Національний технічний університет України
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Кафедра прикладної радіоелектроніки

[RE-281] КОМП'ЮТЕРНІ МЕРЕЖІ ТА БЕЗПЕКА ЗА ТЕХНОЛОГІЯМИ CISCO

Робоча програма навчальної дисципліни (Силабус)

Реквізити навчальної дисципліни

Рівень вищої освіти	Перший (бакалаврський)
Галузь знань	G - Інженерія, виробництво та будівництво
Спеціальність	G5 - Електроніка, електронні комунікації, приладобудування та радіотехніка
Освітня програма	Всі ОП
Статус дисципліни	Вибіркова (Ф-каталог)
Форма здобуття вищої освіти	Очна
Рік підготовки, семестр	Доступно для вибору починаючи з 2-го курсу, осінній семестр
Обсяг дисципліни	4 кред. (Лекц. 16 год, Практ. 30 год, Лаб. 0 год, СРС. 74 год)
Семестровий контроль/контрольні заходи	Залік
Розклад занять	https://schedule.kpi.ua
Мова викладання	Українська
Інформація про керівника курсу / викладачів	Лекц.: Нікітчук А. В., Практ.: Нікітчук А. В.,
Розміщення курсу	https://do.ipo.kpi.ua/course/view.php?id=5928

Програма навчальної дисципліни

1. Опис навчальної дисципліни, її мета, предмет вивчання та результати навчання

Сучасні інформаційні технології суттєво залежать від комп'ютерних мереж, що складаються з мільярдів взаємопов’язаних пристроїв. Це створює унікальні виклики в управлінні,

масштабуванні та забезпеченні безпеки. Для надійного та ефективного обміну даними використовується різноманітне мережеве обладнання, технології та протоколи збору, зберігання, передачі, обробки та захисту інформації.
Вивчення даної дисципліни буде корисним для будь-кого, хто працює з комп'ютерами, даними і інформацією, та допоможе розробляти і впроваджувати стратегії і заходи безпеки для запобігання кібератакам, оцінювати вразливості мереж та ризики пов'язані з ними, а також адекватно реагувати на кіберподії.

Студенти здобудуть знання/навички:

- основ кібербезпеки та найбільших проблем, з якими сьогодні стикаються в кіберпросторі;
- основ мереж та мережевого обладнання, а також правил за якими відбувається обмін даними у мережі;
- налаштування мережевого обладнання та кінцевих вузлів;
- основних загроз, атак та вразливостей, що існують у кіберпросторі;
- основних засобів захисту кінцевих вузлів та мережі;
- оцінки вразливостей мереж і ризиків пов’язаних з ними;
- реагування на кіберподії, для відновлення та збору даних для проведення експертизи.

Вивчення дисципліни дозволить підвищити особисту безпеку в кіберпросторі, а також надасть конкурентну перевагу на ринку праці у різних сферах і ролях. Ссобливо корисними буде для:

- IT-спеціалістів, мережевих адміністраторів, системних адміністраторів та інженерів з мережевої безпеки, що відповідатимуть за налагодження та управління мережевою інфраструктурою, забезпечення безпеки даних та захист мереж від потенційних загроз.
- Спеціалістів з інформаційної безпеки, що займатимуться виявленням та аналізом загроз безпеці, впровадженням заходів для запобігання кібератакам, виконуватимуть тестування на проникнення та розроблятимуть політики безпеки.
- Консультантів з питань мережевої безпеки, що консультуватимуть компанії та організації з питань мережевої безпеки, проводитимуть аудит їхньої інфраструктури та розроблятимуть стратегії захисту від кібератак.

2. Пререквізити та постреквізити дисципліни (місце в структурно-логічній схемі навчання за відповідною освітньою програмою)

Для успішного засвоєння дисципліни студенти повинні володіти:

- знаннями з інформатики та навичками використання ПК;
- англійською мовою або навичками використання онлайн-перекладачів.

Пов'язані дисципліни:

- Програмування вбудованих систем Інтернету речей (застосування комунікаційних протоколів при програмуванні мережевих вузлів/обладнання).

- Технології .NET для розробки програмного забезпечення (розробка веб-застосунків для використання в комп'ютерних мережах).

