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

Кафедра інформаційно-комунікаційних технологій
ім. О. О. Зеленського (№ 504)

ЗАТВЕРДЖУЮ

Гарант освітньої програми

_____ Олександр ТОЦЬКИЙ
(підпис) (ім'я та прізвище)

28 серпня 2025 р.

СИЛАБУС ОБОВ'ЯЗКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Кібербезпека інфокомунікаційних систем

(назва навчальної дисципліни)

Галузь знань: G «Інженерія, виробництво та будівництво»
(шифр і найменування галузі знань)

Спеціальність: G5 «Електроніка, електронні комунікації, приладобудування та радіотехніка»
(код і найменування спеціальності)

Освітньо-професійна програма: «Інформаційні мережі зв'язку»
(найменування освітньої програми)

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

Силабус введено в дію з 01.09.2025

Харків – 2025 р.

Розробник: Рубель А. С., старший викладач, доктор філософії
(прізвище та ініціали, посада, науковий ступінь і вчене звання) (підпис)

Силабус навчальної дисципліни розглянуто на засіданні кафедри інформаційно-комунікаційних технологій ім. О. О. Зеленського (№ 504)
(назва кафедри)

Протокол № 1 від « 28 » серпня 2025 р.

Завідувач кафедри д.т.н., професор (науковий ступінь і вчене звання) (підпис) Володимир ЛУКІН (ім'я та прізвище)

Погоджено з представником здобувачів освіти:

(підпис) Кирило МЕЗЕНЦЕВ (ім'я та прізвище)

1. Загальна інформація про викладача

ПІБ: Рубель Андрій Сергійович
Посада: старший викладач
Науковий ступінь: доктор філософії (PhD)
Вчене звання: -
Перелік дисциплін, які викладає: *Цифрова обробка сигналів (КР); Основи машинного навчання; Програмування мобільних додатків; Кібербезпека інфокомунікаційних систем*
Напрями наукових досліджень: *цифрова обробка зображень, цифрова обробка сигналів, машинне навчання*
Контактна інформація: a.rubel@khai.edu

2. Опис навчальної дисципліни

Форма здобуття освіти	Денна
Семестр	2-й
Мова викладання	Українська
Тип дисципліни	Обов’язкова
Обсяг дисципліни: кредити ЄКТС/ кількість годин	5 кредитів ЄКТС / 150 годин (64 аудиторних, з яких: лекції – 32, практичні – 32; СРЗ – 86)
Види навчальної діяльності	Лекції, практичні заняття, самостійна робота
Види контролю	Поточний контроль, модульний контроль, семестровий контроль – іспит
Пререквізити	«Інтернет речей», «Хмарні інформаційні системи»

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

Мета – набуття студентами знань, вмінь і навичок, використання їх у своїй практичній роботі, пов'язаній з виявленням порушень кібербезпеки і реагуванням на події безпеки, керуванням системами безпеки, роботою аналітика безпеки молодшого рівня, який працює в центрі моніторингу та управління безпекою (SOC).

Завдання – вивчення основних методів оцінки, виявлення та реагування на загрози безпеки мереж і кінцевих пристроїв, а також опанування сучасних інструментів моніторингу і реагування на події безпеки.

Компетентності, які набуваються:

Інтегральна компетентність:

Здатність розв’язувати складні задачі та проблеми в галузі побудови інформаційних мереж зв’язку, що передбачає проведення досліджень та/або здійснення інновацій при застосуванні методів і принципів побудови та оптимізації сучасних технологій розподілу і обробки інформації.

Загальні компетентності (ЗК)

Після закінчення цієї програми здобувач освіти буде здатен:

- навички використання інформаційних і комунікаційних технологій;
- здатність досліджувати проблеми з використанням системного аналізу, синтезу, комп’ютерного моделювання та методів оптимізації;
- здатність аналізувати, верифікувати, оцінювати повноту інформації та працювати в умовах невизначеності;
- знання іншої мови(мов).

