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

Кафедра телекомунікацій

ПРОТИДІЯ ХАКЕРСЬКИМ АТАКАМ В МОБІЛЬНИХ ІНФОКОМУНІКАЦІЯХ

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	*Інженерія інноваційних інформаційно-телекомунікаційних технологій та систем*
Статус дисципліни	*Вибіркова*
Форма навчання	*очна(денна)*
Рік підготовки, семестр	*1 курс, весняний семестр*
Обсяг дисципліни	*5 кредитів - 150 годин*
Семестровий контроль/ контрольні заходи	*Екзамен / МКР*
Розклад занять	*3 години на тиждень, https://rozklad.kpi.ua*
Мова викладання	*Українська*
Інформація про керівника курсу / викладачів	Лектор: *д.т.н., професор, лауреат Державної премії України в галузі науки і техніки, Кравчук Сергій Олександрович, http://tk-its.kpi.ua/uk/node/237* Практичні / Семінарські: *Баранов Олександр Андрійович*, http://intellect.kpi.ua/profile/pim14
Розміщення курсу	Google classroom, код курсу: eexg3yt, https://classroom.google.com/c/MTUyNzI1MDIyNzcw

Програма навчальної дисципліни

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

Метою дисципліни є формування у студентів знань з основ інженерно-технічного захисту інформації в телекомунікаційних системах, а також навичок і вміння в застосуванні знань для конкретних умов. Крім того, метою дисципліни є розвиток в процесі навчання системного мислення, необхідного для вирішення завдань інженерно-технічного захисту інформації з урахуванням вимог системного підходу. Курс надає компетенції щодо освоєння принципів та методів протидії несанкціонованому доступу в мобільних інфокомунікаціях, оцінки можливих вразливостей комунікаційних мереж для хакерських атак.

Предметом дисципліни є безпека інформаційно-телекомунікаційних систем з підтримкою мобільності від можливих хакерських атак.

Дисципліна надає компетенції щодо застосування технічних засобів і методів захисту інформації при проектуванні і експлуатації систем забезпечення безпеки телекомунікаційних систем і мереж нових інформаційно-телекомунікаційних технологій. Курс допоможе сформувати творчу особистість студента та навчить самоактуалізації його творчого потенціалу.

Набуті знання:

- технології підтримання безпеки доступу користувачів до інфокомунікаційних мереж;
- основні положення та методи захисту мобільних інфокомунікацій від зовнішніх хакерських атак;
- концепції інженерно-технічного захисту інформації в телекомунікаційних мережах;
- теоретичні основи інженерно-технічного захисту інформації;
- фізичні основи технічного захисту інформації;
- технічні засоби захисту інформації в телекомунікаційних системах;
- організаційні основи інженерно-технічного захисту інформації;
- технології та методи визначення атак від мобільних терміналів та базових станцій; методи локалізації зовнішніх вторгнень до мережі Телекому.

Набуття навичок і вмінь: виконувати науково-дослідні роботи по вдосконаленню сучасних інфокомунікаційних мереж щодо підвищення їх ефективності і безпеки; проводити технічне обслуговування (програмними засобами) системи керування мережею; поєднувати дослідницьку, проектну і виробничу діяльність у власній практиці.

Уміння виконувати роботи щодо застосування інженерних засобів і методів протидії хакерським атакам; проектувати дослідницьку роботу і отримувати з неї теоретичні і практичні результати. Курс допоможе сформувати творчу особистість студента та навчить самоактуалізації його творчого потенціалу.

Досвід:

- набути навичок практичного використання теоретичних знань у практичній діяльності;

- дослідження можливостей нових методів протидії атакам зловмисників та фроду в інформаційно-телекомунікаційних системах з метою підтримки стабільного функціонування останніх.

