ЗАТВЕРДЖЕНО

Вченою радою факультету
інформаційно-комп'ютерних технологій
31 серпня 2023 р., протокол № 5
Голова Вченої ради
Тетяна НІКІТЧУК

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ ОК 24 «МЕРЕЖНА БЕЗПЕКА»

для здобувачів вищої освіти освітнього ступеня «бакалавр»
спеціальності 123 «Комп'ютерна інженерія»
освітньо-професійна програма «Комп'ютерна інженерія»
факультет інформаційно-комп'ютерних технологій
кафедра комп'ютерної інженерії та кібербезпеки

Схвалено на засіданні
кафедри комп'ютерної інженерії та
кібербезпеки
28 серпня 2023 р., протокол № 7
Завідувач кафедри
Андрій ЄФІМЕНКО

Гарант освітньо-
професійної програми
Олена ГОЛОВНЯ

Розробник: кандидат технічних наук, доцент, завідувач кафедри комп'ютерної інженерії та кібербезпеки Єфіменко Андрій Анатолійович

Житомир
2025-2026 н.р.

1. Опис навчальної дисципліни

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, спеціальність, освітній ступінь</td><td colspan="2">Характеристика навчальної дисципліни</td></tr>
<tr><td colspan="2">денна форма навчання</td></tr>
<tr><td>Кількість кредитів 7</td><td>Галузь знань
12 «Інформаційні технології»</td><td colspan="2">Нормативна</td></tr>
<tr><td>Модулів – 2</td><td rowspan="5">Спеціальність
123 «Комп’ютерна інженерія»</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td rowspan="2">Змістових модулів – 4</td><td colspan="2">3-й</td></tr>
<tr><td colspan="2">Семестр</td></tr>
<tr><td rowspan="2">Загальна кількість годин – 210</td><td>5-й</td><td>6-й</td></tr>
<tr><td colspan="2">Лекції</td></tr>
<tr><td rowspan="11">Тижневих годин для денної форми навчання:
аудиторних –
4 (5-й семестр),
4 (6-й семестр)
самостійної роботи –
1,6 (5-й семестр),
3,5 (6-й семестр)</td><td rowspan="11">Освітній ступінь «бакалавр»</td><td>16 год.</td><td>16 год.</td></tr>
<tr><td colspan="2">Практичні</td></tr>
<tr><td>–</td><td>–</td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>48 год.</td><td>48 год.</td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>26 год.</td><td>56 год.</td></tr>
<tr><td colspan="2"></td></tr>
<tr><td colspan="2">Вид контролю:
5 семестр – залік,
6 семестр – екзамен ,
курсовий проект</td></tr>
</table>

Співвідношення кількості годин аудиторних занять до самостійної та індивідуальної роботи становить:

для денної форми навчання – 61% аудиторних занять, 39% самостійної та індивідуальної роботи;

2. Мета та завдання навчальної дисципліни

Метою навчальної дисципліни є: дати студентам знання базових понять теорії, принципів побудови, стандартів, алгоритмів функціонування сучасних захищених комп'ютерних систем та мереж, знання базових підходів до побудови, технологій, протоколів, обладнання, програмного забезпечення в сфері захисту комп'ютерних систем та мереж.

Завданнями вивчення навчальної дисципліни є:

– розуміння основ організації і функціонування комп'ютерних систем та мереж, їх стандартів, протоколів та сервісів, що надаються;

– розуміння основних видів загроз інформації в комп'ютерних системах та мережах;

– розуміння основних методів і засобів реалізації віддалених мережевих атак на комп'ютерні системи та мережі;

– розуміння та оволодіння основними методами і засобами протидії віддаленим мережевим атакам на комп'ютерні системи та мережі;

– розуміння та оволодіння основними протоколами безпеки, програмними та апаратними засобами захисту інформації в комп'ютерних системах та мережах;

– розуміння організаційно-правових та нормативних основ захисту інформації в комп'ютерних системах та мережах;

– знання та розуміння основ побудови комплексної системи захисту для ресурсів комп'ютерних систем та мереж;

– розуміння основних тенденцій та закономірностей розвитку комп'ютерних систем та мереж і засобів їх реалізації;

– знання основних тенденції і закономірності розвитку засобів і методів захисту інформації в комп'ютерних системах та мережах.