Спеціальні компетентності

Після закінчення цієї програми здобувач освіти буде здатен:

- здатність застосовувати відповідні математичні, наукові і технічні методи, а також комп’ютерне програмне забезпечення для вирішення завдань в сфері розподілу і обробки інформації;
- здатність визначати ефективність рішень в сфері розподілу і обробки інформації з використання аналітичних методів і методів моделювання;
- здатність продемонструвати знання і розуміння математичних принципів і методів, необхідних для підтримки спеціалізацій з телекомунікацій.

Програмні результати навчання:

- спроможність аналізувати складні інженерні задачі, процеси і системи відповідно до спеціалізації; обирати і застосовувати придатні типові аналітичні, розрахункові та експериментальні методи; уміння інтерпретувати результати таких досліджень;

- знання основних принципів реалізації інформаційних та телекомунікаційних мереж на різних етапах життєвого циклу;

- знання основних принципів організації і побудови інформаційно-комунікаційних систем, вміння враховувати особливості галузей їх застосування, визначати характеристики систем і окремих їх модулів;

- знання принципів керування інформаційними мережами, керування та методів оцінювання якості їх функціонування та надання послуг;

- знання принципів побудови сервісних платформ інформаційних мереж;

- знати та уміти застосовувати засоби сучасних інформаційних технологій для вирішення задач в сфері інформаційно-комунікаційних технологій;

- здатність ефективно застосовувати роботу з комп'ютером, його технічним та програмним забезпеченнями (носіями інформації, базами даних тощо).

4. Зміст навчальної дисципліни

МОДУЛЬ 1

Змістовний модуль 1. Зловмисники і захисники

Тема 1. Небезпека

В основу дисципліни покладено курс CyberOps Associate мережевої академії Cisco, що є світовим лідером у галузі мережних технологій.

Основні питання: Предмет вивчення і задачі дисципліни. Місце дисципліни в учбовому плані. Історії атак. Суб'єкти загроз. Вплив загроз.

Лекція № 1. Вступ до дисципліни. Атаки і загрози. Операційний центр безпеки (SOC).

Самостійна робота здобувача освіти: опрацювання матеріалу лекції.

Тема 2. Бійці у війні проти кіберзлочинності.

Сучасний Операційний центр безпеки (SOC). Елементи, люди і процес в SOC. Основні ролі в центрі моніторингу та управління безпекою. Задачі аналітиків різних рівнів. Функцію центру моніторингу та управління безпекою. Технології в SOC – SIEM. Технології в SOC – SOAR. Метрики SOC.

Лекція № 1. Вступ до дисципліни. Атаки і загрози. Центри моніторингу та управління безпекою (SOC).

Самостійна робота здобувача освіти: опрацювання матеріалу лекції, підготовка до модульної контрольної роботи.

Модульний контроль 1 «Зловмисники і захисники».

Змістовний модуль 2. Огляд операційних систем Windows і Linux

Тема 3. Операційна система Windows.

Архітектура та работа ОС Windows. Конфігурація та моніторинг Windows: інтерфейс командного рядка та PowerShell, інструментарій керування Windows. Безпека Windows: команда netstat, локальна політика безпеки, Windows Defender.

Лекція № 2. Огляд операційних систем Windows і Linux.

Самостійна робота здобувача освіти: опрацювання матеріалу лекції.

Тема 4. Огляд Linux.

Linux у SOC. Робота у shell. Лекція № 2. Огляд операційних систем Windows і Linux. Сервери, сервіси і їх порти. Базове адміністрування Linux сервера. Шкідливе програмне забезпечення на Linux хості.

Лекція № 2. Огляд операційних систем Windows і Linux.

Практична робота «Linux-сервери».

Практична робота «Пошук файлів журналів».

Практична робота «Навігація у файловій системі Linux та встановлення дозволів».

Самостійна робота здобувача освіти: опрацювання матеріалу лекції, виконання практичних робіт, підготовка до модульної контрольної роботи.

Модульний контроль 2 «Огляд операційних систем Windows і Linux».