Вивчення навчальної дисципліни додатково забезпечує:

- формування у студентів таких *програмних компетентностей*:

ЗК 2 Здатність генерувати нові ідеї й нестандартні підходи до їх реалізації (креативність);

ЗК 8 Здатність до ефективних комунікаційних взаємодій, в тому числі засобами інформаційних технологій;

ФК 5 Здатність використовувати інформаційні технології, методи інтелектуалізації та візуалізації, штучного інтелекту для дослідження та аналізу процесів у системах електронних комунікацій та радіотехнічних системах;

ФК 19 Здатність будувати, забезпечувати безпеку та функціонування, аналізувати і вдосконалювати мережі радіо доступу, конвергентні IoT мережі, інфокомунікаційні інфраструктури операторського класу;

- набуття студентами наступних *програмних результатів навчання*:

ПРН 6 Досліджувати процеси у системах електронних комунікацій та радіотехнічних системах з використанням засобів автоматизації інженерних розрахунків, планування та проведення наукових експериментів з обробкою і аналізом результатів;

ПРН 18 Практикувати інформаційний та науковий пошук, використовувати бази даних і знань, критично осмислювати та інтерпретувати результати, робити висновки та формувати напрями дослідження з урахуванням вітчизняного й закордонного досвіду.

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

Для успішного засвоєння дисципліни студент повинен *володіти знаннями*, які отримані при здобутті вищої освіти першого (бакалаврського) рівня.

Навчальна дисципліна додатково підготовлює студентів до проходження науково-дослідної практики, виконання магістерської дисертації та подальшої роботи за фахом.

3. Зміст навчальної дисципліни

Тема 1. Підтримка мобільності в телекомунікаційних системах абонентського доступу

Тема 2. Передача обслуговування. Визначення та класифікація

Тема 1. Моделі загроз. Вступ до безпеки
Моделі загроз
Безпека мережі
Поділ хакерів на категорії
Санкціоноване і несанкціоноване одержання інформації
Система технічних засобів для забезпечення функцій оперативно-розшукових заходів - СОРМ

Тема 2. Канали витоку інформації в телекомунікаційних системах та мережах
Поняття і особливості витоку інформації.
Канали витоку інформації за рахунок паразитних зв'язків.
Контроль і прослуховування телефонних каналів зв'язку.
Побудова захищених розподілених систем на основі безпроводових мереж

Тема 3. Захист інформації в мережах мобільного зв’язку
Проблеми захисту інформації в мережах мобільного зв’язку третього покоління
Аналіз вразливостей мобільних стільникових мереж та способи їх усунення

Тема 4. Сигналізація та вразливості
Сигналізація в системах мобільного зв’язку
Від SS7 до SIGTRAN в GSM/GPRS
SS7 та роумінг
Вразливості мереж мобільного зв'язку через SS7
Протидія фрод-атакам
Підключення до мережі оператора для здійснення несанкціонованого втручання
SMS фрод. Класифікація та методи захисту

Тема 5. Системи глибокого аналізу та візуалізації
Системи глибокого аналізу трафіку DPI мобільних операторів
Система візуалізації подій мережі
Тема 6. Захист в мобільних мережах 5-го покоління
Програмні модулі або мережні функції архітектури 5G
Розділ площин керування і користувачів CUPS
Мережне нарізання Network Slicing
Ідентифікатори користувачів
Загальні положення безпеки в мережі 5G
Процедура аутентифікації та узгодження ключів
Основні аспекти концепції безпеки мережі 5G

Тема 6. Вразливості технологій хмарних обчислень
Концепції хмарних обчислень
Використання хмарних сервісів для генерування DDOS атак
Запуск неправомірних кодів підбору та зламу паролів
Розміщення шкідливого програмного забезпечення
Створення ботнет мереж
Неможливість контролювання коректності організації доступу на стороні клієнта

Тема 7. Основи безпеки даних в Телекомі
Застосування технології шифрування
Технології безпеки даних
Технології аутентифікація
RADIUS
Технології цілісності і конфіденційності
Технології видаленого доступу до віртуальних приватних мереж

Тема 8. Безпека блокчейна
Криптографічні алгоритми
Ключі (гаманці)
Алгоритми консенсусу
Смарт-контракти
Можливість проведення атаки DNS
Компоненти інтерфейсу користувача та додатків

Тема 9. Захищеності сучасних безпроводових технологій IoT
smart-пристрої;
мережеві шлюзи та канали передачі даних;
програмні IoT-платформи.

