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

Кафедра комп'ютерних систем, мереж і кібербезпеки (№ 503)

ЗАТВЕРДЖУЮ

Гарант освітньої програми

_____ Дмитро УЗУН
(підпис) (ім'я та ПРІЗВИЩЕ)

«_31_» ____серпня____2025 р.

СИЛАБУС ОБОВ'ЯЗКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Домени кібербезпеки. Теорія та практика
(назва навчальної дисципліни)

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

Спеціальність: F5 «Кібербезпека та захист інформації»
(код і найменування спеціальності)

Освітньо-професійна програма: «Кібербезпека та захист інформації»
(найменування освітньої програми)

Рівень вищої освіти: **другий (магістерський)**

Силабус введено в дію з 01.09.2025

Харків – 2025 р.

Розробник (и): Узун Д.Д., професор, к.т.н., доцент _____
(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:

_____ Іван ОЛЕФІРЕНКО
(підпис) (ім'я та ПРІЗВИЩЕ)

1. Загальна інформація про викладача

ПІБ: Узун Дмитро Дмитрович

Посада: професор

Науковий ступінь: кандидат технічних наук

Вчене звання: доцент

Перелік дисциплін, які викладає:

Домени кібербезпеки
Технології ДевСекОпс
Технології ДевОпс
Операційні системи
Безпека хмарних технологій
ДевОпс та хмарні технології

Напрями наукових досліджень:

Впровадження сучасних технологій автоматизації циклу розробки та забезпечення стану безпеки ІТ-проектів

Контактна інформація:

d.uzun@khai.edu

2. Опис навчальної дисципліни

Форма здобуття освіти	Денна
Семестр	1
Мова викладання	Українська
Тип дисципліни	Обов’язкова
Обсяг дисципліни: кредити ЄКТС/ кількість годин	3 кредити ЄКТС / 90 годин (48 аудиторних, з яких: лекції – 32, лабораторні – 16; СРЗ – 42)
Види навчальної діяльності	Лекції, лабораторні заняття, самостійна робота
Види контролю	Поточний контроль, модульний контроль, семестровий контроль – іспит
Пререквізити	Дисципліна є обов’язковим компонентом освітньої програми і базується на знаннях, отриманих під час вивчення дисциплін у циклі загальної і професійної підготовки, передбачених навчальним планом спеціальності

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

Мета дисципліни – формування у здобувачів вищої освіти системи теоретичних знань та практичних умінь у сфері кібербезпеки відповідно до основних доменів інформаційної безпеки (згідно з CISSP), а також набуття практичних навичок застосування сучасних засобів виявлення вразливостей, аналізу загроз, моніторингу, тестування на проникнення та забезпечення безпеки інформаційних систем у локальному та хмарному середовищах.

Завдання:

– сформувати знання про основні загрози, вразливості та методи атак на інформаційні системи, мережі та застосунки;
– забезпечити оволодіння теоретичними основами та практичними навичками використання інструментів аналізу безпеки;
– навчити здійснювати пошук, аналіз та оцінювання вразливостей з використанням відкритих баз даних вразливостей;
– сформувати навички аналізу мережевого трафіку за допомогою систем IDS/IPS (Suricata);
– забезпечити набуття практичного досвіду тестування на проникнення та оцінювання рівня захищеності інформаційних систем;
– сформувати компетентності з організації безпечного доступу, захисту даних та моніторингу подій безпеки у хмарних середовищах (AWS);
– розвинути здатність аналізувати інциденти інформаційної безпеки та приймати обґрунтовані рішення щодо реагування та мінімізації їх наслідків.

Компетентності, які набуваються:

Інтегральна компетентність:

Здатність особи розв’язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки.

Загальні компетентності (ЗК):

ЗК1. Здатність до адаптації та дій в новій ситуації.
ЗК2. Здатність до абстрактного мислення, аналізу і синтезу.
ЗК3. Здатність проводити дослідження на відповідному рівні.
ЗК4. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
ЗК5. Здатність генерувати нові ідеї (креативність).
ЗК6. Здатність виявляти, ставити та вирішувати проблеми.
ЗК7. Здатність приймати обґрунтовані рішення.
ЗК8. Здатність спілкуватися іноземною мовою.

Спеціальні компетентності (СК):

СК2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного

спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки.

СК10. Здатність проводити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки.

Програмні результати навчання (ПРН):

ПРН1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.
ПРН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.
ПРН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.
ПРН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.
ПРН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.
ПРН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.
ПРН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.
ПРН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.
ПРН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
ПРН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і

технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.
ПРН15. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб.
ПРН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.
ПРН17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об’єктивно оцінювати результати навчання.
ПРН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.
ПРН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.
ПРН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.
ПРН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.
ПРН25. Аналізувати, обґрунтовувати вибір, розробляти і впроваджувати методи і засоби розгортання безпечних хмарних та інших ІТ-інфраструктур.

4. Зміст навчальної дисципліни

МОДУЛЬ 1
Змістовний модуль 1.

