

Рекомендовано  
на засіданні кафедри  
транспортного зв'язку  
прот. № 1 від 11.09.2023 р.

СИЛАБУС З ДИСЦИПЛІНИ  
**БЕЗПЕКА ТЕЛЕКОМУНІКАЦІЙНИХ  
СИСТЕМ ТА МЕРЕЖ**  
II семестр 2023-2024 навчального року

Освітній рівень другий (магістерський)

Галузь знань 17 Електроніка, автоматизація та електронні комунікації

Спеціальність 172 Електронні комунікації та радіотехніка

Освітня програма Телекомунікації та радіотехніка

Проведення занять згідно розкладу <http://rasp.kart.edu.ua/>

Команда викладачів:

Лектор:

Індик Сергій Володимирович (кандидат технічних наук, ст. викладач),  
Контакти: +38 (057) 730-10-81, e-mail: [serhii.indyk@kart.edu.ua](mailto:serhii.indyk@kart.edu.ua)

Асистент лектора:

Індик Сергій Володимирович (кандидат технічних наук, ст. викладач),  
Контакти: +38 (057) 730-10-81, e-mail: [serhii.indyk@kart.edu.ua](mailto:serhii.indyk@kart.edu.ua)

Години прийому та консультації: вівторок з 14.10-15.30

Веб сторінка курсу: <http://do.kart.edu.ua/>

Додаткові інформаційні матеріали: <http://metod.kart.edu.ua>

Завданням дисципліни є навчання студентів побудуванню аналітичних моделей порушників, оцінки їх можливостей та інтерпретації результатів аналізу і оцінки ризиків безпеки, застосування методів системного аналізу у вирішенні задач захисту інформації. Вивчення студентами сучасних методів побудови безпечних систем, що відповідають вимогам провідних міжнародних стандартів. Студент буде вміти розробляти вимоги та обирати для впровадження заходи захисту інформації; вибирати та застосовувати критерії та показники оцінки рівня захищеності; розробляти функціональні моделі процесів захисту інформації, організувати діяльність персоналу згідно вимог ISO/IEC 27001; розробляти моделі загроз безпеці інформації; розробляти та верифікувати профілі захисту інформації згідно вимог НД ТЗІ; оцінювати ризики безпеки згідно вимог ISO/IEC 27005; застосовувати стандартні пакети при розв'язанні прикладних задач моделювання процесів захисту інформації.

### **Курс має на меті сформувати та розвинути наступні компетентності студентів:**

Здатність до абстрактного мислення, аналізу та синтезу (ЗК-1).

Здатність працювати в команді (ЗК-2).

Здатність виявляти, ставити та вирішувати проблеми (ЗК-3).

Здатність до пошуку, оброблення та аналізу інформації з різних джерел (ЗК-4).

Здатність приймати обґрунтовані рішення (ЗК-5).

Здатність працювати в міжнародному контексті (ЗК-6).

Здатність вирішувати комплексні проблеми у галузі телекомунікацій та радіотехніки, у тому числі в умовах залізничного транспорту, із застосуванням різноманітних методів та підходів (ФК-1).

Здатність застосовувати системний підхід до вирішення інженерних проблем з розробки, проектування, побудови, експлуатації, ремонту, модернізації об'єктів телекомунікаційної інфраструктури, у тому числі технологічного зв'язку залізничного транспорту (ФК-2).

Здатність досліджувати, аналізувати та вдосконалювати технологічні процеси в телекомунікаційній інфраструктурі, у тому числі залізничного транспорту на основі технологій передавання, обробки, кодування, зберігання інформації (ФК-3).

Здатність приймати ефективні рішення щодо вибору методів, засобів, обладнання та заходів для реалізації новітніх телекомунікаційних технологій в телекомунікаційній інфраструктурі, у тому числі технологічного зв'язку залізничного транспорту (ФК-4).

Здатність грамотно здійснювати аналіз і синтез під час проектування, експлуатації, ремонту та технічного обслуговування об'єктів телекомунікаційної інфраструктури, зокрема систем технологічного зв'язку залізничного транспорту (ФК-5).

Здатність вибирати та застосовувати на практиці методи дослідження, планування та проведення експериментів; інтерпретувати результати та робити висновки щодо рішень, що приймаються у сфері виробництва, експлуатації та ремонту об'єктів телекомунікаційної інфраструктури, у тому числі для вирішення задач залізничного транспорту (ФК-6).

Здатність використовувати закони й принципи інженерії в сфері телекомунікацій та радіотехніки, математичний апарат високого рівня для проектування, розробки, експлуатації, технічного обслуговування та модернізації об'єктів, явищ і процесів, у тому числі в умовах залізничного транспорту (ФК-7).