4. Навчальні матеріали та ресурси

Базова література:

1. Ільченко М.Ю., Кравчук С.О. Телекомунікаційні системи. – Київ: Наукова думка, 2017. – 730 с.
2. Дистанційний курс «Протидія хакерським атакам в інфокомунікаціях. Вразливість інфокомунікаційних мереж хакерським атакам». URL розміщення на сайті: https:// https://classroom.google.com/c/MTU5MjAyMzEwMTAx.
3. Системи зв’язку з рухомими об’єктами / С.О. Кравчук, О.Г. Голубничий, А.Г. Тараненко, В.Г. Потапов, О.П. Ткаліч: підручник. – К.: Спринт-Сервіс, 2012. – 452 с.

4. Досягнення в телекомунікаціях 2019 / за наук. ред. М.Ю. Ільченка, С.О. Кравчука: монографія. - Київ: Інститут обдарованої дитини НАПН України, 2019.- 336 с. Рекомендовано до друку ВР КПІ ім.І.Сікорського (прот.№10 від 04.11.2019 р.) ISBN 978-617-7734-12-2

Додаткова література (монографії, статті, документи, електронні ресурси):

1. Chirillo J. Hack Attacks Revealed: A Complete Reference for UNIX, Windows, and Linux with Custom Security Toolkit. - Wiley Computer Publishing, 2001. - 862 p. (ISBN 0471232823).
2. Erickson J. Hacking: The Art of Exploitation. - No Starch Press; 2nd edition, 2008. – 488 p. (ISBN-10: 1593271441)
3. Flow S. How to Hack Like a GOD: Master the secrets of hacking through real life scenarios. – 2017. - 250 p.
4. Tech-invite all 3GPPSpecs + all IETFRFCs https://www.tech-invite.com/index.html
5. Yang Q., Huang L. Inside Radio: An Attack and Defense Guidec. Publishing House of Electronics Industry, Beijing and Springer Nature Singapore Pte Ltd. 2018 ISBN 978-981-10-8446-1 ISBN 978-981-10-8447-8 (eBook), https://doi.org/10.1007/978-981-10-8447-8.
6. Барабаш П.А. Навчально-методичний комплекс «Безпека телекомунікаційних мереж» за спеціальністю 230201.65 Інформаційні системи та технології (Спеціалізація Безпека інформаційних систем) – СПб.: СУРАО, 2013. - 38 с.
7. 3GPP TS 33.501 - Security architecture and procedures for 5G system (Release 15)
8. Huang A. The Hardware Hacker: Adventures in Making and Breaking Hardware Hardcover. - No Starch Press. – 2017. – 416 p. (ISBN-10 : 159327758X).

Навчальний контент

5. Методика опанування навчальної дисципліни (освітнього компонента)

Застосовуються стратегії активного і колективного навчання: методи проблемного навчання; особистісно-орієнтовані (розвиваючі) технології, засновані на активних формах і методах навчання; інформаційно-комунікаційні технології, що забезпечують проблемно-дослідницький характер процесу навчання та активізацію самостійної роботи студентів (електронні презентації для лекційних занять, використання аудіо-, відео-підтримки навчальних занять).

На лекціях розкриваються найбільш суттєві теоретичні питання, які дозволяють забезпечити студентам можливість глибокого самостійного вивчення всього програмного матеріалу.

На практичних заняттях студенти отримують навики у вирішенні розрахункових задач, навчаються методикам оцінки результатів вимірювань.

Лекційні заняття

Лекція 1. Моделі загроз. Вступ до безпеки
Моделі загроз
Безпека мережі
Поділ хакерів на категорії

Лекція 2. Санкціоноване і несанкціоноване одержання інформації
Система технічних засобів для забезпечення функцій оперативно-розшукових заходів - СОРМ
Обладнання для СОРМ
Система перехоплення телекомунікацій (СПТ)
Встановлення шпигунського трояна
Підроблена базова станція
Вразливості технологій хмарних обчислень
Символьна вразливість мобільних терміналів

Лекція 3. Канали витоку інформації в телекомунікаційних системах та мережах
Поняття і особливості витоку інформації.
Структура, класифікація та основні характеристики технічних каналів витоку інформації.
Технічні канали витоку інформації при передачі її в телекомунікаційних системах.
Електромагнітні канали витоку інформації.
Канали витоку інформації за рахунок паразитних зв'язків.
Контроль і прослуховування телефонних каналів зв'язку.