Тема 1. Вступ до дисципліни. Домени кібербезпеки.

Анотація: Розглядається роль кібербезпеки в сучасному цифровому середовищі, основні типи загроз і кібератак, а також актуальні виклики для організацій і користувачів. Аналізуються міжнародні стандарти та принципи кібербезпеки, етичні аспекти діяльності фахівця з безпеки. Окрема увага приділяється доменам кібербезпеки відповідно до моделі CISSP та їх взаємозв'язку.
Тема лекції 1: Основи кібербезпеки та домени CISSP.
Самостійна робота здобувача: Опрацювання лекційного матеріалу, підготовка короткого огляду основних доменів кібербезпеки.

Тема 2. Віртуалізація та підготовка лабораторного середовища

Анотація: Вивчаються основи віртуалізації та її роль у кібербезпеці. Розглядаються типи гіпервізорів, принципи роботи віртуальних машин та їх застосування для навчання і тестування. Аналізуються особливості встановлення VirtualBox або VMware, а також процес інсталяції Kali Linux або Parrot OS.
Тема лекції 2: Основи віртуалізації та гіпервізори.
Тема лекції 3: Встановлення та налаштування Kali Linux (Parrot OS).
Самостійна робота здобувача: Встановлення гіпервізора та створення віртуальної машини з Kali Linux.

Тема 3. Командний рядок Linux для фахівця з кібербезпеки

Анотація: Розглядаються основи роботи з командним рядком Linux, структура файлової системи, типові адміністративні команди та утиліти. Вивчаються команди навігації, керування файлами, процесами та користувачами, а також базові принципи автоматизації.
Тема лекції 4: Основи командного рядка Linux.
Самостійна робота здобувача: Виконання базових команд роботи з файлами, каталогами та процесами.

Тема 4. Вразливості та оцінювання безпеки

Анотація: Вивчається поняття вразливості, її життєвий цикл та роль у кібератаках. Розглядаються методи оцінювання вразливостей, використання

баз даних CVE, NVD та інших публічних ресурсів. Аналізуються принципи роботи сканерів вразливостей та їх практичне застосування.
Тема лекції 5: Основи вразливостей і бази даних CVE/NVD.
Тема лекції 6: Сканери вразливостей і методи оцінювання.
Самостійна робота здобувача: Аналіз опису вразливості з бази CVE та визначення її рівня критичності.

Тема 5. Основи комп'ютерних мереж та аналіз трафіку

Анотація: Розглядається модель OSI, основні мережеві протоколи та принципи передачі даних у мережі. Вивчаються методи перехоплення та аналізу мережевого трафіку, фільтрація пакетів та базовий синтаксис інструментів tcpdump і Wireshark.
Тема лекції 7: Модель OSI та мережеві протоколи.
Тема лекції 8: Аналіз мережевого трафіку з tcpdump і Wireshark.
Лабораторна робота 1: Перехоплення та аналіз мережевого трафіку у тестовому середовищі.
Самостійна робота здобувача: ознайомлення з функціонуванням моделі OSI та мережевими протоколами за допомогою tcpdump і Wireshark.

Тема 6. Сканування мережі та засоби виявлення вторгнень.

Анотація:
Вивчаються принципи сканування мереж, виявлення активних хостів і відкритих портів. Розглядаються техніки сканування, визначення версій сервісів, ідентифікація операційної системи та використання скриптів (Nmap). Аналізуються найкращі практики енумерації. Наводяться основи та приклади використання систем виявлення та протидії вторгненням (Suricata).
Тема лекції 9: Основи сканування мережі та виявлення хостів.
Лабораторна робота 2: Виконання різних типів сканування Nmap і аналіз результатів у лабораторному середовищі.
Тема лекції 10: Поглиблене сканування, NSE-скрипти та енумерація.
Лабораторна робота 3: Базове налаштування IDS/IPS Suricata для аналізу трафіку, що генерує використання Nmap у лабораторному середовищі.
Самостійна робота здобувача: ознайомлення з функціонуванням nmap та встановлення взаємозв'язку з tcpdump і Wireshark.

МОДУЛЬ 2
Змістовний модуль 2.

Змістовний модуль 2. Безпека хмарної інфраструктури AWS

Тема 7. Безпечний доступ до хмарних ресурсів AWS

Анотація: Розглядається модель спільної відповідальності у хмарі AWS. Вивчаються принципи управління ідентифікацією та доступом (IAM), політики безпеки на основі сутностей і ресурсів, а також практики безпечної аутентифікації.
Тема лекції 11: Модель спільної відповідальності та IAM.
Лабораторна робота 4: Використання політик на основі ресурсів для захисту S3-бакета.
Самостійна робота здобувача: Налаштування користувачів і ролей у тестовому середовищі AWS.