– визначення і усування основних загрози інформаційної безпеки для комп'ютерних систем та мереж;

– вміння будувати модель порушника інформаційної безпеки комп'ютерних систем та мереж;

– вміння виявляти і усувати вразливості в основних компонентах комп'ютерних систем та мереж;

– вміння виявляти, переривати та попереджувати віддалені мережеві атаки за їх характерними ознаками;

– вміння розробляти політику інформаційної безпеки для комп'ютерних систем та мереж;

– вміння проектувати і реалізовувати комплексну системи забезпечення інформаційної безпеки комп'ютерних систем та мереж;

– вміння тестувати і на основі результатів тестування робити обґрунтований вибір засобів захисту для комп'ютерних систем та мереж;

– вміння здійснювати моніторинг мережевої безпеки адмініструвати комп'ютерні системи та мережі.

Зміст навчальної дисципліни направлений на формування наступних **компетентностей**, визначених стандартом вищої освіти зі спеціальності 123 «Комп'ютерна інженерія» та освітньо-професійною програмою «Комп'ютерна інженерія»:

КЗ 1. Здатність до абстрактного мислення, аналізу і синтезу.

КЗ 2. Здатність вчитися і оволодівати сучасними знаннями.

КЗ 3. Здатність застосовувати знання у практичних ситуаціях.

КЗ 7. Вміння виявляти, ставити та вирішувати проблеми.

КЗ 11. Здатність до розуміння предметної галузі та професійної діяльності.

КФ 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі комп'ютерної інженерії.

КФ 2. Здатність використовувати сучасні методи і мови програмування для розроблення алгоритмічного та програмного забезпечення.

КФ 4. Здатність забезпечувати захист інформації, що обробляється в комп'ютерних та кіберфізичних системах та мережах з метою реалізації встановленої політики інформаційної безпеки.

КФ 5. Здатність використовувати засоби і системи автоматизації проектування до розроблення компонентів комп'ютерних систем та мереж, Інтернет додатків, кіберфізичних систем тощо.

КФ 6. Здатність проектувати, впроваджувати та обслуговувати комп'ютерні системи та мережі різного виду та призначення.

КФ 8. Готовність брати участь у роботах з впровадження комп'ютерних систем та мереж, введення їх до експлуатації на об'єктах різного призначення.

КФ 9. Здатність системно адмініструвати, використовувати, адаптувати та експлуатувати наявні інформаційні технології та системи.

КФ 10. Здатність здійснювати організацію робочих місць, їхнє технічне оснащення, розміщення комп'ютерного устаткування, використання організаційних, технічних, алгоритмічних та інших методів і засобів захисту інформації.

КФ 12. Здатність ідентифікувати, класифікувати та описувати роботу програмно-технічних засобів, комп'ютерних та кіберфізичних систем, мереж та їхніх компонентів шляхом використання аналітичних методів і методів моделювання.

КФ 14. Здатність проектувати системи та їхні компоненти з урахуванням усіх аспектів їх життєвого циклу та поставленої задачі, включаючи створення, налаштування, експлуатацію, технічне обслуговування та утилізацію.

КФ 15. Здатність аргументувати вибір методів розв'язування спеціалізованих задач, критично оцінювати отримані результати, обґрунтовувати та захищати прийняті рішення.

КФ 17. Здатність забезпечувати проєктування та розроблення програмних і технічних засобів комп'ютерних систем та мереж.

КФ 18. Здатність організовувати збір, оброблення та зберігання даних у базах та сховищах даних, передачу та захист інформації в комп'ютерних системах та мережах.

КФ 19. Здатність застосовувати сучасних інформаційних технологій, технологій комп'ютерної інженерії, методів та засобів забезпечення кібербезпеки та захисту інформації під час виконання функціональних завдань та обов'язків.

Отримані знання з навчальної дисципліни стануть складовими наступних **програмних результатів** навчання за спеціальністю 123 «Комп'ютерна інженерія» та освітньо-професійною програмою «Комп'ютерна інженерія»:

РН 1. Знати і розуміти наукові положення, що лежать в основі функціонування комп'ютерних засобів, систем та мереж.

РН 2. Мати навички проведення експериментів, збирання даних та моделювання в комп'ютерних системах.

РН 3. Знати новітні технології в галузі комп'ютерної інженерії.

РН 4. Знати та розуміти вплив технічних рішень в суспільному, економічному, соціальному і екологічному контексті.

РН 6. Вміти застосовувати знання для ідентифікації, формулювання і розв'язування технічних задач спеціальності, використовуючи методи, що є найбільш придатними для досягнення поставлених цілей.

РН 7. Вміти розв'язувати задачі аналізу та синтезу засобів, характерних для спеціальності.

РН 9. Вміти застосовувати знання технічних характеристик, конструктивних особливостей, призначення і правил експлуатації програмно-технічних засобів комп'ютерних систем та мереж для вирішення технічних задач спеціальності.

РН 11. Вміти здійснювати пошук інформації в різних джерелах для розв'язання задач комп'ютерної інженерії.