## Чому ви маєте обрати цей курс?

Вивчивши курс студент буде обізнаним з факторами та каналами уразливості інформації, основними методами, принципами, способами, алгоритмами та протоколами захисту інформації; критеріями та показниками оцінки якості захисту інформації; методами оцінювання та аналізу загроз та ризиків безпеки; основними протиріччями, проблемами, тенденціями та напрямками розвитку теорії та практики захисту інформації, прогнозування їх можливостей та можливостей порушників; функціональними можливостями та порядком застосування сучасних методів аналізу ризиків безпеки; методами оцінки ефективності систем управління інформаційною безпекою.

Команда викладачів і Ваші колеги будуть готові надати будь-яку допомогу з деякими з найбільш складних аспектів курсу по електронній пошті і особисто – у робочий час.

## Огляд курсу

Цей курс, який вивчається протягом другого семестру, дає студентам глибоке розуміння в розробці та пропонуванні нових технічних рішень та застосувань нових технологій у сфері безпеки телекомунікаційних систем та мереж.

Курс складається з лекцій та лабораторних занять. Курс супроводжується пояснювально-ілюстративним матеріалом. Студенти матимуть можливість застосовувати отримані знання та вирішувати практичні завдання протягом обговорень на заняттях.

### Схема курсу

<b>Поміркуй</b>	Лекції	<b>Виконай</b>
	Матеріал для самостійної роботи	
	Обговорення на заняттях	
	Лабораторні заняття	
	Курсовий проект	
	Консультації	
	Екзамен	

Лабораторні заняття курсу передбачають виконання завдань щодо оцінки критичності інформаційних ресурсів, дослідження функціональних можливостей спеціалізованого програмного забезпечення, програмній реалізації виявлення мережових атак, оцінку ефективності систем захисту інформації.

## Ресурси курсу

Інформація про курс розміщена на сайті Університету (<http://metod.kart.edu.ua/>), включаючи навчальний план, матеріали, завдання та правила оцінювання курсу).

Додатковий матеріал та посилання на електронні ресурси доступні на сайті Університету у розділі «дистанційне навчання» поряд із питаннями, над якими необхідно поміркувати під час підготовки для обговорення на заняттях. Необхідна підготовка повинна бути завершена до початку наступного заняття. Під час обговорення ми запропонуємо Вам критично поміркувати над тим, як відбуваються процеси безпеки телекомунікаційних систем та мереж. Ви повинні бути готовими до дискусій та мозкових штурмів – ми хочемо знати, що Ви думаєте!

## Приклади питань для обговорення на заняттях:

- 1) Що таке ARP-SPOOFING атака?
- 2) Назвіть засоби перегляду мережевого трафіку.
- 3) На основі яких стандартів відбувається оцінка критичності інформаційних ресурсів телекомунікаційної мережі?

## Опис навчальної дисципліни

Кількість кредитів – 6.

Загальна кількість годин вивчення дисципліни – 180.

Кількість годин відведена на проведення лекцій – 30.

Кількість годин відведена на проведення практичних занять – 30.

Кількість годин відведена на самостійну роботу – 120.

Рік та курс навчання – 2023/2024 рік, 1 курс.

Термін викладання – II семестр.

## Теми курсу

Тема 1. Основні поняття та визначення інформаційної безпеки. Структура інформаційної безпеки.

Тема 2. Загальні положення щодо захисту від несанкціонованого доступу.

Тема 3. Класифікація загроз інформації. Несанкціонований доступ до комп'ютерних систем.

Тема 4. Оцінка вразливостей інформаційних ресурсів. Окремі моделі загрози та порушника.

Тема 5. Класифікація типових віддалених атак.

Тема 6. Загрози інформації стека TCP IP. Комп'ютерні віруси.

Тема 7. Класифікація каналів витоку інформації.

Тема 8. Методи та засоби захисту від витоку інформації.

## Практичні заняття

Оцінка критичності інформаційних ресурсів на основі вимог стандарту NIST SP 800-60.

Дослідження функціональних можливостей програмного забезпечення Wireshark.

Програмне логування мережевих пакетів в файл.

Дослідження функціональних можливостей програмного забезпечення Wireshark.

Використання Wireshark для перегляду мережного трафіку.

Дослідження функціональних можливостей програмного забезпечення Wireshark.

Використання Wireshark для дослідження кадрів Ethernet.

Дослідження динамічного управління ризиками.

Програмна реалізація виявлення заданої мережевої атаки, автоматичне реагування і логування підозрілої активності.

Оцінка ефективності систем захисту інформації.

Виявлення ARP-SPOOFING атаки.

## Вимоги викладача

Система вимог та правил поведінки студентів на заняттях, рекомендації щодо виконання контрольних заходів, присутність на заняттях та академічна активність, що

гарантують високу ефективність навчального процесу і є обов'язковою для студента, визначаються Положенням про організацію освітнього процесу в УкрДУЗТ.