Лекція 4. Побудова захищених розподілених систем на основі безпроводових мереж
Основні принципи проектування захищених бездротових мереж.
Створення аутентифікаційної інфраструктури.
Застосування криптографічних алгоритмів.
Застосування інфраструктури відкритих ключів (PKI)

Лекція 5. Проблеми захисту інформації в мережах мобільного зв’язку третього покоління
Архітектура мережі
Види атак
Механізми захисту

Лекція 6. Аналіз вразливостей мобільних стільникових мереж та способи їх усунення
Вразливості системи стільникового зв'язку стандарту GSM
Вразливості системи стільникового зв'язку стандарту UMTS
Вразливості системи стільникового зв'язку стандарту LTE

Лекція 7. Сигналізація в системах мобільного зв’язку
Стек протоколів SS7 та його особливості в мережах стільникового зв’язку
Закальнокальна система сигналізації №7 (Signalling System #7, або ж просто SS7)
SS7 в системі GSM
SS7 архітектура vs модель OSI/ISO
SS7 архітектура, стислий опис рівнів та підсистем
Від SS7 до SIGTRAN в GSM/GPRS
Рівень MTP. Адресація та маршрутизація
Рівень SCCP. Адресація та маршрутизація
Рівень MAP. Способи застосування. Основні транзакції
SS7 та роумінг

Лекція 8. Вразливості мереж мобільного зв'язку через SS7- 1
Уразливості мереж SS7. Актуальність проблеми
Еволюція проблем безпеки сигналізації
Категорії SS7 MAP повідомлень
Основні сценарії фрод-атак
Основні документи GSMA
Рекомендації щодо протидії фрод-атакам

Лекція 9. Вразливості мереж мобільного зв'язку через SS7 - 2
Підключення до мережі оператора для здійснення несанкціонованого втручання
Сценарій атаки з розкриття ідентифікатора мобільного абонента (IMSI)
Сценарій атаки з розкриття місцезнаходження мобільного абонента
Сценарій атаки з перехоплення вхідних СМС-повідомлень
Сценарій атаки з порушення доступності абонента
Сценарій атаки з маніпуляції з USSD
Сценарій атаки зі зміною профілю абонента в VLR

Сценарій атаки з прослуховування вихідних дзвінків
Схема атаки з перенаправленням вхідного виклику
Схема атаки з перенаправленням вхідного виклику на дорогий міжнародний напрямок
Схема атаки на відмову в обслуговуванні MSC для вхідних голосових викликів
Процедура/запит sendRoutingInfoForSM

Лекція 10. Системи глибокого аналізу та візуалізації
Системи глибокого аналізу трафіку DPI мобільних операторів
Аналіз мережного трафіку
Поверховий аналіз пакетів SPI
Середній аналіз пакетів MPI
Глибокий аналіз пакетів DPI
Системи глибокого аналізу трафіку DPI для мобільних операторів
Система візуалізації подій мережі
Система візуалізації подій мережі
Інтелектуальні Системи-ГЕО
Візуалізація інформації на карті

Лекція 11. SMS фрод. Класифікація та методи захисту
Актуальність проблеми
Постановка проблеми – SMS фрод
Основні сценарії атак та методи захисту

Лекція 12. Захист в мобільних мережах 5-го покоління - 1
Особливості і становлення систем 5G
Архітектура мережі 5G
Програмні модулі або мережні функції архітектури 5G
Розділ площин керування і користувачів CUPS
Мережне нарізання Network Slicing
PDU-сесії
Ідентифікатори користувачів

Лекція 13. Захист в мобільних мережах 5-го покоління - 2
Загальні положення безпеки в мережі 5G
Процедура аутентифікації та узгодження ключів
Ієрархія криптографічних ключів
Захист користувальницького та сигнального трафіку
Основні аспекти концепції безпеки мережі 5G

Лекція 14. Вразливості технологій хмарних обчислень
Концепції хмарних обчислень
Можливості хмарних обчислень
Використання хмарних сервісів для генерування DDOS атак
Запуск неправомірних кодів підбору та зламу паролів
Розміщення шкідливого програмного забезпечення
Створення ботнет мереж
Неможливість контролювання коректності організації доступу на стороні клієнта

