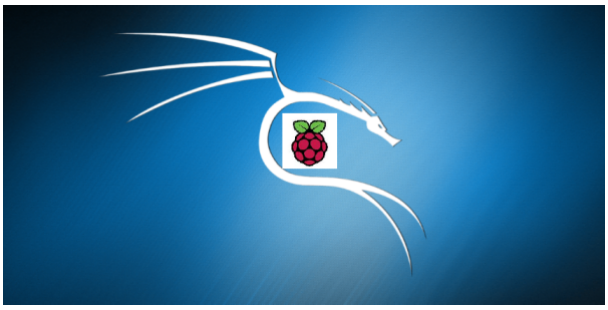
Національний технічний університет України
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Кафедра
радіотехнічних систем

[RE-77] ІНФОРМАЦІЙНА БЕЗПЕКА



Робоча програма навчальної дисципліни (Силабус)

Реквізити навчальної дисципліни

Рівень вищої освіти	Другий (магістерський)
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	Очна
Рік підготовки, семестр	Доступно для вибору починаючи з 1-го курсу, весняний семестр
Обсяг дисципліни	4 кред. (Лекц. 18 год, Практ. год, Лаб. 36 год, СРС. 66 год)
Семестровий контроль/контрольні заходи	Залік
Розклад занять	https://rozklad.kpi.ua
Мова викладання	Українська
Інформація про керівника курсу / викладачів	Лекц.: Могильний С. Б., Лаб.: Могильний С. Б., СРС.: Могильний С. Б.
Розміщення курсу	

Програма навчальної дисципліни

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

Навчальна дисципліна складається з одного розділу.

Мета навчальної дисципліни

Метою навчальної дисципліни є підготовка фахівця, який має базові компетенції в області сучасних технологій використання методів захисту інформації та програмних засобів і прикладних програм для перевірки рівня захисту інформаційних систем обміну даними.

Метою навчальної дисципліни є формування у студентів **компетентностей**:

- використовувати засоби розмежування доступу;
- виявляти атаки на комп’ютерні системи;
- застосовувати засоби цифрового підпису;
- виконувати мережеве екранування;
- застосовувати криптографічний захист інформації.

Предмет вивчення дисципліни

Предмет навчальної дисципліни – сукупність апаратних та програмних рішень для аналізу захищеності мережі, виявлення вторгнень та впровадження заходів для безпечного обміну інформацією в телекомунікаційних системах.

Програмовані результати навчання

- Використовувати засоби криптографічного захисту інформації.
- Застосовувати засоби розмежування доступу.
- Використовувати засоби виявлення атак.
- Використовувати засоби цифрового підпису.
- Впроваджувати засоби мережевого екранування.

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

Перелік дисциплін або знань та умінь, володіння якими необхідні здобувачу вищої освіти для успішного засвоєння дисципліни	Перелік дисциплін, які базуються на результатах навчання з даної дисципліни
Дисципліна вивчається на основі предметів цифрових технологій та програмування: «Інформатика», «Цифрове оброблення сигналів», «Схемотехніка»	• Наукова робота за темою бакалаврської роботи • Практика

3. Зміст навчальної дисципліни

Тема 1. Вступ в інформаційну безпеку

Тема 2. Шифрування і хешування. Служба Secure Shell.

Тема 3. Радіозакладки та методи їх виявлення.

Тема 4. Безпека фізичного і канального рівнів, міжмережеві екрани.

Тема 5. Виявлення мережевих атак.

Тема 6. Нові тенденції в технологіях захисту.

Тема 7. Національний стандарт шифрування ДСТУ 7624:2014.

Тема 8. Стандартизація у галузі захисту інформації.

4. Навчальні матеріали та ресурси

Базова література:

1. Могильний С.Б. Інформаційна безпека при роботі в Інтернеті : навчально-методичний посібник, 2018. / [За редакцією О.В.Лісового та ін.]. -К., 2018, - 105 с. (Електронна версія http://isearch.kiev.ua/uk/book/1954-445000-information-security-when-browsing-the-interne)
2. Кавун С. В. Інформаційна безпека. Навчальний посібник / С. В. Кавун, В. В. Носов, О. В.