Тема 8. Захист інфраструктури в AWS

Анотація: Вивчається глобальна інфраструктура AWS, принципи сегментації мережі та захисту ресурсів. Розглядаються механізми контролю доступу, групи безпеки, мережеві ACL та базові засоби захисту інфраструктури.
Тема лекції 12: Мережева архітектура та захист ресурсів у AWS.
Лабораторна робота 5: Захист ресурсів VPC за допомогою груп безпеки.
Самостійна робота здобувача: Налаштування базових політик безпеки в тестовій інфраструктурі.

Тема 9. Захист даних у хмарних застосунках

Анотація: Розглядаються принципи захисту даних під час зберігання та передачі. Вивчаються механізми шифрування, управління ключами та сервіси AWS для забезпечення конфіденційності й цілісності даних.
Тема лекції 13: Шифрування та захист даних у AWS.
Лабораторна робота 6: Шифрування даних під час зберігання за допомогою AWS KMS.
Самостійна робота здобувача: Аналіз варіантів шифрування для різних типів ресурсів.

Тема 10. Логування, моніторинг та реагування на інциденти в AWS

Анотація: Вивчаються сервіси логування та моніторингу в AWS, їх роль у забезпеченні безпеки та виявленні інцидентів. Розглядаються принципи реагування на інциденти, автоматизації процесів безпеки та використання допоміжних сервісів.
Тема лекції 14: Логування та моніторинг у AWS.
Лабораторна робота 7: Моніторинг та сповіщення за допомогою CloudTrail і CloudWatch.
Тема лекції 15: Реагування на інциденти в хмарному середовищі.
Лабораторна робота 8: Усунення інциденту за допомогою AWS Config і Lambda.

Самостійна робота здобувача: Аналіз журналів подій та моделювання сценарію реагування.

Тема 11. Професійні сертифікації у сфері кібербезпеки та хмарних технологій

Анотація: Розглядаються основні міжнародні сертифікації у сфері кібербезпеки, мережевих технологій та хмарних сервісів. Аналізуються напрями сертифікацій для початківців і фахівців середнього рівня: CompTIA, Cisco, AWS, (ISC)² та інші.

Тема лекції 16: Огляд міжнародних сертифікацій з кібербезпеки та хмарних технологій.

Самостійна робота здобувача: Аналіз вимог обраної сертифікації (наприклад, Security+, CCNA, AWS Cloud Practitioner, AWS Cloud Security), підготовка короткого плану особистої траєкторії сертифікації.

5. Індивідуальні завдання

Не передбачено

6. Методи навчання

Проведення аудиторних лекцій, лабораторних 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			
Виконання і захист лабораторних робіт	0…8	3	0…24
Модульний контроль	0…26	1	0…26
Змістовний модуль 2			
Виконання і захист лабораторних робіт	0…8	3	0…24
Модульний контроль	0…26	1	0…26
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 (максимальна кількість балів за кожне – 25), та практичного запитання (максимальна кількість балів – 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) – Показати мінімум знань та умінь. Захистити не менше 50% від усіх завдань лабораторних занять. Знати основні складові дисципліни. Уміти користуватись інструментальними засобами, що розглянуті в курсі.

Добре (75-89) – Знати та розуміти теоретичну частину, захистити не менше 75% завдань лабораторних занять. Знати ключові концепції кожного модуля курсу. Вміти обґрунтовано впроваджувати потрібні інструментальні засоби відповідно до поставленої задачі.

Відмінно (90-100) – Здати всі контрольні точки з оцінкою «відмінно». Досконально знати всі теми та уміти їх застосовувати. Вміти обґрунтовано користуватись інструментальними засобами з метою їх інтеграції при проведенні комплексного дослідження стану кібербезпеки ІТ-рішень.

9. Політика навчального курсу

Відвідування занять. Інтерактивний характер курсу передбачає обов'язкове відвідування лабораторних занять. Здобувачі освіти, які за певних обставин не можуть відвідувати лабораторні 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=3695

11. Рекомендована література

Базова

1. Tarandach I., Coles M. Threat Modeling. A Practical Guide for Development Teams. O'Reilly, 2021. 208 p
2. Messier R. Learning Kali Linux. O'Reilly; 2024. 520 p
3. Hoffman A. Web Application Security. O'Reilly; 2024. 444 p
4. Berlin A., Brotherston L., Defensive Security Handbook. O'Reilly; 2024. 363 p
5. Armitage J. Cloud Native Security Cookbook. O'Reilly; 2022. 516 p

Допоміжна

1. Dotson C. Practical Cloud Security. O'Reilly; 2024. 231 p

12. Інформаційні ресурси

1. CISSP Domains [Ел. ресурс].URL: URL:https://destcert.com/resources/8-cissp-domains-explained/
2. Kali Linux [Ел. ресурс]. URL: https://www.kali.org/docs/
3. AWS Academy [Ел. ресурс].URL: https://www.awsacademy.com/
4. MITRE ATT&CK [Ел. ресурс].URL: https://attack.mitre.org/
5. OWASP Top 10:2025 [Ел. ресурс].URL: https://owasp.org/Top10/
6. NVD [Ел. ресурс].URL: https://nvd.nist.gov/