Змістовний модуль 3. Основи комп'ютерних мереж

Тема 5. Мережні протоколи

Мережні комунікації. Протоколи зв'язку. Стек протоколів TCP/IP. Форматування та інкапсуляція повідомлення. Синхронізація повідомлень. Unicast, Multicast, та Broadcast. Еталонна модель OSI. Протокольна модель TCP/IP. Інкапсуляція даних. Сегментація повідомлень. Протокольні блоки даних (Protocol Data Units).

Лекція № 3. Мережні протоколи. Ethernet та Internet Protocol (IP).

Практична робота «Знайомство з Wireshark».

Самостійна робота здобувача освіти: опрацювання матеріалу лекції, виконання практичної роботи.

Тема 6. Ethernet та Internet Protocol (IP)

Ethernet. Інкапсуляція Ethernet. Поля кадру Ethernet. Формат MAC-адреси. IPv4. IP інкапсуляція. Характеристики IP-протоколу. Заголовок пакета IPv4. Поля заголовка пакета IPv4. Основи IP-адресації. Типи адрес IPv4. Шлюз за замовчуванням. Таблиці маршрутизації хоста. IPv6. Формати адрес IPv6. Довжина префікса IPv6.

Лекція № 3. Мережні протоколи. Ethernet та Internet Protocol (IP).

Самостійна робота здобувача освіти: опрацювання матеріалу лекції.

Тема 7. Перевірка підключення

Протокол ICMP. ICMPv4 повідомлення. RS та RA повідомлення ICMPv6. Утиліти Ping та Traceroute. Тестування мережі та перевірка командами CLI. Утиліта Traceroute - Тестування шляху.

Лекція № 4. Перевірка підключення. Протокол визначення адрес ARP.

Самостійна робота здобувача освіти: опрацювання матеріалу лекції.

Тема 8. Address Resolution Protocol (Протокол визначення адрес)

MAC- та IP-адреси. Вузол призначення в тій же мережі. Вузол призначення у віддаленій мережі. Протокол ARP: огляд, функції. Роль ARP в обміні даними з віддаленим хостом. ARP - таблиці на мережних пристроях.

Лекція № 4. Перевірка підключення. Протокол визначення адрес ARP.

Практична робота «Використання Wireshark для дослідження кадрів Ethernet».

Самостійна робота здобувача освіти: опрацювання матеріалу лекції, виконання практичної роботи.

Тема 9. Транспортний рівень

Характеристики транспортного рівня Роль і обов'язки транспортного рівня. Протоколи транспортного рівня. Протокол керування передаванням (Transmission Control Protocol, TCP). Заголовок TCP. Поля заголовка TCP. Протокол користувацьких дейтаграм (User Datagram Protocol, UDP).UDP-заголовок. Поля заголовка UDP. Пари сокетів. Створення сеансу транспортного шару. Встановлення TCP-з'єднання. Закриття сеансу. Надійність TCP - Гарантована і впорядкована доставка. Керування потоком TCP.

Лекція № 5. Транспортний рівень. Протоколи TCP і UDP. Мережні сервіси.

Практична робота «Використання Wireshark для спостереження за тристороннім рукостисканням TCP».

Самостійна робота здобувача освіти: опрацювання матеріалу лекції, виконання практичної роботи.

Тема 10. Мережні сервіси

Протокол динамічного налаштування вузла (DHCP). Принципи роботи протоколу DHCP. Формат повідомлення DHCP. Огляд DNS. Ієрархія DNS. Формат DNS-повідомлень. Динамічний DNS. Протокол WHOIS. Приватний адресний простір IPv4. NAT. Трансляція адреси і номера порту (PAT). Протоколи FTP та TFTP. Протокол блоку серверних повідомлень (SMB). Електронна пошта. Протоколи електронної пошти SMTP, POP3, IMAP. Протокол передавання гіпертексту (HTTP). Принцип роботи протоколу HTTP. Коди стану HTTP. HTTP/2 . Захист HTTP - HTTPS.

Лекція № 5. Транспортний рівень. Протоколи TCP і UDP. Мережні сервіси.

Практична робота «Використання Wireshark для дослідження захоплених UDP DNS повідомлень».

Практична робота «Використання Wireshark для дослідження TCP та UDP захоплених пакетів».

Практична робота «Використання Wireshark для дослідження HTTP та HTTPS трафіку».