Манжай. — Харків: Вид. ХНЕУ, 200’. — 352 с.
3. Інформаційна безпека : навчальний посібник / Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник, А. П. Бондарєв, С. С. Войтусік, А. Я. Горпенюк, О. А. Нємкова, І. М. Журавель, Б. М. Березюк, Є. І. Яковенко, В. І. Отенко, І. Я. Тишик ; за заг. ред. д-ра техн. наук, проф. Ю. Я. Бобала та д-ра техн. наук, доц. І. В. Горбатого. – Львів : Видавництво Львівської політехніки, 2019. – 580 с.

Додаткова література:

1. Akashdeep Bhardwaj, Varun Sapra. Security Incidents & Response Against Cyber Attacks. Springer, 2021, - 250 p.
2. Інформаційна безпека. Підручник / В. В. Остроухов, М. М. Присяжнюк, О. І. Фармагей, М. М. Чеховська та ін.; під ред. В. В. Остроухова – К.: Видавництво Ліра-К, 2021. – 412 с.
3. Грайворонський, М. В. Безпека інформаційно-комунікаційних систем [Електронний ресурс] : підручник / М. В. Грайворонський, О. М. Новіков. – Київ : Видавнича група BHV, 2009. – 698 с.

Інформаційні ресурси Інтернету:

1. Персональний сайт викладача: - http://isearch.kiev.ua/uk/searchpractice/internetsecurity
2. Сайт дистанційного навчання на платформі Moodle Академії Mikrotik: - http://iot.kpi.ua/lms/
3. Платформа дистанційного навчання «Сікорський»: - https://www.sikorsky-distance.org/

Навчальний контент

5. Методика опанування навчальної дисципліни (освітнього компонента)

Лекції

Лекція 1. Вступ в безпеку комп’ютерних мереж

Зміст лекції:

1. Типова IP-мережа організації.
2. Рівні інформаційної інфраструктури корпоративної мережі.
3. Концепція глибокоешелонованого захисту**.**
4. Термінологія. Загрози, вразливості і атаки**.**
5. Джерела виникнення вразливостей.
6. Класифікація вразливостей за ступенем (рівнем) ризику.

Лекція 2. Шифрування і хешування для захисту інформації

Зміст лекції:

1. Симетричне і асиметричне шифрування, їх переваги і недоліки.
2. Хешування паролів.
3. Методи злому паролів, демаскуючі фактори спроб компрометації паролів.
4. Особливості системи шифрування, вбудованої в ОС Windows.
5. Базова структура системи шифрування, впровадженої в корпорації.
6. Стандарти та програмні реалізації протоколу SSH (*Secure SHell* — «безпечна оболонка»).
7. Поняття SSH-сервера і SSH-клієнта. Команди SSH. SSH-тунель. Вразливості протоколу SSH.

Лекція 3. Типи радіозакладок, їх особливості та дешифруючі фактори

Зміст лекції:

1. Джерела витоку інформації.
2. Радіоканали витоку інформації.
3. Типові конструкції радіозакладок та їх демаскуючі фактори.

Лекція 4. Методи виявлення радіозакладок

Зміст лекції:

1. Вимірювачі потужності джерел випромінювання.
2. Аналізатори спектру.
3. Нелінійні локатори.

Лекція 5. Безпека фізичного і канального рівнів в комп'ютерних мережах

Зміст лекції:

1. MAC-адреса і розмежування доступу**.** Зміна MAC-адреси**.**
2. Мережеві аналізатори («сніфери»). Захист від «сніферів». Виявлення сніферів.

1. Захист периметра. Базові відомості про міжмережеві екрани. Технологія «stateful inspection».
2. Шлюзи рівня з'єднання. Шлюзи прикладного рівня. Системи аналізу вмісту.
3. Пакетний фільтр на базі Linux (iptables). Приклад конфігурування iptables.

1. Різновиди VPN-технологій. Реалізація VPN-технологій. Схеми використання технологій VPN.
2. Короткі відомості про IPsec. Протокол Authentication Header (AH). Протокол Encapsulated Security Payload (ESP).
3. Алгоритми, рекомендовані RFC 4305. Протокол IKE. Протокол L2TP. Протокол PPTP.

