувати сирцевий код та прогнозувати можливі вразливості (статичний аналіз коду). 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.** 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. 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.

**Вирішення конфліктів.** Порядок і процедури врегулювання конфліктів 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. Сторінка дисципліни у системі дистанційного навчання «Ментор» [Ел. ресурс]. URL: https://mentor.khai.edu/course/view.php?id=7365

## 11. Рекомендована література

**Базова**

1. William Shotts. The Linux Command Line, 2nd Edition: A Complete Introduction / No Starch Press, 2019. – 504 p.
2. Christen M., Gordijn B., Loi M. The Ethics of Cybersecurity / edited by Markus Christen, Bert Gordijn, Michele Loi. – Cham : Springer, 2020. – 388 p.
3. ДСТУ ISO/IEC 27001:2023 Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою.
4. Богуш В. М., Богуш В. В., Бровко В. Д., Настрадін В. П. Основи кіберпростору, кібербезпеки та кіберзахисту / Ліра-К, 2021. – 554 с.

**Допоміжна**

1. Козюра В. Д., Хорошко В. О., Шелест М. Є., Ткач Ю. М., Балюнов О.О. Захист інформації в комп'ютерних системах: підручник / Ніжин: ФОП Лук'яненко В.В., ТПК «Орхідея», 2020. – 236 с.

## 12. Інформаційні ресурси

1. Kali Linux Tools Listing [Ел. ресурс]. URL: https://en.kali.tools/
2. National Vulnerability Database [Ел. ресурс]. URL: https://nvd.nist.gov/