Самостійна робота здобувача освіти: опрацювання матеріалу лекції, виконання практичних робіт, підготовка до модульної контрольної роботи.

Модульний контроль 3 «Основи комп'ютерних мереж».

Змістовний модуль 4. Інфраструктура мережної безпеки

Тема 11. Пристрої мережевого з'єднання

Мережні пристрої. Кінцеві пристрої. Маршрутизатори. Робота комутації. Мережі VLAN. Бездротові з'єднання. Структура кадру 802.11. CSMA/CA.

Лекція № 6. Мережні пристрої. Інфраструктура мережної безпеки.

Самостійна робота здобувача освіти: опрацювання матеріалу лекції.

Тема 12. Інфраструктура мережної безпеки

Мережні топології. Трирівнева модель проектування мереж. Загальновідомі безпекові архітектури. Пристрої безпеки. Міжмережні екрани. Пристрої запобігання та виявлення вторгнень. Переваги та недоліки IDS та IPS. Служби безпеки. Контроль трафіку за допомогою ACL. Протокол SNMP. NetFlow. Дзеркалювання портів. Сервери Syslog. Протокол NTP. AAA-сервери. VPN.

Лекція № 6. Мережні пристрої. Інфраструктура мережної безпеки.

Самостійна робота здобувача освіти: опрацювання матеріалу лекції, підготовка до модульної контрольної роботи.

Модульний контроль 4 «Інфраструктура мережної безпеки».

Змістовний модуль 5. Загрози та атаки

Тема 13. Зловмисники та їхні інструменти

Загрози, вразливість та ризик. Кіберзлочинці. Завдання кібербезпеки. Індикатори кіберзагроз. Інструменти зловмисників. Огляд інструментів атак. Категорії атак.

Лекція № 7. Загрози і атаки.

Самостійна робота здобувача освіти: опрацювання матеріалу лекції.

Тема 14. Типові загрози і атаки

Типи шкідливого програмного забезпечення. Віруси. Троянські коні. Хробаки. Програми - вимагачі.

Лекція № 7. Загрози і атаки.

Самостійна робота здобувача освіти: опрацювання матеріалу лекції.

Тема 15. Моніторинг мережі та інструменти моніторингу

Загальні відомості про моніторинг мережі. Топологія мережної безпеки. Методи моніторингу мережі. Мережні відгалуджувачі. Дзеркалювання трафіку та SPAN. Інструменти моніторингу мережної безпеки. Аналізатори мережних протоколів. NetFlow. SIEM і SOAR.

Лекція № 8. Моніторинг мережі та інструменти моніторингу. Атаки на базові функції, IP-сервіси і корпоративні сервіси.

Самостійна робота здобувача освіти: опрацювання матеріалу лекції.

Тема 16. Атаки на базові функції

Вразливості IP. Атаки на основі ICMP. Атаки за методом підсилення та відбиття. Атаки з підміною адрес. Вразливості TCP та UDP.

Лекція № 8. Моніторинг мережі та інструменти моніторингу. Атаки на базові функції, IP-сервіси і корпоративні сервіси.

Самостійна робота здобувача освіти: опрацювання матеріалу лекції.

Тема 17. Атаки на те, що ми робимо

IP-сервіси. Вразливості ARP. Отруєння ARP-кешу. Атаки на основі DNS. Тунелювання DNS (DNS Tunneling). Атаки, пов'язані з DHCP. Атаки, пов'язані з DHCP. Поширені експлойти HTTP. Скрипти на стороні клієнта.

Лекція № 8. Моніторинг мережі та інструменти моніторингу. Атаки на базові функції, IP-сервіси і корпоративні сервіси.

Практична робота «Дослідження DNS-трафіку».

Самостійна робота здобувача освіти: опрацювання матеріалу лекції, виконання практичної роботи, підготовка до модульної контрольної роботи.

Модульний контроль 5 «Загрози та атаки»

Змістовний модуль 6. Захист мережі

Тема 18. Розуміння захисту

Поглиблений захист. Активи, вразливості, загрози. Ідентифікація активів. Визначення вразливостей. Визначення загроз. Підхід Поглибленого захисту. Аналогії «цибуля безпеки» та «артишок безпеки». Політики безпеки, правила та стандарти. Політики BYOD.