Лекція 6. Аналіз захищеності мережевих ресурсів та виявлення мережевих атак

Зміст лекції:

1. Керування вразливостями. Архітектура систем керування вразливостями.
2. Мережеві агенти сканування. Ідентифікація вразливостей.
3. Статистика аналізу захищеності. Висновки та рекомендації інструментального аналізу захищеності.
4. Необхідність технології виявлення атак. Архітектура систем виявлення атак**.**
5. Джерела даних**.** Технологія виявлення**.** Механізми реагування.
6. Система виявлення атак Snort.

Лекція 7. Використання машинного навчання для підвищення безпеки комп'ютерних мереж, безпека в IoT: архітектура системи безпеки

Зміст лекції:

1. Технології машинного навчання (МН) і їх застосування в телекомунікаціях**.**
2. Алгоритми МН для виявлення ознак втручання в систему.
3. Особливості алгоритмів МН для фільтрації спаму. Використання нейромережі для виявлення атак.

1. Моделювання ризиків в основі безпеки**.** Ключові етапи та кроки моделювання.
2. Безпека в середовищі IoT. Зони пристрою, польового і хмарного шлюзів, служб. Порівняння інформаційних і спеціалізованих пристроїв. Управління пристроєм і взаємодія з даними на пристрої.
3. Еталонна архітектура Azure IoT: моделювання ризиків.

Лекція 8. Симетричний блоковий шифр «Калина». Національний стандарт ДСТУ 7624:2014

Зміст лекції:

1. Стандартні режими роботи**.**
2. Нові режими роботи: призначення та властивості.
3. Позначення та приклади для перевірки.
4. Перспективи розвитку блокових перетворень в умовах постійного вдосконалення криптоаналітичних комплексів.

Лекція 9. Нормативно-правові засади захисту інформації та стандартизація в галузі захисту інформації

Зміст лекції:

1. Етапи створення системи захисту інформації.
2. Базові документи правових засад систем захисту інформації.
3. Офіційні документи для стандартизації рішень в галузі захисту інформації.
4. Послідовність впровадження та сертифікації систем захисту інформації.

Лабораторні роботи

Лабораторна робота 1. Використання вбудованих в ОС Windows методів шифрування

Теоретична частина

Використовується матеріал Лекції 2 та ресурсу Інтернет (навчальна платформа Moodle) для СРС.

Практична частина під час роботи в аудиторії

Вбудований парольний захист для документів MS Office. Налаштування шифрування EFS. Використання шифрування томів жорсткого диску BitLocker.

Оформлення протоколу і його збереження у відповідній папці завдання на платформі Moodle.

Завдання для самостійної роботи

Завдання та контрольні питання для самоперевірки викладені на інформаційному ресурсі Інтернету для СРС.

Лабораторна робота 2. Налаштування SSH для роботи на віддаленому комп’ютері

Теоретична частина

Використовується матеріал Лекції 2 та ресурсу Інтернет (навчальна платформа Moodle) для СРС.

Практична частина під час роботи в аудиторії

Встановлення та налаштування сервера SSH. Генерування ключів для шифрування каналу передачі даних. Перевірка роботи.

Оформлення протоколу і його збереження у відповідній папці завдання на платформі Moodle.

Завдання для самостійної роботи

Завдання та контрольні питання для самоперевірки викладені на інформаційному ресурсі Інтернету для СРС.

Лабораторна робота 3. Kali Linux на Raspberry Pi як інструмент пентестера

Теоретична частина

Використовується матеріал Лекції 1-2 та ресурсу Інтернет (навчальна платформа Moodle) для СРС.

Практична частина під час роботи в аудиторії

Встановлення Kali Linux на Raspberry Pi. Оновлення та початкове налаштування. Ознайомлення з основними інструментами пентестера. Дослідження інструментів моніторингу та тестування каналів бездротового зв’язку.

Оформлення протоколу і його збереження у відповідній папці завдання на платформі Moodle.

Практична частина для самостійної роботи

Завдання та контрольні питання для самоперевірки викладені на інформаційному ресурсі Інтернету для СРС.

Лабораторна робота 4. Використання Wireshark для аналізу трафіку

Теоретична частина

Використовується матеріал Лекції 2 та ресурсу Інтернет (навчальна платформа Moodle) для СРС.