3. Зміст навчальної дисципліни

Розділ 1. Основи комп’ютерних мереж та кібербезпеки

- Тема 1. Основи безпеки в кіберпросторі та комп’ютерних мережах
- Тема 2. Мережі та їх характеристики. Мережеве обладнання
- Тема 3. Організація мереж та еталонна модель OSI. Принципи побудови глобальних комп'ютерних мереж

- Тема 4. Протоколи мережевого рівня та їх вразливості
- Тема 5. Протоколи транспортного і прикладного рівня та їх вразливості

Розділ 2. Безпека кінцевих вузлів, захист мережі та управління кіберзагрозами

- Тема 6. Типи загроз кібербезпеці та способи захисту від них
- Тема 7. Характеристики комп'ютерних мереж. Пристрої, служби та дані безпеки
- Тема 8. Глибокий захист, брандмауери, списки контролю доступу та політики безпеки

4. Навчальні матеріали та ресурси

Базова:

1. *Організація комп’ютерних мереж: лабораторний практикум [Електронний ресурс] : навч. посіб. для студ. спеціальності 121 «Інженерія програмного забезпечення», спеціалізації «Програмне забезпечення комп’ютерних та інформаційно-пошукових систем» / Л.М. Олещенко ; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 4,68 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2018. – 137 с. (Можна знайти в мережі інтернет, студент має ознайомитись, дати відповіді на контрольні запитання)*
2. *А. О. Азарова, Н. В. Лисак. Комп’ютерні мережі та телекомунікації/Навчальний посібник Вінниця ВНТУ 2012. (Можна знайти в мережі інтернет, студент має ознайомитись)*

Додаткова:

1. Grubb, Sam. How Cybersecurity Really Works: A Hands-On Guide for Total Beginners. Сполучені Штати Америки: No Starch Press, 2021.
2. Zach, Coding. Computer Programming and Cybersecurity for Beginners: This Book Includes: Python Machine Learning, SQL, Linux, Hacking with Kali Linux, Ethical Hacking. Coding and Cyber Security Fundamentals.. N.p.: Rdf Publishing Limited, 2021.
3. Lewis, Elijah. Ethical Hacking: 3 in 1- Beginner's Guide+ Tips and Tricks+ Advanced and Effective Measures of Ethical Hacking. N.p.: Amazon Digital Services LLC - KDP Print US, 2020.
4. Morgan, Kevin. Computer Networking Beginners Guide: The Complete Basic Guide to Master Network Security, Computer Architecture, Wireless Technology, and Communications Systems Including Cisco, CCNA and the OSI Model. N.p.: Tommaso Sammartano, 2021.
5. White, Michael B.. Computer Networking: The Complete Guide to Understanding Wireless Technology, Network Security, Computer Architecture and Communications Systems (Including Cisco, CCNA and CCENT). N.p.: CreateSpace Independent Publishing Platform, 2018.
6. Kiser, Quinn. Cybersecurity: A Simple Beginner's Guide to Cybersecurity, Computer Networks and Protecting Oneself from Hacking in the Form of Phishing, Malware, Ransomware, and Social Engineering. Сполучені Штати Америки: Primasta, 2020.

Описи протоколів, стандартів, термінів та ін. можна знайти в мережі Інтернет, наприклад на сайті Wikipedia (https://www.wikipedia.org) або офіційних сайтах виробників мережевого обладнання та розробників стандартів.

Навчальний контент

5. Методика опанування навчальної дисципліни (освітнього компонента)

Розділ 1. Основи комп’ютерних мереж та кібербезпеки	
Лекція 1	Основи безпеки в кіберпросторі та комп’ютерних мережах
Лекція 2	Мережі та їх характеристики. Мережеве обладнання
Лекція 3	Організація мереж та еталонна модель OSI. Принципи побудови глобальних комп'ютерних мереж
Лекція 4	Протоколи мережевого рівня та їх вразливості