Лекція № 9. Поглиблений захист. Керування доступом та аналіз загроз.

Самостійна робота здобувача освіти: опрацювання матеріалу лекції.

Тема 19. Керування доступом

Концепції контролю доступу. Безпека передачі даних - CIA. Концепція безпеки - Нульова довіра. Моделі контролю доступу. Використання та принципи роботи AAA.

Лекція № 9. Поглиблений захист. Керування доступом та аналіз загроз.

Самостійна робота здобувача освіти: опрацювання матеріалу лекції.

Тема 20. Аналіз загроз

Джерела Інформації. Служби кіберрозвідки. Cisco Talos. FireEye. База даних вразливостей (CVE). Стандарти обміну даними для аналітики кіберзагроз. Платформи аналітики кіберзагроз.

Лекція № 9. Поглиблений захист. Керування доступом та аналіз загроз.

Самостійна робота здобувача освіти: опрацювання матеріалу лекції, підготовка до модульної контрольної роботи.

Модульний контроль 6 «Захист мережі»

Змістовний модуль 7. Криптографія та захист кінцевої точки

Тема 21. Криптографія

Цілісність і автентичність. Захист передавання даних. Криптографічні хеш-функції. Аутентифікація джерела. Конфіденційність даних. Симетричне шифрування. Асиметричне шифрування. Алгоритм Діффі-Геллмана. Криптографія з відкритим ключем. Цифрові підписи для підписання коду. Цифрові підписи для цифрових сертифікатів. Центри сертифікації і довірча система PKI. Інфраструктура відкритих ключів. Взаємодія різних постачальників PKI. Реєстрація, аутентифікація і відкликання сертифікатів.

Лекція № 10. Криптографія

Практична робота «Сховища центрів сертифікації».

Самостійна робота здобувача освіти: опрацювання матеріалу лекції, виконання практичної роботи.

Тема 22. Захист кінцевої точки

Захист від зловмисних програм. Загрози для кінцевих точок. Безпека кінцевих точок. Захист від зловмисного ПЗ на основі вузла. Мережний захист від шкідливих програм. Запобігання вторгненням на основі вузла. Функціонування HIDS. Безпека застосунків. Поверхня вразливості до атак. Застосування чорного та білого списків застосунків. Ізоляція в «пісочниці» на основі системи.

Лекція № 11. Захист кінцевої точки та оцінки вразливості кінцевої точки.

Самостійна робота здобувача освіти: опрацювання матеріалу лекції.

Тема 23. Оцінка вразливості кінцевої точки

Профілювання мережі та сервера. Виявлення аномалій в мережі. Тестування мережі на вразливості. Загальна система оцінки вразливостей (CVSS). Безпечне керування пристроями. Управління вразливостями. Управління ресурсами. Управління мобільними пристроями. Управління конфігураціями. Системи управління інформаційною безпекою (СУІБ). ISO-27001. Фреймворк кібербезпеки NIST.

Лекція № 11. Захист кінцевої точки та оцінки вразливості кінцевої точки.

Самостійна робота здобувача освіти: опрацювання матеріалу лекції, підготовка до модульної контрольної роботи.

Модульний контроль 7 «Криптографія та захист кінцевої точки».

Змістовний модуль 8. Протоколи та файли журналу

Тема 24. Технології та протоколи

Моніторинг основних протоколів: Syslog та NTP, DNS, HTTP і HTTPS, протоколи електронної пошти, ICMP. Технології безпеки. ACL. NAT та PAT. Шифрування, інкапсуляція та тунелювання. Однорангові мережі та Tor.

Лекція № 12. Технології та протоколи.

Самостійна робота здобувача освіти: опрацювання матеріалу лекції.

Тема 25. Дані про безпеку мережі

Типи даних про безпеку. Дані сеансу та транзакції. Повне захоплення пакетів. Статистичні дані. Журнали кінцевих пристроїв. Syslog. SIEM і збирання журналів. Мережні журнали. Tcpdump. NetFlow. Журнали фільтрування вмісту. Журнали проксі (Proxy Logs). Міжмережні екрани нового покоління.