РН 13. Вміти ідентифікувати, класифікувати та описувати роботу комп'ютерних систем та їх компонентів.

РН 14. Вміти поєднувати теорію і практику, а також приймати рішення та виробляти стратегію діяльності для вирішення завдань спеціальності з урахуванням загальнолюдських цінностей, суспільних, державних та виробничих інтересів.

РН 15. Вміти виконувати експериментальні дослідження за професійною тематикою.

РН 16. Вміти оцінювати отримані результати та аргументовано захищати прийняті рішення.

РН 19. Здатність адаптуватись до нових ситуацій, обґрунтовувати, приймати та реалізовувати у межах компетенції рішення.

РН 20. Усвідомлювати необхідність навчання впродовж усього життя з метою поглиблення набутих та здобуття нових фахових знань, удосконалення креативного мислення.

РН 21. Якісно виконувати роботу та досягати поставленої мети з дотриманням вимог професійної етики.

РН 22. Використовувати знання з фундаментальних природничих, математичних та загально-інженерних дисциплін для вирішення типових завдань проєктування, побудови та адміністрування комп’ютерних систем та мереж.

РН 23. Використовувати навички розроблення алгоритмів та програмування мовами низького та високого рівнів, навички проєктування, розроблення, адміністрування і захисту баз даних та інформаційних ресурсів (зокрема веб-ресурсів).

РН 24. Обґрунтовувати застосування методів, способів та технологій збору, зберігання, оброблення, передавання та захисту даних у комп’ютерних системах та мережах.

3. Програма навчальної дисципліни

Модуль 1

Змістовий модуль 1. СТАНДАРТИЗАЦІЯ І МОДЕЛЬНЕ ПРЕДСТАВЛЕННЯ КОМП'ЮТЕРНИХ СИСТЕМ ТА МЕРЕЖ. ІНТРАНЕТ ЯК ВІДКРИТА СИСТЕМА

ТЕМА 1. ОСНОВНІ ЕЛЕМЕНТИ ТА СТАНДАРТИ КОМП'ЮТЕРНИХ СИСТЕМ ТА МЕРЕЖ

Мета, завдання та порядок вивчення дисципліни. Інформаційно-методичне забезпечення дисципліни: основна та додаткова література, перелік рекомендованих інформаційних джерел у мережі Інтернет.

Основні елементи відкритих інформаційно-комунікаційних систем. Основні поняття і визначення. Концепція відкритих інформаційно-комунікаційних систем. Роль стандартів в технології відкритих інформаційно-комунікаційних систем. Основні групи стандартів і організації по стандартизації.

ТЕМА 2. МОДЕЛЬНЕ ПРЕДСТАВЛЕННЯ КОМП'ЮТЕРНИХ СИСТЕМ ТА МЕРЕЖ. ІНТРАНЕТ ЯК ВІДКРИТА СИСТЕМА

Сумісність відкритих інформаційно-комунікаційних систем. Переносимість і здатність до взаємодії. Базова модель інформаційної системи. Системний підхід до опису функціональності на базі модельного представлення інформаційних систем. Розширення базової моделі інформаційної системи для взаємодіючих систем. Переносимість. Способи реалізації переносимості. Класифікація сервісів платформи додатків по критеріях переносимості. Здатність до взаємодії. Способи реалізації здатності до взаємодії. Класифікація сервісів платформи додатків по критеріях здатності до взаємодії. Основні моделі відкритих систем. Модель OSI. Модель POSIX.

ТЕМА 3. ІНТРАНЕТ

Поняття інтранета. Структура інтранета. Еталонна модель інтранета. Етапи створення інтранета. Види інтранета. Стандарти створення інтранета. Інтранет як частина середовища відкритих систем. Інтранет і екстранет.

ТЕМА 4. ПОРТАЛ

Портал і інтранет. Класифікація порталів. Логічна структура і компоненти порталу. Схема порталу. Базові сервіси порталу.

Змістовий модуль 2. ВРАЗЛИВОСТІ КОМП'ЮТЕРНИХ СИСТЕМ ТА МЕРЕЖ НА ПРИКЛАДІ ІНТРАНЕТА. АТАКИ НА ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ СИСТЕМИ

ТЕМА 5. ЗАГРОЗИ ТА ВРАЗЛИВОСТІ РЕСУРСІВ ІНТРАНЕТА

Загрози ресурсам інтранета і причини їх реалізації. Уразливість архітектури клієнт-сервер. Конфігурація системи. Уразливість операційних систем. Уразливість серверів. Уразливість робочих станцій. Уразливість каналів зв'язку.

