



[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	17 - Електроніка, автоматизація та електронні комунікації
Спеціальність	172 - Електронні комунікації та радіотехніка
Освітня програма	Всі ОП
Статус дисципліни	Вибіркова (Ф-каталог)
Форма здобуття вищої освіти	Заоч.
Рік підготовки, семестр	Доступно для вибору починаючи з 2-го курсу, осінній семестр
Обсяг дисципліни (год)	4 кред. (Лекц. 6 год, Практик. год, Лаб. 4 год, СРС. 110 год)
Семестровий контроль/контрольні заходи	Залік
Розклад занять	https://schedule.kpi.ua
Мова викладання	Українська
Розміщення курсу	https://do.ipk.kpi.ua/course/view.php?id=5928

Програма навчальної дисципліни

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

Сучасний етап розвитку електронних комунікацій характеризується тісним поєднанням телекомунікаційних мереж та інформаційних технологій. Комп'ютерні мережі є основою для передавання, розподіленої обробки та зберігання інформації в радіотехнічних та інфокомунікаційних системах, а розуміння принципів мережевої архітектури та механізмів кібербезпеки є базовою вимогою до кваліфікованого ІТ-фахівця.

Метою курсу є формування цілісної системи знань про архітектуру, протоколи та технології сучасних комп'ютерних мереж, а також набуття практичних навичок їх адміністрування, діагностики та захисту. Предметом вивчення є протоколи різних рівнів моделей мережевої взаємодії (OSI, TCP/IP), мережеве обладнання на базі Cisco IOS, а також методи захисту від внутрішніх і зовнішніх загроз та реагування на кіберінциденти.

Вивчення дисципліни дозволить перейти від прикладного використання мережевих ресурсів до фахового проектування, адміністрування та захисту критичної інформаційної інфраструктури, а компетентності, отримані в межах курсу, будуть основою для подальшого професійного зростання у різних галузях, наприклад:

- Інженерія зв'язку – проектування та обслуговування стійких систем передачі даних.
- Кібербезпека (SOC/Analyst) – моніторингу трафіку, виявлення аномалій та блокування атак.
- Системне адміністрування – налаштування корпоративної інфраструктури та бездротових мереж.
- IoT та Smart Systems – розбудова мереж «розумних» пристроїв та промислової автоматизації.

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

Для успішного засвоєння дисципліни студенти повинні володіти:

- навичками використання ПК;
- англійською мовою або навичками використання онлайн-перекладачів.

Пов'язані дисципліни (вибіркові):

- [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

- Тема 1. Основи безпеки в кіберпросторі та комп'ютерних мережах.
- Тема 2. Різновиди мереж та мережевого обладнання.
- Тема 3. Організація та принципи побудови мереж.
- Тема 4. Протоколи мережевого рівня та їх вразливості.
- Тема 5. Протоколи транспортного і прикладного рівня та їх вразливості.
- Тема 6. Загрози кібербезпеці та способи захисту від них.
- Тема 7. Пристрої, служби та дані безпеки.
- Тема 8. Глибокий захист, брандмауери, списки контролю доступу та політики безпеки.

4. Навчальні матеріали та ресурси

1. Тарнавський, Ю. А. Організація комп'ютерних мереж [Електронний ресурс] : підручник для студ. спеціальності 121 «Інженерія програмного забезпечення» та 122 «Комп'ютерні науки» / Ю. А.Тарнавський, І. М. Кузьменко ; КПІ ім. Ігоря Сікорського. - Електронні

- текстові дані (1 файл: 2,78 Мбайт). - Київ : КПІ ім. Ігоря Сікорського, 2018. - 259 с. - Назва з екрана.
2. Олещенко, Л. М. Організація комп'ютерних мереж [Електронний ресурс] : лабораторний практикум для студентів 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: 4,61 Мбайт). - Київ : КПІ ім. Ігоря Сікорського, 2018. - 137 с. - Назва з екрана.
 3. Вступ до кібербезпеки [Електронний ресурс]: Cisco Networking Academy. URL: <https://www.netacad.com/courses/introduction-to-cybersecurity>
 4. Основи мереж [Електронний ресурс]: Cisco Networking Academy. URL: <https://www.netacad.com/courses/networking-basics>
 5. Мережеві пристрої та початкова конфігурація [Електронний ресурс]: Cisco Networking Academy. URL: <https://www.netacad.com/courses/networking-devices-and-initial-configuration>
 6. Безпека кінцевих вузлів [Електронний ресурс]: Cisco Networking Academy. URL: <https://www.netacad.com/courses/endpoint-security>
 7. Захист мережі [Електронний ресурс]: Cisco Networking Academy. URL: <https://www.netacad.com/courses/network-defense>
 8. Управління загрозами у кібербезпеці [Електронний ресурс]: Cisco Networking Academy. URL: <https://www.netacad.com/courses/cyber-threat-management>
 - 9.