Лекція № 13. Дані про безпеку мережі.

Самостійна робота здобувача освіти: опрацювання матеріалу лекції, підготовка до модульної контрольної роботи.

Модульний контроль 8 «Протоколи та файли журналу».

Змістовний модуль 9. Аналіз даних безпеки

Тема 26. Оцінка сповіщень

Джерела сповіщень. Security Onion. Інструменти виявлення для збирання даних сповіщень. Інструменти аналізу. Генерація сповіщень. Правила та сповіщення. Структура правила Snort. Оцінювання сповіщень.

Лекція № 14. Оцінка сповіщень

Практична робота «Правила Snort та правила міжмережного екрану».

Самостійна робота здобувача освіти: опрацювання матеріалу лекції, виконання практичної роботи.

Тема 27. Робота з даними про безпеку мережі

Спільна платформа даних. Стек ELK (Elasticsearch, Logstash і Kibana). Перетворення даних. Нормалізація даних. Архівування даних. Дослідження даних мережі. Робота у Sguil. Робота в ELK. Дослідження процесів або викликів API. Докладне дослідження файлу. Активізація роботи аналітика з кібербезпеки.

Лекція № 15. Робота з даними про безпеку мережі

Практична робота «Вилучення виконуваного файлу з PCAP».

Практична робота «Інтерпретація даних HTTP та DNS для ізоляції нападників».

Практична робота «Ізоляція скомпрометованого хоста за допомогою кортежу із 5-ти елементів».

Практична робота «Дослідження атаки на хост Windows».

Самостійна робота здобувача освіти: опрацювання матеріалу лекції, виконання практичних робіт.

Тема 28. Цифрова технічна експертиза та аналіз інцидентів і реагування

Робота з доказами та атрибуція атаки. Цифрова технічна експертиза. Процес цифрової технічної експертизи. Типи доказів. Послідовність збору доказів. Ланцюжок забезпечення збереження доказів. Цілісність та збереження даних. Атрибуція атаки. Ланцюжок кібервбивства. Ромбоподібна модель аналізу вторгнення. Реагування на інциденти. Життєвий цикл реагування на інциденти NIST. Вимоги до звітності та обмін інформацією.

Лекція № 16. Цифрова технічна експертиза та аналіз інцидентів і реагування

Самостійна робота здобувача освіти: опрацювання матеріалу лекції, підготовка до модульної контрольної роботи.

Модульний контроль 9 «Аналіз даних безпеки».

5. Індивідуальні завдання

Не передбачені навчальним планом.

6. Методи навчання

Використовуються наступні методи навчання: словесні, наочні та практичні, а саме: проведення лекцій (із застосуванням пояснювально-ілюстративного та проблемного викладання навчального матеріалу), робота на практичних заняттях (із застосуванням як репродуктивного методу, так і проблемного викладання), консультації протягом семестру, самостійна робота за матеріалами, опублікованими кафедрою, та матеріалами мережевої академії Cisco (конспекти, інтерактивні вправи, тестові завдання, навчальні відеофільми тощо), використання мережі Internet.

7. Методи контролю

Поточний контроль: виконання практичних завдань, контроль засвоєння навчального матеріалу, запланованого на самостійне опрацювання студентом.

Контроль:

- поточний контроль (оцінювання роботи студентів на практичних заняттях);;

- модульний контроль за змістовними модулями

Семестровий контроль – іспит (проводиться у формі тестових завдань).