Лекція 5	Протоколи транспортного і прикладного рівня та їх вразливості
ПР 1	Початок роботи в Cisco Packet Tracer
ПР 2	Функції канального, мережевого та транспортного рівнів
ПР 3	Мережева операційна система Cisco IOS
ПР 4	Налаштування мережевого обладнання
Розділ 2. Безпека кінцевих вузлів, захист мережі та управління кіберзагрозами	
Лекція 6	Типи загроз кібербезпеці та способи захисту від них
Лекція 7	Характеристики комп'ютерних мереж. Пристрої, служби та дані безпеки
Лекція 8	Глибокий захист, брандмауери, списки контролю доступу та політики безпеки
ПР 5	Дослідження загроз кінцевим вузлам
ПР 6	Підвищення безпеки в Windows: дослідження, моніторинг, керування та налаштування
ПР 7	Дослідження потоків даних у локальній мережі за допомогою Wireshark
ПР 8	Налаштування базових функцій безпеки WLAN
ПР 9	Налаштування контролю доступу та аутентифікації
ПР 10	Дані для моніторингу безпеки
ПР 11	Списки контролю доступу. Налаштування стандартних ACL
ПР 12	Списки контролю доступу. Налаштування розширених ACL
ПР 13	Управління заходами безпеки та ризиками
ПР 14	Аналіз кіберзагроз
ПР 15	Реагування на інциденти

6. Самостійна робота студента

1. На протязі семестру:

- *Вивчення матеріалів, що виносяться на самостійне опрацювання в кінці кожної лекції.*
- *Опрацювання літературних джерел.*
- *Відповіді на запитання для самоперевірки та проходження тестів.*

2. На протязі тижня перед запланованою активністю:

- *Підготовка до практичних робіт.*
- *Підготовка до написання контрольної роботи.*
- *Підготовка та виконання домашньої контрольної роботи.*
- *Підготовка до заліку.*

Політика та контроль

7. Політика навчальної дисципліни (освітнього компонента)

Правила відвідування занять:

- *для лекцій та практичних - відвідування занять (відеоконференцій Zoom) за розкладом;*
- *допускається самостійне вивчення матеріалу за допомогою записів лекцій та інших матеріалів розміщених у відповідному дистанційному курсі;*
- *допускається виконання практичних завдань в асинхронному режимі.*

Правила поведінки на заняттях:

- *на заняттях необхідно використовувати мережу Інтернет для: виконання завдань в дистанційному курсі; ознайомлення з наведеними посиланнями; доступу до сучасних впорядкованих джерел інформації;*
- *допускається використання мобільних телефонів, ноутбуків та іншої техніки.*

Правила виконання практичних робіт:

- *у разі виникнення у викладача запитань до отриманих результатів - необхідно усно пройти процедуру захисту (відповісти на запитання);*
- *вчасним вважається проходження процедури захисту на занятті присвяченому роботі або на наступному за розкладом.*

Правила призначення заохочувальних балів:

- *заохочувальні бали призначаються за виконання зазначених в роботах додаткових завдань.*

Правила призначення штрафних балів:

- *штрафні бали можуть призначатися за невчасну здачу/захист практичних робіт.*

Політика дедлайнів та перескладань:

- *проходження тестів, контрольних та здача практичних робіт виконується до останнього в семестрі заняття з дисципліни.*

8. Види контролю та рейтингова система оцінювання результатів навчання (РСО)

- *Поточний контроль: виконання практичних робіт (64 бали), опитування за темою заняття (16 бали), МКР (10 бали), ДКР (10 балів).*
- *Календарний контроль: провадиться двічі на семестр як моніторинг поточного стану виконання вимог силабусу.*
- *Семестровий контроль: залік.*
- *Умови допуску до семестрового контролю: семестровий рейтинг більше 60 балів.*

Таблиця відповідності рейтингових балів оцінкам за університетською шкалою

Кількість балів	Оцінка
100-95	Відмінно
94-85	Дуже добре
84-75	Добре
74-65	Задовільно
64-60	Достатньо
Менше 60	Незадовільно
Не виконані умови допуску	Не допущено

9. Додаткова інформація з дисципліни (освітнього компонента)

Опис матеріально-технічного та інформаційного забезпечення дисципліни

В дисципліні заплановано виконання практичних робіт на ПК з використанням програмного забезпечення *Cisco Packet Tracer*, *Wireshark*, засобів *Windows*.

Заняття проводяться онлайн, за допомогою платформи Zoom. Практичні роботи виконуються на власних ПК або на ПК в комп’ютерних лабораторіях кафедри.

Завдання, тести (опитування) та посилання на записи лекцій розміщені на платформі дистанційного навчання "Сікорський".

Робочу програму навчальної дисципліни (силабус):

Складено Нікітчук А. В.;
Ухвалено кафедрою ПРЕ (протокол № 06/2025 від 24.06.2025)
Погоджено методичною комісією факультету/ННІ (протокол № 06/2025 від 25.06.2025)