Практична частина під час роботи в аудиторії

Встановлення Wireshark та організація роботи по захопленню пакетів. Фільтри для аналізу накопичених даних. Приклади використання Wireshark.

Оформлення протоколу і його збереження у відповідній папці завдання на платформі Moodle.

Завдання для самостійної роботи

Завдання та контрольні питання для самоперевірки викладені на інформаційному ресурсі Інтернету для СРС.

Лабораторна робота 5. Захоплення і розшифровка бездротового трафіку

Теоретична частина

Використовується матеріал Лекції 2 та ресурсу Інтернет (навчальна платформа Moodle) для СРС.

Практична частина під час роботи в аудиторії

Налаштування режиму моніторингу в Raspberry Pi. Аналіз оточення та виявлення бездротових мереж. Використання Wireshark для захоплення трафіку. Методи аналізу накопичених даних.

Оформлення протоколу і його збереження у відповідній папці завдання на платформі Moodle.

Завдання для самостійної роботи

Завдання та контрольні питання для самоперевірки викладені на інформаційному ресурсі Інтернету для СРС.

Лабораторна робота 6. Інвентаризація мережевих ресурсів з використанням утиліти nmap

Теоретична частина

Використовується матеріал Лекції 3 та ресурсу Інтернет (навчальна платформа Moodle) для СРС.

Практична частина під час роботи в аудиторії

Завантаження та запуск утиліти nmap на мікрокомп’ютері та ПК з ОС Windows. Дослідження можливостей nmap. Експериментальні дослідження з використанням nmap.

Оформлення протоколу і його збереження у відповідній папці завдання на платформі Moodle.

Завдання для самостійної роботи

Завдання та контрольні питання для самоперевірки викладені на інформаційному ресурсі Інтернету для СРС.

Лабораторна робота 7. Базове налаштування файрвола в Mikrotik

Теоретична частина

Використовується матеріал Лекції 5 та ресурсу Інтернет (навчальна платформа Moodle) для СРС.

Практична частина під час роботи в аудиторії

Дослідження файрволу з параметрами за замовчуванням. Аналіз правил. Створення власної конфігурації файрволу. Перевірка роботи файрволу.

Оформлення протоколу і його збереження у відповідній папці завдання на платформі Moodle.

Завдання для самостійної роботи

Завдання та контрольні питання для самоперевірки викладені на інформаційному ресурсі Інтернету для СРС.

Лабораторна робота 8. Побудова виділеного VPN-сервера на Raspberry Pi

Теоретична частина

Використовується матеріал Лекції 5 та ресурсу Інтернет (навчальна платформа Moodle) для СРС.

Практична частина під час роботи в аудиторії

Завантаження та встановлення ПЗ. Налаштування VPN-сервера. Перевірка роботи каналу доступу з використанням VPN**.**

Оформлення протоколу і його збереження у відповідній папці завдання на платформі Moodle.

Завдання для самостійної роботи

Завдання та контрольні питання для самоперевірки викладені на інформаційному ресурсі Інтернету для СРС.

Лабораторна робота 9. Встановлення та налаштування IDS на Snort

Теоретична частина

Використовується матеріал Лекції 6 та ресурсу Інтернет (навчальна платформа Moodle) для

СРС.

Практична частина під час роботи в аудиторії

Встановлення ПЗ для організації системи виявлення вторгнення. Налаштування системи виявлення вторгнення. Збереження логів та їх аналіз.

Оформлення протоколу і його збереження у відповідній папці завдання на платформі Moodle.

Завдання для самостійної роботи

Завдання та контрольні питання для самоперевірки викладені на інформаційному ресурсі Інтернету для СРС.

6. Самостійна робота студента

До самостійної роботи студентів включається підготовка до аудиторних занять шляхом опанування матеріалів лекцій, вивчення базової, додаткової літератури, виконання практичних робіт. Всі матеріали для СРС розміщуються на платформі дистанційного навчання Moodle (https://iot.kpi.ua/lms) та копіюються на платформу дистанційного навчання «Сікорський» (https://do.ipo.kpi.ua/course/index.php?categoryid=29).