ТЕМА 6. СЛАБКОСТІ СИСТЕМНИХ УТИЛІТ, КОМАНД, МЕРЕЖЕВИХ СЕРВІСІВ, ТЕХНОЛОГІЙ ПРОГРАМУВАННЯ

Слабкості системних утиліт, команд і мережевих сервісів. Telnet. FTP. NFS. DNS. NIS. World Wide Web. Команди видаленого виконання. Sendmail і електронна пошта. Інші утиліти. Слабкості сучасних технологій програмування. Помилки в програмному забезпеченні. Мережеві віруси.

ТЕМА 7. ВІДДАЛЕНІ АТАКИ НА КОМП'ЮТЕРНІ СИСТЕМИ ТА МЕРЕЖІ

Віддалені атаки на відкриті системи. Аналіз мережевого трафіку. Підміна довіреного об'єкту або суб'єкта. Помилковий об'єкт. "Відмова в обслуговуванні". Віддалений контроль над станцією в мережі.

ТЕМА 8. Типові сценарії і рівні атак

Типові сценарії і рівні атак. Етапи реалізації атак. Рівні атак. Класичні і сучасні методи, використовувані нападниками для проникнення у відкриті системи. Перехоплення даних і виявлення прослуховуючих додатків Моніторинг в графічних інтерфейсах. Підміна системних утиліт. Атаки з використанням мережевих протоколів. Приклади деяких атак.

Модуль 2

Змістовий модуль 3. ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В КОМП'ЮТЕРНИХ СИСТЕМАХ ТА МЕРЕЖАХ. АУТЕНТИФІКАЦІЯ СУБ'ЄКТІВ І ОБ'ЄКТІВ ВЗАЄМОДІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ. МІЖМЕРЕЖЕВІ ЕКРАНИ. ВІРТУАЛЬНІ ПРИВАТНІ МЕРЕЖ

ТЕМА 9. ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В КОМП'ЮТЕРНИХ СИСТЕМАХ ТА МЕРЕЖАХ

Чотирьохрівнева модель відкритої системи. Специфіка захисту ресурсів відкритих систем на прикладі інтранета. Вибір мережевої топології інтранета при підключенні до інших зовнішніх мереж. Фізична ізоляція. Ізоляція протоколу. Виділені канали і маршрутизатори. Принципи створення захищених засобів зв'язку об'єктів у відкритих системах. Стандарті ISO 7498-2. Стандарт ISO 17799. Стандарт ISO 15408. Вимоги до захищених каналів зв'язку у відкритих системах. Політика безпеки для відкритих систем. Визначення політики безпеки. Причини вироблення політики безпеки. Основні вимоги до політики безпеки. Етапи вироблення політики безпеки. Зміст політики безпеки. Реалізація політики безпеки. Аудит за проведенням політики безпеки.

ТЕМА 10. СЕРВІСИ БЕЗПЕКИ

Ідентифікація/аутентифікація. Розмежування доступу. Протоколювання і аудит. Екранування. Тунелювання. Шифрування. Контроль цілісності. Контроль захищеності. Виявлення відмов і оперативне відновлення. Управління. Засоби

забезпечення інформаційної безпеки у відкритих системах. Створення комплексної системи забезпечення безпеки відкритих систем. Управління безпекою відкритих систем. Організаційно-правові методи захисту відкритих систем. Деякі рекомендації по забезпеченню інформаційної безпеки відкритих систем. Що робити у разі злому системи. Як простежити за роботою користувачів. Короткі рекомендації адміністраторам інформаційної безпеки

ТЕМА 11. МЕРЕЖЕВА АУТЕНТИФІКАЦІЯ

Мережева аутентифікація – «перший рубіж» захисту відкритої системи. Уніфікація даних про суб'єктів і об'єкти. Єдина система аутентифікації. Єдина система авторизації. Єдина система персоналізації. Єдина система делегованого управління даннями про суб'єктів і об'єкти. Єдина система аудиту доступу.

ТЕМА 12. ПІДСИСТЕМА АУТЕНТИФІКАЦІЇ

Аутентифікація в клієнт-серверних системах. Типові моделі аутентифікації. Методи аутентифікації. Протоколи аутентифікації. Сервери аутентифікації. Ринок засобів аутентифікації.

ТЕМА 13. БУДОВА ТА ФУНКЦІЇ, КЛАСИФІКАЦІЯ МІЖМЕРЕЖЕВИХ ЕКРАНІВ.

Основні компоненти міжмережевого екрану. Функції міжмережевих екранів. Профілі захисту для міжмережевих екранів. Типи міжмережевих екранів. Екрануючі концентратори. Пакетні фільтри. Шлюзи сеансового рівня. Шлюзи прикладного рівня. Міжмережеві екрани експертного рівня. Персональні міжмережеві екрани.