Навчальний контент

Методика опанування навчальної дисципліни (освітнього компонента)

Формат	Обсяг, год.	Тема
Лекційне заняття 1	2	Основи безпеки в кіберпросторі та комп'ютерних мережах
Лекційне заняття 2	2	Різновиди мереж та мережевого обладнання
Лекційне заняття 3	2	Організація та принципи побудови комп'ютерних мереж
СРС (відео-лекція 4)	2	Протоколи мережевого рівня та їх вразливості
СРС (відео-лекція 5)	2	Протоколи транспортного і прикладного рівня та їх вразливості
СРС (комп. практикум 1)	2	Початок роботи в Cisco Packet Tracer
СРС (комп. практикум 2)	2	Функції каналного, мережевого та транспортного рівнів
СРС (комп. практикум 3)	2	Мережева операційна система Cisco IOS
СРС (комп. практикум 4)	2	Налаштування мережевого обладнання
СРС (відео-лекція 6)	2	Типи загроз кібербезпеці та способи захисту від них
СРС (відео-лекція 7)	2	Характеристики комп'ютерних мереж. Пристрої, служби та дані безпеки
СРС (відео-лекція 8)	2	Глибокий захист, брандмауери, списки контролю доступу та політики безпеки
СРС (комп. практикум 5)	2	Дослідження загроз кінцевим вузлам
СРС (комп. практикум 6)	2	Підвищення безпеки в Windows: дослідження, моніторинг, керування та налаштування
СРС (комп. практикум 7)	2	Дослідження потоків даних у локальній мережі за допомогою Wireshark
СРС (комп. практикум 8)	2	Налаштування базових функцій безпеки WLAN
СРС (комп. практикум 9)	2	Налаштування контролю доступу та аутентифікації
СРС (комп. практикум 10)	2	Дані для моніторингу безпеки
СРС (комп. практикум 11)	2	Списки контролю доступу. Налаштування стандартних ACL
СРС (комп. практикум 12)	2	Списки контролю доступу. Налаштування розширених ACL
СРС (комп. практикум 13)	2	Управління заходами безпеки та ризиками
СРС (комп. практикум 14)	2	Аналіз кіберзагроз
СРС (комп. практикум 15)	2	Реагування на інциденти
Лабораторне заняття 1	2	Розгляд самостійно виконаних робіт

5. Самостійна робота студента

1. Перегляд відео-лекцій - 10 год.
2. Самоконтроль та тестування - 5 год.
3. Підготовка та написання модульної контрольної роботи - 5 год.
4. Виконання комп'ютерних практикумів - 30 год.
5. Виконання домашньої контрольної роботи - 15 год.
6. Опрацювання модулів дистанційного курсу, літературних джерел, підготовка до підсумкового контролю - 45 год.

(1) 9,1%	(2) 4,5%	(3) 4,5%	(4) 27,3%	(5) 13,6%	(6) 40,9%
-------------	-------------	-------------	-----------	-----------	-----------

Політика та контроль

6. Політика навчальної дисципліни (освітнього компонента)

Правила відвідування та поведінки на заняттях:

- присутність на заняттях за розкладом є важливою складовою навчального процесу, але при роботі в асинхронному режимі допускається самостійне вивчення теоретичних матеріалів.
- студенти заохочуються до використання пристроїв з доступом до мережі Інтернет в освітніх цілях (пошук інформації в мережі, доступ до навчальних матеріалів тощо).
- під час роботи в лабораторії студенти зобов'язані суворо дотримуватися правил техніки безпеки при поводженні з електрообладнанням та мережевими пристроями.

Правила захисту робіт та призначення додаткови/штрафних балів:

- захист робіт, передбачає демонстрацію конфігураційного файлу та відповіді на контрольні запитання, проходження тестів під час виконання роботи.
- роботи захищаються на відповідних заняттях за розкладом.
- штрафні бали можуть призначатися за невчасне виконання/захист (запізнення більше тижня).
- додаткові бали призначуються за виконання додаткових завдань та завдань підвищеної складності.

7.

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

- Виконання комп'ютерних практикумів (64 бали), опитування за темами лекцій (16 балів), МКР (10 балів), ДКР (10 балів).
- Умова допуску до семестрового контролю: семестровий рейтинг 60 балів і більше.

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* та засобів ОС *Windows*.

Заняття проводяться онлайн, за допомогою платформи Zoom. Комп'ютерні практикуми 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 ПРЄ (протокол № 06/2025 від 25.06.2025)

Погоджено методичною комісією факультету/ННІ (протокол № 06/2025 від 26.06.2025)