Тема 1. Вступ в безпеку комп’ютерних мереж

Тема 2. Шифрування і хешування для захисту інформації. Служба Secure Shell

СРС до Лабораторної роботи 1.

СРС до Лабораторних робіт 2-3.

Тема 3. Типи радіозакладок, їх особливості та дешифруючі фактори. Методи виявлення радіозакладок.

СРС до Лекцій 3-4.

Тема 4. Безпека фізичного і канального рівнів в комп’ютерних мережах

СРС до Лабораторних робіт 4-8.

Тема 5. Аналіз захищеності мережевих ресурсів та виявлення мережевих атак

СРС до Лабораторної роботи 9.

Тема 6. Використання машинного навчання для підвищення безпеки комп’ютерних мереж. Безпека в IoT: архітектура системи безпеки.

СРС до Лекції 7.

Тема 7. Національний стандарт шифрування ДСТУ 7624:2014

СРС до Лекції 8.

Тема 9. Нормативно-правові засади захисту інформації та стандартизація в галузі захисту інформації

СРС до Лекції 9.

Підготовка до заліку.

Політика та контроль

7. Політика навчальної дисципліни (освітнього компонента)

7.1. Форми роботи

Лекції проводяться з використанням наочних засобів представлення матеріалу та з використанням методичних матеріалів, доступ до яких наявний у здобувачів вищої освіти. Студенти отримують всі матеріали через навчальну платформу Moodle, e-mail, кампус чи telegram-групу.

Здобувачі вищої освіти залучаються до обговорення лекційного матеріалу та задають питання, щодо його сутності.

При виконанні лабораторних робіт застосовуються форми індивідуальної та колективної роботи (командна робота, парна робота) для реалізації завдань викладача на набуття навичок самостійної практичної роботи.

Під час вивчення курсу застосовуються стратегії активного і колективного навчання, які визначаються наступними методами і технологіями:

1. методи проблемного навчання (проблемний виклад, частково-пошуковий (евристична бесіда) і дослідницький метод);
2. особистісно-орієнтовані (розвиваючі) технології, засновані на активних формах і методах навчання («мозковий штурм», «аналіз ситуацій» тощо);
3. інформаційно-комунікаційні технології, що забезпечують проблемно-дослідницький характер процесу навчання та активізацію самостійної роботи здобувачів вищої освіти (електронні презентації, застосування на основі комп'ютерних і мультимедійних засобів практичних завдань (тести), доповнення традиційних навчальних занять засобами взаємодії на основі мережевих комунікаційних можливостей (програмні засоби, мобільні додатки тощо).

7.2. Правила відвідування занять

Заняття можуть проводитись в навчальних аудиторіях згідно розкладу. Також заняття можуть проводитись дистанційно в асинхронному режимі з використанням навчальної платформи Moodle з однозначною ідентифікацією здобувача вищої освіти. Проведення занять онлайн повинне бути передбачене відповідним наказом по КПІ ім. Ігоря Сікорського.

За наявності поважних причин здобувач вищої освіти повинен завчасно (за 1 день) повідомити викладача про причини можливого пропуску контрольного заходу. Всі контрольні заходи (тести) в дистанційному режимі проводяться синхронно (одночасно для всіх студентів).

Якщо завчасно повідомити не вдалось, здобувач вищої освіти протягом одного тижня має зв'язатись з викладачем для погодження форми і порядку усунення заборгованості.

Якщо аудиторне заняття випадає на неробочий день (святковий, пам'ятний тощо), то матеріал такого заняття частково переходить в категорію «Самостійна робота здобувачів вищої освіти», а частково додається до наступного заняття.

7.3. Правила призначення заохочувальних та штрафних балів

Заохочувальні бали:

+10 балів – студенту автору статті (доповіді на конференції) за тематикою курсу (тільки за умови подання комплекту матеріалів).

Сума всіх заохочувальних балів не може перевищувати 10 балів.

Штрафні бали:

-1 бал за затримку завантаження протоколу ЛР (понад 5 днів) та відсутність без поважних причин на лабораторній роботі.