ТЕМА 14. ТИПОВІ СХЕМИ ПІДКЛЮЧЕННЯ МІЖ МЕРЕЖЕВИХ ЕКРАНІВ

Схеми підключення міжмережевих екранів. Слабкості міжмережевих екранів. Вибір реалізацій міжмережевих екранів. Приклади між мережевих екранів.

ТЕМА 15. ЗАХИСТ НА КАНАЛЬНОМУ РІВНІ

Проколи PPTP. Протокол L2TP. Протокол L2F.

ТЕМА 16. ЗАХИСТ НА МЕРЕЖЕВОМУ ТА СЕАНСОВОМУ РІВНЯХ

Архітектура засобів безпеки IPSec. Захист даних, що передаються за допомогою протоколів AH та ESP. Протокол управління криптоключами IKE. Особливості реалізації засобів IPSec. Захист на сеансовому рівні – протоколи SSL, TLS, SOCKS.

ТЕМА 17. ЗАХИСТ БЕЗПРОВІДНИХ МЕРЕЖ

Загальні відомості про особливості організації захисту бепровідних мереж. Протоколи захисту бепровідних мереж.

ТЕМА 18. СПЕЦИФІКА ТА ПРОТОКОЛИ ПОБУДОВИ ВІРТУАЛЬНИХ ПРИВАТНИХ МЕРЕЖ

Визначення віртуальних приватних обчислювальних мереж. Цілі і завдання побудови VPN. Специфіка побудови VPN. Тунелювання у VPN. Схема VPN. Політики безпеки для VPN. Стандартні протоколи побудови VPN. Рівні

захищених каналів. Захист даних на канальному рівні. Захист даних між канальним і мережевим рівнями. Захист даних на мережевому рівні Захист на сеансовому рівні. Порівняння функціональних можливостей протоколів.

ТЕМА 19. ВАРІАНТИ ПОБУДОВИ VPN

VPN на базі мережевої операційної системи. VPN на базі маршрутизаторів VPN на базі міжмережевих екранів. VPN на базі спеціалізованого програмного забезпечення VPN на базі апаратних засобів. Види VPN залежно від вирішуваних завдань. Intranet VPN. Client/server VPN. Extranet VPN. Remote Access VPN. Топології VPN. VPN-консорциум про VPN. Рекомендації фахівців з вибору рішень для побудови VPN. Проблеми і уразливості сучасних VPN.

ТЕМА 20. ВІРТУАЛЬНІ ЛОКАЛЬНІ ОБЧИСЛЮВАЛЬНІ МЕРЕЖІ.

Призначення і технології VLAN. Види VLAN. Переваги технології VLAN. Протоколи побудови VLAN

Змістовий модуль 4. СИСТЕМИ АНАЛІЗУ ЗАХИЩЕНОСТІ, СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ, СИСТЕМИ ПОПЕРЕДЖЕННЯ ВТОРГНЕНЬ

ТЕМА 21. АУДИТ І МОНІТОРИНГ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У КОМП'ЮТЕРНИХ СИСТЕМАХ ТА МЕРЕЖАХ

Аудит і моніторинг інформаційної безпеки у відкритих системах. Місце і завдання систем аналізу захищеності в захисті відкритих систем. Класифікації систем аналізу захищеності.

ТЕМА 22. МЕРЕЖЕВІ СКАНЕРИ

Мережеві сканери. Розміщення агентів мережевих сканерів. Принципи роботи мережевих сканерів. Етапи роботи мережевих сканерів. Порівняння поширених мережевих сканерів. Системні сканери. Сканери безпеки для додатків. Критерії вибору сканерів безпеки .

ТЕМА 24. ОСНОВИ ПОБУДОВИ СИСТЕМ ВИЯВЛЕННЯ ВТОРГНЕНЬ

Методи відбиття вторгнень. Запобігання вторгненням. Переривання вторгнення. Заборона вторгнення. Відхилення вторгнення. Виявлення вторгнень. Усунення наслідків вторгнення. Основи побудови систем виявлення вторгнень. Структура систем виявлення вторгнень. Класифікація систем виявлення вторгнень. Ефективність систем виявлення вторгнень. Системне виявлення вторгнень. Принципи роботи системних систем виявлення вторгнення. Переваги і недоліки систем виявлення вторгнення. Мережеве виявлення вторгнень. Принципи роботи мережевих систем виявлення вторгнення. Розміщення мережевих систем виявлення вторгнення. Переваги і недоліки мережевих систем виявлення вторгнення. Поведінкове виявлення вторгнень. Інтелектуальне виявлення вторгнень. Комплексне виявлення вторгнень. Вибір системи виявлення вторгнень. Визначення вимог. Оцінка продукту. Розгортання системи виявлення вторгнень. Практика виявлення вторгнень. Обмеженість систем

виявлення вторгнень.