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			
Модульний контроль (теми 1–2)	0…4	1	**0…4**
Змістовний модуль 2			
Виконання практичних робіт	0…3	3	**0…9**
Модульний контроль (теми 3-4)	0…4	1	**0…4**
Змістовний модуль 3			
Виконання практичних робіт	0…3	6	**0…18**
Модульний контроль (тема 5-10)	0…4	1	**0…4**
Змістовний модуль 4			
Модульний контроль (тема 11-12)	0…4	1	**0…4**
Змістовний модуль 5			
Виконання практичних робіт	0…3	1	**0…3**
Модульний контроль (теми 13-17)	0…4	1	**0…4**
Змістовний модуль 6			
Модульний контроль (тема 18-20)	0…4	1	**0…4**
Змістовний модуль 7			
Виконання практичних робіт	0…3	1	**0…3**
Модульний контроль (тема 21-23)	0…4	1	**0…4**
Змістовний модуль 8			
Модульний контроль (тема 24-25)	0…4	1	**0…4**
Змістовний модуль 9			
Виконання практичних робіт	0…3	5	**0…15**
Модульний контроль (тема 26-28)	0…4	1	**0…4**
Підсумковий контроль	0…16	1	**0…16**
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 60 запитань (теоретичних питань та практичних завдань) з 4 – 6 варіантами відповідей (окремі питання потребують вибору декількох правильних відповідей). За кожну вірну відповідь здобувач отримує 1 бал (сума – 100 балів).

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 мінімально-достатній рівень знань та умінь. Вміти викладати отримані знання в усній чи письмовій формі; при цьому неповний обсяг засвоєного навчального матеріалу не повинен перешкоджати засвоєнню наступного програмного матеріалу; допускаються окремі істотні помилки, виправлені за допомогою викладача. Виконати всі практичні роботи з навчальної дисципліни. Відповідати на теоретичні питання на елементарному рівні в межах конспекту лекцій. Вирішувати найпростіші задачі модульного контролю. Скласти підсумковий модульний контроль з результатом не менше 60% успішності. Вміти пояснити типові алгоритми та програмні рішення, що використовувалися під час виконання практичних робіт.

Добре (75-89). Показати середній рівень знань та умінь. Викладати отримані знання в усній чи письмовій формі у достатньому обсягу, системно, відповідно до вимог навчальної програми (допускаються окремі несуттєві помилки, що виправляються студентом після указівки викладача). Виділяти істотні ознаки вивченого за допомогою операцій аналізу і синтезу; підкріпляти вивчений матеріал відомими фактами і відомостями; виявляти причинно-наслідкові зв'язки досліджуваних процесів та явищ; формулювати висновки і узагальнення, у яких можуть бути окремі несуттєві помилки. Виконати всі практичні роботи з навчальної дисципліни. Відповідати на теоретичні питання на достатньому рівні в межах конспекту лекцій та рекомендованих підручників, вміти обґрунтовано обирати типові рішення. Вирішувати задачі модульного контролю середнього рівня складності. Скласти підсумковий модульний контроль з результатом не менше 75% успішності. Вміти застосовувати типові алгоритми та програмні рішення, подібні використовуваним на практичних заняттях.

Відмінно (90-100). Показати відмінний рівень знань та умінь. Викладати отримані знання в усній чи письмовій формі у повному обсягу, системно, відповідно до вимог навчальної програми (припустимими є одиничні несуттєві помилки, які студент виправляє самостійно). Виділяти істотні ознаки вивченого за допомогою операцій аналізу і синтезу; вільно оперувати відомими фактами і відомостями; виявляти причинно-наслідкові зв'язки досліджуваних процесів та явищ; формулювати висновки і узагальнення. Виконати всі практичні роботи з навчальної дисципліни. Відповідати на теоретичні питання на високому рівні в межах конспекту лекцій, рекомендованих підручників та додаткової літератури, вміти аналізувати надану інформацію та пропонувати нестандартні рішення, вміти їх обґрунтовувати. Вирішувати задачі модульного контролю високого рівня складності. Скласти підсумковий модульний контроль з результатом не менше 90% успішності.

9. Політика навчального курсу

Відвідування занять. Регуляція пропусків. Відвідування лекційних та практичних занять є обов'язковим. Допускаються пропуски занять з таких поважних причин, як хвороба, сімейні обставини, участь в олімпіаді, творчому конкурсі тощо за попереднього домовленістю та згодою викладача за умови дозволу деканату (викладачу надаються копії довідок, документів або інших матеріалів, які підтверджують причину пропуску). За умов дистанційного навчання поважними причинами пропусків можуть бути порушення у функціонуванні електромереж і збої в роботі Інтернету. Відпрацювання пропущених занять є обов'язковим незалежно від причини пропущеного заняття. Відпрацювання лекційного матеріалу передбачає самостійне вивчення пропущеного теоретичного матеріалу та складання тесту за цим матеріалом. Відпрацювання практичного заняття полягає в самостійному виконанні завдань пропущеної практичної роботи та складанні письмового звіту з роботи.

