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

Операційні 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	4
Мова викладання	Українська
Тип дисципліни	Обов’язкова
Обсяг дисципліни: кредити ЄКТС/ кількість годин	3,5 кредити ЄКТС / 105 годин (48 аудиторних, з яких: лекції – 32, лабораторні – 16; СРЗ – 57)
Види навчальної діяльності	Лекції, лабораторні заняття, самостійна робота
Види контролю	Поточний контроль, модульний контроль, семестровий контроль – іспит
Пререквізити	ОК11 «Архітектура комп’ютерів і квантових процесорів»

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

Мета – ознайомитись з основними загрозами і вразливостями операційних систем, а також прикладного програмного забезпечення. Оволодіти навичками роботи з інструментальними засобами для пошуку вразливостей прикладного програмного забезпечення.

Завдання – знайомство з інструментами тестування безпеки Kali Linux; робота з базами даних вразливостей на прикладі застарілого програмного забезпечення; огляд загроз і вразливостей операційних систем різного типу; знайомство з методами атак на віддалені сервери; пошук вразливостей вебзастосунків; робота з фреймворком тестування безпеки Metasploit; знайомство з методами соціальної інженерії та захисту від них.

Компетентності, які набуваються:

Загальні компетентності (ЗК):

– ЗК1. Здатність застосовувати знання у практичних ситуаціях.

– ЗК2. Знання та розуміння предметної області і розуміння професійної діяльності.

– ЗК3. Здатність спілкуватися державною мовою як усно, так і письмово.

– ЗК4. Здатність спілкуватися іноземною мовою.

– ЗК5. Здатність вчитися і оволодівати сучасними знаннями

Спеціальні компетентності (СК):

– СК3. Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки та захисту інформації.

– СК5. Здатність відновлювати функціонування інформаційних інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв і відмов різних класів та походження.

– СК6. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо).

– СК10. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.

Результати навчання (РН):

– РН1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків.

– РН2. Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації.

– РН12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки.

– РН13. Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних і програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних й інформаційно-комунікаційних систем та/або інфраструктури організації в цілому.

4. Зміст навчальної дисципліни

МОДУЛЬ 1
Змістовний модуль 1. Огляд сучасних проблем безпеки програмного забезпечення

Тема 1. Знайомство з VirtualBox. Встановлення операційної системи Kali Linux

Стисла анотація: Базовий та розширений функціонал засобу віртуалізації VirtualBox. Доповнення гостьової операційної системи. Зміна параметрів жорсткого диска. Закріплення навичок роботи в Linux-подібних системах.

Тема 2. Перелік загальних слабких місць програмного забезпечення. Загальні вразливості та загрози. Бази даних вразливостей

Стисла анотація: Бази CWE та CVE. Класифікація загальних слабких місць програмного забезпечення. Загальна система оцінки вразливостей. Життєвий цикл вразливості. Пошук інформації за відомим ідентифікатором вразливості.

Лабораторна робота №1. Встановлення операційної системи Kali Linux.

Самостійна робота: Відпрацювання матеріалів лекції за темою 2.

Тема 3. Вразливості операційних систем. Огляд специфіки

Стисла анотація: Принципи створення захищених систем. Основні підсистеми комплексу засобів захисту операційної системи. Модель загроз операційної системи. Комплекс засобів захисту операційних систем.

Лабораторна робота №2. Пошук застарілого програмного забезпечення.

Самостійна робота: Відпрацювання матеріалів лекції за темою 3.

Тема 4. Мережеві атаки. Особливості атак та їх наслідки

Стисла анотація: Сценарії здійснення атак та інструменти атак. Атака «людина посередині». Сканування вузлів мережі. Бездротові мережі. Засоби забезпечення безпечної передачі даних у мережі..

Лабораторна робота №3. Вразливості операційних систем.

Самостійна робота: Відпрацювання матеріалів лекції за темою 4.

МОДУЛЬ 2
Змістовний модуль 2. Автоматизовані засоби пошуку проблем безпеки та вплив персоналу на захищеність кіберсистем

Тема 5. Сканери вразливостей вебзастосунків. Поширені проблеми безпеки вебзастосунків

Стисла анотація: Розробки проекту Open Web Application Security Project. Особливості систем керування вмістом як об'єкта дослідження проблем кібербезпеки. Виявлення атак і ліквідація наслідків. Кращі світові практики оцінювання і забезпечення кібербезпеки вебзастосунків. Стандарт PCI DSS.

Лабораторна робота №4. Мережеві атаки.

Самостійна робота: Відпрацювання матеріалів лекції за темою 5.

Тема 6. Виконання команд в операційній системі під час атаки. Фреймворк Metasploit

Стисла анотація: Можливості фреймворку Metasploit під час тестування проблем безпеки. Способи завантаження виконуваної оболонки в операційну систему сервера. Робота з виконуваною оболонкою.

Лабораторна робота №5. Сканери вразливостей вебзастосунків.

Самостійна робота: Відпрацювання матеріалів лекції за темою 6.

Тема 7. Методи соціальної інженерії

Стисла анотація: Актуальні і перспективні техніки соціальної інженерії. Захист від методів соціальної інженерії. Роль штучного інтелекту при виконанні зловмисних дій.

Лабораторна робота №6. Робота з Metasploit.

Самостійна робота: Відпрацювання матеріалів лекції за темою 7.

Тема 8. Штучний інтелект як інструмент захисту

Стисла анотація: Вплив штучного інтелекту при створенні систем захисту інформації.

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

Самостійна робота: Відпрацювання матеріалів лекції за темою 8.

5. Індивідуальні завдання

Не передбачено

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…25	1	0…25
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…25	1	0…25
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 вебзастосунків 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=3726

11. Рекомендована література

Базова

1. Терейковський І. А., Гнатюк С. О. Захист інформації в комп'ютерних системах : навч. посіб. / І. А. Терейковський, С. О. Гнатюк. – Київ : Університет «Україна», 2019. – 220 с.
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. Common Weakness Enumeration [Ел. ресурс]. URL: https://cwe.mitre.org/