ТЕМА 25. СИСТЕМИ ПОПЕРЕДЖЕННЯ ВТОРГНЕНЬ

Системи запобігання вторгненням. Реагування на вторгнення в інтранет, виявлені системами виявлення вторгнень. Етапи реагування. Реагування на виявлення вірусів і черв'яків. Реагування після атаки зловмисників. Збереження доказів вторгнення. Принципи і етапи збору доказів. Інструментальні засоби збору доказів. Стандарти в області виявлення вторгнень.

ТЕМА 26. ЗАХИСТ СИСТЕМ ЕЛЕКТРОННОЇ ПОШТИ

Інші засоби забезпечення безпеки у відкритих системах. Захист від спаму в електронній пошті. Визначення спаму. Методи детектування спаму. Архітектура захищеної від спаму електронної пошти . Правові аспекти боротьби із спамом. Приклади засобів захисту від спаму.

ТЕМА 27. БАГАТОФУНКЦІОНАЛЬНІ ПРИСТРОЇ ЗАХИСТУ ВІД МЕРЕЖЕВИХ АТАК

Багатофункціональні пристрої захисту від мережевих атак. Системи аналізу і управління ризиками. Системи забезпечення інформаційної безпеки на рівні підприємства.

4. Структура (тематичний план) навчальної дисципліни

Змістові модулі	Кількість годин			
	Всього	Лекції	Лабораторні	Самостійна робота
2	3	4	5	6
Модуль 1				
Змістовий модуль 1. СТАНДАРТИЗАЦІЯ І МОДЕЛЬНЕ ПРЕДСТАВЛЕННЯ КОМП'ЮТЕРНИХ СИСТЕМ ТА МЕРЕЖ. ІНТРАНЕТ ЯК ВІДКРИТА СИСТЕМА	45	8	24	13
Змістовий модуль 2. ВРАЗЛИВОСТІ ВІДК КОМП'ЮТЕРНИХ СИСТЕМ ТА МЕРЕЖ НА ПРИКЛАДІ ІНТРАНЕТА. АТАКИ НА КОМП'ЮТЕРНІ СИСТЕМИ ТА МЕРЕЖІ	45	8	24	13
Разом модуль 1	90	16	48	26
Модуль 2				
Змістовий модуль 3. ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В КОМП'ЮТЕРНИХ СИСТЕМАХ ТА МЕРЕЖАХ. АУТЕНТИФІКАЦІЯ СУБ'ЄКТІВ І ОБ'ЄКТІВ ВЗАЄМОДІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ ТА МЕРЕЖАХ. МІЖМЕРЕЖЕВІ ЕКРАНИ. ВІРТУАЛЬНІ ПРИВАТНІ МЕРЕЖ	45	8	24	13
Змістовий модуль 4. СИСТЕМИ АНАЛІЗУ ЗАХИЩЕНОСТІ, СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ, СИСТЕМИ ПОПЕРЕДЖЕННЯ ВТОРГНЕНЬ	45	8	24	13
Разом модуль 2	90	16	48	26
КУРСОВИЙ ПРОЕКТ	30			30
ВСЬОГО	210	32	96	82

5. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
		денна форма
1.	Лабораторна робота № 1. НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ БАЗОВИХ ЗАСОБІВ ЗАХИСТУ МЕРЕЖНОЇ ОПЕРАЦІЙНОЇ СИСТЕМИ CISCO IOS ТА МЕРЕЖНОГО ОБЛАДНАННЯ CISCO	4
2.	Лабораторна робота № 2. НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ ЗАСОБІВ ПРОТИДІЇ АТАКАМ КАНАЛЬНОГО РІВНЯ MAC-FLOODING ТА MAC-SPOOFING У МЕРЕЖІ НА БАЗІ КОМУТАТОРІВ CISCO	4
3.	Лабораторна робота № 3. НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ ЗАСОБІВ ПРОТИДІЇ АТАКАМ НА ПРОТОКОЛ STP/PVST+ У МЕРЕЖІ НА БАЗІ КОМУТАТОРІВ CISCO	4
4.	Лабораторна робота № 4. НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ РОБОТИ ТЕХНОЛОІЇ VLAN НА ОСНОВІ ГРУПУВАННЯ ПОРТІВ У МЕРЕЖІ НА БАЗІ КОМУТАТОРІВ CISCO	4
5.	Лабораторна робота № 5. НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ РОБОТИ ВІРТУАЛЬНИХ ЛОКАЛЬНИХ МЕРЕЖ НА ОСНОВІ ГРУПУВАННЯ ПОРТІВ ТА ТРАНКОВИХ ПРОТОКОЛІВ У МЕРЕЖІ НА БАЗІ КОМУТАТОРІВ CISCO	4
6.	Лабораторна робота № 6. НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ РОБОТИ ВІРТУАЛЬНИХ ЛОКАЛЬНИХ МЕРЕЖ типу Private VLAN У МЕРЕЖІ НА БАЗІ КОМУТАТОРІВ CISCO	4
7.	Лабораторна робота № 7. НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ РОБОТИ ПРОТОКОЛУ VTP У МЕРЕЖІ НА БАЗІ КОМУТАТОРІВ CISCO	4
8.	Лабораторна робота № 8. НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ ЗАСОБІВ ПРОТИДІЇ АТАКАМ НА ПРОТОКОЛ ARP	4
9.	Лабораторна робота № 9. НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ ЗАСОБІВ ПРОТИДІЇ АТАКАМ НА СЕРВІСИ ПРОТОКОЛУ DHCP	4
10.	Лабораторна робота № 10. НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ РОБОТИ ПІДСИСТЕМИ ДЗЕРКАЛЮВАННЯ ТРАФІКУ У МЕРЕЖІ НА БАЗІ ОБЛАДНАННЯ CISCO	4
11.	Лабораторна робота № 11. НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ ЗАСОБІВ АУТЕНТИФІКАЦІЇ ПРОТОКОЛІВ КАНАЛЬНОГО РІВНЯ	4
12.	Лабораторна робота № 12. НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ РОБОТИ ЗАСОБІВ ПРОТОКОЛУ PPPoE У МЕРЕЖІ НА БАЗІ ОБЛАДНАННЯ CISCO	4
13.	Лабораторна робота № 13. НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ ЗАСОБІВ АУТЕНТИФІКАЦІЇ ПРОТОКОЛІВ МАРШРУТИЗАЦІЇ	4
14.	Лабораторна робота № 14. НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ РОБОТИ АУТЕНТИФІКАЦІЇ НА ОСНОВІ МОДЕЛІ AAA ТА ПРОТОКОЛІВ RADIUS ТА TACACS+ У МЕРЕЖІ НА БАЗІ ОБЛАДНАННЯ CISCO	4

15.	Лабораторна робота № 15. НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ РОБОТИ ПРОТОКОЛУ ТУНЕЛЮВАННЯ GRE У МЕРЕЖІ НА БАЗІ ОБЛАДНАННЯ CISCO	4
16.	Лабораторна робота № 16. НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ РОБОТИ ЗАСОБІВ ПРОТОКОЛУ PPTP У МЕРЕЖІ НА БАЗІ ОБЛАДНАННЯ CISCO	4
17.	Лабораторна робота № 17. НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ РОБОТИ ЗАСОБІВ ПРОТОКОЛУ L2TP У МЕРЕЖІ НА БАЗІ ОБЛАДНАННЯ CISCO	4
18.	Лабораторна робота № 18. НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ МІЖМЕРЕЖНИХ ЕКРАНІВ НА БАЗІ СТАНДАРТНИХ СПИСКІВ ДОСТУПУ	4
19.	Лабораторна робота № 19. НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ МІЖМЕРЕЖНИХ ЕКРАНІВ НА БАЗІ РОЗШИРЕНИХ СПИСКІВ ДОСТУПУ	4
20.	Лабораторна робота № 20. НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ РОБОТИ ОСНОВНИХ ЗАСОБІВ ЗАХИСТУ АПАРАТНОГО МІЖМЕРЕЖНОГО ЕКРАНУ CISCO ASA 5505	4
21.	Лабораторна робота № 21. НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ РОБОТИ ДОДАТКОВИХ ЗАСОБІВ ЗАХИСТУ АПАРАТНОГО МІЖМЕРЕЖНОГО ЕКРАНУ CISCO ASA 5505	4
22.	Лабораторна робота № 22. НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ РОБОТИ ВІРТУАЛЬНИХ ПРИВАТНИХ МЕРЕЖ ТИПУ SITE-TO-SITE	4
23.	Лабораторна робота № 23. НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ РОБОТИ ВІРТУАЛЬНИХ ПРИВАТНИХ МЕРЕЖ ТИПУ DMVPN	4
24.	Лабораторна робота № 24. НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ РОБОТИ СИСТЕМ IDS/IPS	4
	Разом	96

6. Завдання для самостійної роботи

Відпрацювання матеріалу навчального курсу Cisco Network Security (проходження онлайн навчання, виконання тестових контрольних робіт, виконання тестових проміжних оцінювань).

7. Індивідуальні завдання

Не передбачені.