Лекція 15. Основи безпеки даних в Телекомі
Криптографія
Симетричне шифрування
Асиметричне шифрування

Безпечні хеш-функції
Застосування технології шифрування

Лекція 16. Технології безпеки даних
Технології аутентифікація
RADIUS
Технології цілісності і конфіденційності
Технології видаленого доступу до віртуальних приватних мереж

Лекція 17. Безпека блокчейна
Криптографічні алгоритми
Ключі (гаманці)
Алгоритми консенсусу
Смарт-контракти
Можливість проведення атаки DNS
Компоненти інтерфейсу користувача та додатків

Лекція 18. Захищеності сучасних безпроводових технологій IoT
smart-пристрої;
мережеві шлюзи та канали передачі даних;
програмні IoT-платформи.

Практичні заняття

Основні завдання циклу практичних занять: закріплення студентами теоретичних положень навчальної дисципліни і набуття умінь та досвіду їх практичного застосування.

Основні увага циклу практичних занять є навчання (на прикладах) роботи студентів щодо технологій визначення місця розташування абонентів у системах стільникового зв'язку.

№ з/п	Назва теми практичних занять та перелік основних питань
1	**Практичне заняття 1.** Атаки переповнення буфера Buffer overflows Ознайомитьсь із вразливими місцями переповнення буфера в контексті веб-сервера під назвою zookws Пошук переповнення буфера Впровадження коду Повернення до libc атакам Виправлення переповнення буфера та інші помилки
2	**Практичне заняття 2**. Загальні поняття захисту інформації в телекомунікаційних системах (ТКС) і мережах Система безпеки. Система захисту інформації. Криптографічне забезпечення інформаційної безпеки в ТКС
3	**Практичне заняття 3**. Класифікація загроз безпеки інформації в телекомунікаційних системах та мережах Основні питання: Загрози несанкціонованого доступу (НСД). Варіант атаки з використанням DNS-сервера.
4	**Практичне заняття 4**. Загрози програмно-математичного впливу і способи захисту від них. Основні питання: Деструктивні функції шкідливих немережевих програм

	Заходи захисту від несанкціонованого доступу, створювані на етапі розробки програмного забезпечення. Заходи захисту від несанкціонованого доступу, що формуються і застосовуються на етапі експлуатації об'єкта, що захищається. Антивірусні сканери, програми-ревізори, програми-фільтри ("вартові") і антивірусні блокувальники, іммунізатори
5	**Практичне заняття 5**. Захист інформації від загроз, пов'язаних з несанкціонованим доступом Індукційні канали витоку інформації Програмні засоби адміністрування (розмежування повноважень, реєстрації та контролю). Сканери безпеки. Міжмережеві екрани.
6	**Практичне заняття 6**. Побудова захищених розподілених систем на основі бездротових мереж Основні питання: Приклади застосування інфраструктури відкритих ключів (PKI)
7	**Практичне заняття 7**. Організаційні основи інженерно-технічного захисту інформації в телекомунікаційних системах та мережах Вимоги до підсистеми забезпечення цілісності інформації.Особливості інструментального контролю ефективності інженерно-технічного захисту інформації.
8	**Практичне заняття 8**. Практичні приклади атак усередині GSM мережі-2 Встановлюємо osmo-sip-connector та asterisk Налаштовуємо Asterisk Захоплення абонента в нашу мережу GSM MCC/MNC MITM під час GPRS-серфінгу CMC-фішинг Перенаправлення та запис голосових дзвінків Radio Resource LCS (Location Service) Protocol
9	**Практичне заняття 9**. Детально про атаку на порт SIM-карти Подробиці атаки Послідовність подій урок та рекомендації

Семінарські заняття

Семінарських занять по дисципліні не передбачено.

Лабораторні заняття (комп’ютерний практикум)

Лабораторних занять по дисципліні не передбачено.

6. Самостійна робота студента/аспіранта

Основні види самостійної роботи студента це підготовка до аудиторних занять, повторення навчального матеріалу, який був прослуханий на лекційних заняттях, проведення розрахунків за первинними даними, розв’язок задач.