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. Для ідентифікації виконавця практичної роботи у файлі-сценарію (*.pka) слід обов'язково зазначити персональні дані: прізвище, e-mail (у вікні «User profile»), в іншому випадку робота оцінюватиметься у «0» балів (з можливістю перескладання). У разі виявлення плагіату (шляхом порівняння виконаних практичних робіт) бали за роботу обнуляються без права її перескладання цієї роботи.

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

1. Сторінка дисципліни у системі дистанційного навчання *Ментор* знаходиться за посиланням: https://mentor.khai.edu/course/view.php?id=4162
2. Комп'ютерні мережі : навч. посіб. до лаб. практикуму , Ч. 1 / Ю. О. Кулик, М. О. Момот, А. О. Рева. – Харків : НАУ «ХАІ», 2018. – 106 с.

3. Комп’ютерні мережі : навч. посіб. до лаб. практикуму , Ч. 2 / Ю. О. Кулик, М. О. Момот, Л. С. Смідович, А. В. Калмиков. – Харків : НАУ «ХАІ», 2019. – 78 с . - http://library.khai.edu/library/fulltexts/metod/

4. Проєктування корпоративних мереж : навч. посіб. до лаб. практикуму, Ч. 1. / Ю. О. Кулик, М. О. Момот, Л. С. Смідович, О. В. Сломчинський. – Харків : НАУ «ХАІ», 2025. – 75 с. - http://library.khai.edu/library/fulltexts/metod/

11. Рекомендована література

Базова

1. Santos O. Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide (Certification Guide) / Omar Santos. – Hoboken, NJ: Cisco Press, 2020. – 688 с.

2. Singh G. Cisco Certified CyberOps Associate 200-201 Certification Guide: Learn blue teaming strategies and incident response techniques to mitigate cybersecurity incidents / Glen D. Singh. – Birmingham, UK: Packt Publishing, 2021. – 660 с.

3. NIST SP 800-86: Guide to Integrating Forensic Techniques into Incident Response [Електронний ресурс] / K.Kent, S. Chevalier, T. Grance, H. Dang // National Institute of Standards and Technology. – Режим доступу до ресурсу: https://csrc.nist.gov/pubs/sp/800/86/final.

Допоміжна

1. Bandler J. Cybercrime Investigations: A Comprehensive Resource for Everyone / J. Bandler, A. Merzon. – Boca Raton: CRC Press, 2020. – 360 с.

2. Wylie P. The Pentester BluePrint: Starting a Career as an Ethical Hacker / P. Wylie, K. Crawley. – Indiana: Wiley, 2020. – 192 с.

3. Fischer R. Introduction to Security / R. Fischer, E. Halibozek, D. Walters. – Butterworth-Heinemann, 2018. – 586 с.

4. Комп’ютерні мережі : [Книга 1. Технології комп’ютерних мереж] : навч. посібник / С. П. Євсеєв, Н. В. Дженюк, М. Ю. Толкачов та ін. – Харків : «Новий Світ – 2000», 2025. – 471 с.

5. Матвій, О. В. Основи комп'ютерних мереж: навч. посібник / О. В. Матвій, В. С. Мельник, І. М. Черевко. – Чернівці : Чернівецький національний університет ім. Юрія Федьковича, 2024. – 158 с.

12. Інформаційні ресурси

1. Навчально-методичний комплект матеріалів Networking Academy Cisco з курсу «CyberOps Associate». Режим доступу: www.netacad.com
2. https://mentor.khai.edu
3. https://www.ossec.net/
4. https://elsa.sourceforge.net/
5. https://securityonionsolutions.com/
6. https://www.snort.org/
7. https://talosintelligence.com/