8. Методи навчання

Застосовуються наступні методи навчання:

МН01 – вербальні (лекція, пояснення, розповідь, бесіда, інструктаж);

МН02 – наочні (спостереження, ілюстрація, демонстрація);

МН03 – практичні (різні види вправ та завдань, виконання розрахунків тощо);

МН04 – пояснювально-ілюстративний (передбачає надання готової інформації викладачем та її засвоєння студентами;

МН05 – репродуктивний, в основу якого покладено виконання різного роду завдань за зразком;

МН06 – метод проблемного викладу;

МН07 – частково-пошуковий (евристичний);

МН08 – дискусійний метод;

МН09 – метод активного навчання (проведення ділових ігор, ігрового проектування);

МН10 – ситуаційний метод, розв’язування кейсових завдань.

9. Методи контролю

Передбачено заходи поточного та підсумкового контролю. Під час проведення заходів контролю передбачено використання наступних методів оцінювання:

МО01 – оцінювання роботи під час аудиторних занять;

МО02 – виконання практичних завдань;

МО03 – поточне тестування;

МО04 – виконання аудиторної контрольної роботи;

МО05 – захист індивідуального завдання (за наявності);

МО06 – залік/екзамен (5-й семестр – залік, 6-й семестр – екзамен).

10. Розподіл балів

Семестровий розподіл балів:

– відвідування та робота на лекціях – 4 бали.

– робота на лабораторних заняттях (зокрема і поточні контролі) – 24 бали;

– виконання та захист звітів з лабораторних робіт – 24 бали;

– самостійна робота студентів – 8 балів;

– модульні контролі – 40 балів.

Детальний розподіл балів наводиться у рейтинг-листі дисципліни.

Шкала оцінювання

За шкалою	Екзамен	Залік	Бали
A	Відмінно	Зараховано	90-100
B	Добре	Зараховано	82-89
C			74-81
D	Задовільно	Зараховано	64-73
E			60-63
FX	Незадовільно	Не зараховано	35-59
F		Не зараховано	0-34

11. Рекомендована література

Основна література

1. Barker, Keith. CCNA Security 640-554. Official Cert Guide / Keith Barker, Scott Morris.– Cisco Press, 2013. – 740 p.
2. Conlan J., Patrik. Cisco Network Professional. Advanced Internetworking Guide. / Patrik J. Conlan. – Wiley Publishing, 2009. – 854 p.
3. Paquet, Catherine. Implementing Cisco IOS Network Security (IINS) / Catherine Paquet. – Cisco Press, 2009. – 600 p.
4. Santos, Omar. CCNA Security 210-260. Official Cert Guide / Omar Santos, John Stuppi. – Cisco Press, 2015. – 658 p.
5. Vyncke, Eric. LAN Switch Security: What Hackers Know about Your Switches / Eric Vyncke, Christopher Paggen. – Cisco Press, 2007. – 340 p.
6. Watkins, Michael. CCNA Security. Official Exam Certification Guide / Michael Watkins, Kevin Wallace. – Cisco Press, 2008. – 638 p.
7. Wilkins, Sean. CCNP Security. SECURE 642-637. Official Cert Guide / Sean Wilkins, Franklin H. Smith III. – Cisco Press, 2011. – 738 p.
8. Єфіменко А.А. Захист інформації в інформаційно-комунікаційних системах: методичні рекомендації для виконання лабораторних робіт. Ч. 2 / підг. А. А. Єфіменко. – Житомир: ЖВІ, 2017. – 176 с.
9. Єфіменко А.А. Захист інформації в інформаційно-комунікаційних системах: методичні рекомендації для виконання лабораторних робіт. Ч. 1 / підг. А. А. Єфіменко. – Житомир: ЖДТУ, 2018. – 112 с.

Допоміжна література

10. Грайворонський М. В., Новіков О.М. Безпека інформаційно-комунікаційних систем. – К.: Видавнича группа BHV, 2009. – 608 с.
11. Юдін О.К., Корченко О.Г., Конахович Г.Ф. Захист інформації в мережах передачі даних. – К.: Вид-во ТОВ «НВП»ІНТЕРСЕРВІС», 2009. – 716 с.

12. Інформаційні ресурси мережі Інтернет

1. Навчальний курс Network Security [Електронний ресурс] – Режим доступу: www.netacad.com.
2. Навчальний курс CCNA Security [Електронний ресурс] – Режим доступу: www.netacad.com.
3. Навчальний курс CCNAv7: Enterprise Networking, Security, and Automation [Електронний ресурс] – Режим доступу: www.netacad.com.
4. Навчальний курс CCNP: Core Networking. [Електронний ресурс] – Режим доступу: www.netacad.com.