Політика та контроль

7. Політика навчальної дисципліни (освітнього компонента)

- **Відвідування занять**. відвідування студентами всіх видів навчальних занять є умовою опанування навчального матеріалу, набуття відповідного комплексу знань та умінь. Відсутність на аудиторному занятті не передбачає нарахування штрафних балів, оскільки

фінальний рейтинговий бал студента формується виключно на основі оцінювання результатів навчання. Разом з тим, відповіді на запитання лектора, обговорення результатів виконання практичних завдань, а також захист результатів практичних і контрольних робіт оцінюватимуться тільки під час аудиторних занять.

- **Пропущені контрольні заходи оцінювання**. Кожен студент має право відпрацювати пропущені з поважної причини (лікарняний, мобільність тощо) заняття за рахунок самостійної роботи. Детальніше за посиланням: https://kpi.ua/files/n3277.pdf. **Перескладання** завдань контрольних заходів не передбачено, за виключенням випадків, коли студент був відсутнім на контрольному заході *з поважних причин*. Студенту необхідно бути уважними на заняттях, не відволікатися, не заважати іншим, при проведенні під час занять контрольних заходів (літучки, контрольні роботи) необхідно здійснити відключення засобів зв'язку (смартфонів, планшетів, ноутбуків) для запобігання пошуку інформації на гугл-диску викладача, в інтернеті, тощо.
- **Процедура оскарження результатів контрольних заходів оцінювання**. Студент може підняти будь-яке питання, яке стосується процедури контрольних заходів та очікувати, що воно буде розглянуто згідно із наперед визначеними процедурами. Студенти мають право аргументовано оскаржити результати контрольних заходів, пояснивши з яким критерієм не погоджуються відповідно до оціночного.
- **Календарний контроль** проводиться з метою підвищення якості навчання студентів та моніторингу виконання студентом вимог силабусу.

Критерій	Перший календарний контроль	Другий календарний контроль
Термін календарного контролю	Тиждень 8	Тиждень 14
Умови отримання позитивної оцінки	Не менше 15 балів	Не менше 30 балів

- **Академічна доброчесність**. 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. Під час проведення заходів, які передбачені навчальним планом (аудиторні заняття, контрольні заходи) студентам необхідно дотримуватись правил академічної доброчесності.
- **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.
- **Інклюзивне навчання**. Засвоєння знань та умінь в ході вивчення дисципліни «Геоінформаційні системи» може бути доступним для більшості осіб з особливими освітніми потребами, окрім здобувачів з серйозними вадами зору, які не дозволяють виконувати завдання за допомогою персональних комп'ютерів, ноутбуків та/або інших технічних засобів.
- **Навчання іноземною мовою**. У ході виконання завдань студентам може бути рекомендовано звернутися до англомовних джерел.
- **Заохочувальні** бали можна отримати за підготовку доповіді на тему, яка попередньо обговорюється з викладачем, за зразкове ведення конспекту, підготовку демонстраційних матеріалів (макетів, презентацій) за тематикою занять. Заохочувальні бали також нараховуються викладачем за: написання тез, статті, підготовка оглядів як наукової роботи для участі у конкурсі студентських наукових робіт (тільки за тематикою навчальної дисципліни), участь у міжнародних, всеукраїнських та/або інших заходах та/або конкурсах (тільки за тематикою навчальної дисципліни). Участь в "Sikorsky Challenge" та конференції «Перспективи телекомунікацій». Заохочувальні бали не входять до основної шкали РСО, а їх сума не може перевищувати 10% рейтингової шкали для РСО.

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

Семестрова атестація проводиться у вигляді екзамену. Для оцінювання результатів навчання застосовується 100-бальна рейтингова система.

***Поточний контроль**:* експрес-опитування, опитування за темою заняття, фронтальні опитування, захист практичних робіт, електронне звітування, МКР.

***Календарний контроль**:* провадиться двічі на семестр як моніторинг поточного стану виконання вимог силабусу.
Семестровий контроль: екзамен.
***Умови допуску** до семестрового контролю:* семестровий рейтинг більше 30 балів.

РСО дисципліни з екзаменом має дві складові: стартової – оцінювання навчальної діяльності здобувача впродовж семестру (50 балів) та підсумкової – оцінювання результатів навчальної діяльності здобувача під час проведення екзамену (50 балів).
1. Рейтинг студента з кредитного модуля розраховується виходячи із 100-бальної шкали. Рейтинг студента складається з балів, що він отримує за:
– виконання експрес-контрольних робіт (4 експрес-контроля);
– роботу на практичних заняттях (2 опитування);
– виконання модульної контрольної роботи (МКР);
– відповідь на екзамені (до 50 балів).