Політика університету

Політика щодо академічної доброчесності

Політика та принципи академічної доброчесності визначені у розділі 3 Кодексу честі Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського». Детальніше: https://kpi.ua/code

Норми етичної поведінки

Норми етичної поведінки студентів і працівників визначені у розділі 2 Кодексу честі Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського». Детальніше: https://kpi.ua/code

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

Головна частина рейтингу студента формується через активну участь у лабораторних роботах та отримання результатів модульної контрольної роботи (тестів).

Модульну контрольну роботу та залік проводить лектор - викладач кафедри радіотехнічних систем.

1)Поточний контроль

Проводяться експрес-опитування за темою заняття, виконання тестових завдань.

Рейтинг студента складається з балів, що отримуються за експрес-опитування за темою заняття, обговорення правових кейсів, виконання лабораторних робіт, доповнення відповідей інших студентів у процесі дискусії на лабораторних роботах, виконання тестових завдань онлайн. У випадку відсутності студента на лабораторній роботі, необхідно відпрацювати пропущене заняття. Виконання всіх лабораторних робіт є умовою отримання позитивної оцінки за результатами навчання.

1. Лабораторні заняття

Ваговий бал – 4

За виконання лабораторної роботи:

– завдання виконано повністю і самостійно 4;

– завдання виконано не повністю або за допомогою викладача 1–3;

– завдання практично не виконане 0.

Максимальна кількість балів за практичні заняття: балів.

1. Модульний контроль (МКР) – у вигляді чотирьох тестів.

Правильно і повністю виконані всі завдання тесту – 8 бали, тобто, тобто

максимальна кількість балів за МКР дорівнює:

Штрафні та заохочувальні бали за (сума як штрафних, так і заохочувальних балів не має перевищувати (4 бали):

- відсутність на лабораторній роботі без поважних причин –1

- участь у модернізації, супроводженні та адмініструванні дисципліни, виконання завдань з удосконалення методичних та дидактичних матеріалів з дисципліни +1...+2

Загальний рейтинговий бал дисципліни (максимум 100 балів):

$R_{\Sigma} = R_{І} + R_{ПР} + R_{МКР}$,

де $R_{І}$ – рейтинговий бал за підсумкову контрольну роботу (іспит)з дисципліни (від 0 до 32 балів);

$R_{ПР}$ – рейтингові бали за виконання лабораторних робіт 1-9;

$R_{МКР}$ – рейтингові бали за модульну контрольну роботу (тести)

Остаточний рейтинг не може перевищувати 100 балів.

2)Календарний контроль

Здійснюється двічі на семестр як моніторинг поточного стану виконання вимог силабусу

Критерій	*Перший*	*Другий*
Термін	*8-й тиждень*	*14-й тиждень*
Умови отримання позитивного результату	якщо поточний рейтинговий бал складає не менше 50% від максимально можливого балу на момент календарного контролю	якщо поточний рейтинговий бал складає не менше 50% від максимально можливого балу на момент календарного контролю

3)Залікова контрольна робота

Максимальна рейтингова оцінка без врахування підсумкової контрольної роботи (заліку) складає 70 балів.

Якщо здобувача вищої освіти не задовольняє набрана кількість балів, то результати рейтингової оцінки не скасовуються, а здобувач вищої освіти пише контрольну роботу (здає залік) з дисципліни, бали якої додаються до отриманих раніше.

Підсумкова контрольна робота являє собою тест, який може бути оцінений від 0 до 32 балів.

Тест проводиться на платформі дистанційного навчання Moodle і питання можуть бути різної форми, які можна реалізувати в Moodle.

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

*Лабораторні заняття проводяться в навчальних класах 203-17 і 505-17 Академії MikroTik. Для вивчення методів захисту телекомунікаційних систем використовуються мобільні станції пентестерів на основі мікрокомп'ютерів Raspberry Pi 3B+ та програмного забезпечення Kali Linux. Опис лабораторних робіт є на сайті (*http://isearch.kiev.ua/uk/book/1954-445000-information-security-when-browsing-the-interne)

Робочу програму навчальної дисципліни (силабус):
Складено Могильний С. Б.;
Ухвалено кафедрою РТС (протокол № 06/2023 від 22.06.2023)
Погоджено методичною комісією факультету/ННІ (протокол № 06-2023 від 29.06.2023)