2. Критерії нарахування балів.
2.1. Експрес-контрольні роботи оцінюються із 5 балів кожна:
– «відмінно» – повна відповідь (не менше 90% потрібної інформації) – 5 балів;
– «добре» – достатньо повна відповідь (не менше 75% потрібної інформації) або повна відповідь з незначними неточностями – 4 бали;
– «задовільно» – неповна відповідь (не менше 60% потрібної інформації) та незначні помилки – 3 бали;
– «незадовільно» – відповідь не відповідає вимогам до «задовільно» – 0 балів.

2.2. Робота на практичних заняттях оцінюється із 10 балів:
- «відмінно» – самостійна відповідь (розв'язана задача, виконане завдання) – 9-10 балів;
- «добре» – відповідь (розв'язана задача, виконане завдання) з незначною допомогою викладача (аудиторії) – 7-8 балів;
- «задовільно» – відповідь (розв'язана задача, виконане завдання) зі значною допомогою викладача (аудиторії) – 6 балів;
- «незадовільно» – студент не здатний відповісти на поставлене питання (розв'язати задачу, виконати завдання) навіть з допомогою викладача – 0 балів.

2.3. Модульна контрольна робота оцінюється із 10 балів:
– «відмінно» – правильно і повністю виконані всі завдання (не менше 90% потрібної інформації) – 9-10 балів;
– «добре» – частково виконані завдання (не менше 75% потрібної інформації) – 7-8 балів;
– «задовільно» – завдання контрольної роботи виконані із помилками (не менше 60% потрібної інформації) – 6 балів;
– «незадовільно» – завдання не виконані або містять грубі помилки, МКР не зараховано – 0 балів.

2.4. Екзамен оцінюється із 50 балів. На екзамені студенти відповідають на питання білету та додаткове запитання. Кожен білет містить чотири запитання (завдання). Кожне запитання (+ додаткове) (завдання) оцінюється у 10 балів за такими критеріями:
– «відмінно», повна відповідь, не менше 90% потрібної інформації (повне, безпомилкове розв'язування завдання) – 9-10 балів;
– «добре», достатньо повна відповідь, не менше 75% потрібної інформації, є незначні неточності (повне розв'язування завдання з незначними неточностями) – 7-8 балів;
– «задовільно», неповна відповідь, не менше 60% потрібної інформації, деякі помилки (завдання виконане з певними недоліками) – 6 балів;
– «незадовільно», відповідь не відповідає умовам до «задовільно» – 0 балів.

Календарна проміжна атестація студентів проводиться за значенням поточного рейтингу студента на час атестації. Якщо значення цього рейтингу не менше 50 % від максимально можливого на час атестації, студент вважається атестованим. Умовою позитивної першої атестації є отримання не менше 15 балів.
Для отримання допуску до екзамену потрібно мати рейтинг не менше 30 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
семестровий рейтинг менше 30 балів	Не допущено

9. Додаткова інформація з дисципліни (освітнього компонента)

Передбачена можливість зарахування сертифікатів проходження дистанційних чи онлайн курсів за тематикою навчальної дисципліни або її окремих тем за умови, що кількість годин проходження відповідних курсів не менша ніж кількість годин, що відводиться на вивчення навчальної дисципліни або окремої теми.

Комунікація з викладачем будується за допомогою використання інформаційної системи «Електронний кампус», платформи дистанційного навчання «Сікорський», а також такими інструментами комунікації, як електронна пошта, Telegram і Viber. Під час навчання та для взаємодії зі студентами використовуються сучасні інформаційно-комунікаційні та мережеві технології для вирішення навчальних завдань.

Робочу програму навчальної дисципліни (силабус):

Складено завідувачем кафедри, д.т.н., професором, Кравчуком Сергієм Олександровичем

Ухвалено кафедрою телекомунікацій (протокол № 11 від 25.05.2023 р.)

Погоджено Методичною комісією НН ІТС (протокол № 4 від 08.06.2023 р.)