Зокрема студенти повинні виконувати вимоги з охорони праці, техніки безпеки, виробничої санітарії, протипожежної безпеки, передбачені відповідними правилами та інструкціями; самостійно виконувати навчальні завдання, завдання поточного та підсумкового контролю результатів навчання; відвідувати заняття відповідно до розкладу занять або індивідуального графіку.

### **Правила оцінювання**

Контроль знань у рамках навчальної дисципліни здійснюється з урахуванням кредитно-модульної системи відповідно до Положення про контроль та оцінювання якості знань студентів в УкрДУЗТ.

Методи контролю: поточний контроль знань здійснюється під час проведення практичних та лабораторних занять шляхом опитування; модульний контроль здійснюється шляхом виконання контрольних завдань (тестів); підсумковий контроль знань здійснюється шляхом обчислення середньоарифметичної суми балів двох модульних оцінок за 100-бальною шкалою (без складання екзамену) або проведення екзамену шляхом комп'ютерного тестування або відповідей на питання екзаменаційних білетів; захист курсової роботи здійснюється перед комісією у складі науково-педагогічних працівників кафедри шляхом опитування.

Принцип формування оцінки за модуль у складі залікових кредитів I і II за 100-бальною шкалою показано у таблиці, де наведена максимальна кількість балів, яку може набрати студент за різними видами навчального навантаження.

<b>Максимальна кількість балів за модуль</b>		
<b>Поточний контроль</b>	<b>Модульний контроль (Тести)</b>	<b>Сума балів за модуль</b>
До 60	До 40	До 100
<b>Поточний контроль</b>		<b>I семестр</b>
Відвідування занять. Активність на заняттях (Лекціях, практичних, лабораторних).		10
Здача в строк практичних робіт		50
Підсумок		60
<b>Поточний контроль</b>		<b>2 семестр</b>
Відвідування занять. Активність на заняттях (Лекціях, практичних, лабораторних).		10
Здача в строк практичних робіт		50
Підсумок		60

При заповненні заліково-екзаменаційної відомості та залікової книжки (індивідуального навчального плану) студента, оцінка, виставлена за 100-бальною шкалою, переводиться до державної шкали (5, 4, 3) та шкали ECTS (A, B, C, D, E).

Визначення назви за державною шкалою(оцінка)	Визначення назви за шкалою ECTS	За 100 бальною шкалою	ECTS оцінка
<b>ВІДМІННО – 5</b>	<b>Відмінно</b> – відмінне виконання лише з незначною кількістю помилок	90-100	A
<b>ДОБРЕ – 4</b>	<b>Дуже добре</b> – вище середнього рівня з кількома помилками	82-89	B
	<b>Добре</b> – в загальному правильна робота з певною кількістю грубих помилок	75-81	C
<b>ЗАДОВІЛЬНО - 3</b>	<b>Задовільно</b> - непогано, але зі значною кількістю недоліків	69-74	D
	<b>Достатньо</b> – виконання задовольняє мінімальні критерії	60-68	E
<b>НЕЗАДОВІЛЬНО - 2</b>	<b>Незадовільно</b> – потрібно попрацювати перед тим як отримати залік або екзамен (без повторного вивчення модуля)	35-59	FX
	<b>Незадовільно</b> - необхідна серйозна подальша робота (повторне вивчення модуля)	<35	F

### Результати навчання

РН 1. Вирішувати задачі зі створення, експлуатації, технічного обслуговування об'єктів телекомунікаційної інфраструктури з дотриманням технічних вимог, у тому числі залізничного транспорту.

РН 4. Розробляти та оптимізувати складові об'єктів телекомунікаційної інфраструктури, у тому числі з урахуванням особливостей технологічних процесів на залізничному транспорті.

РН 5. Вільно презентувати та обговорювати наявні результати у галузі телекомунікацій та радіотехніки державною та іноземною мовою, передавати свої знання, рішення і підґрунтя їх прийняття, підсумки виконаної роботи фахівцям і неспеціалістам в ясній і однозначній формі.

РН 7. Розробляти та пропонувати нові технічні рішення та застосовувати нові технології при реалізації телекомунікаційної інфраструктури, у тому числі в умовах залізничного транспорту.

РН 8. Вміти застосовувати у професійній діяльності універсальне і спеціалізоване програмне забезпечення, засоби сучасних телекомунікацій та радіотехніки.

### Команда викладачів:

Індик Сергій Володимирович (<https://kart.edu.ua/staff/indyk-sv>) –лектор в УкрДУЗТ. Отримав ступінь к.т.н. за спеціальністю 05.12.02 телекомунікаційні системи та мережі в УкрДУЗТ в 2021 році. Напрямки наукової діяльності: обробка інформації у телекомунікаційних системах та мережах.

## Кодекс академічної доброчесності

Порушення Кодексу академічної доброчесності Українського державного університету залізничного транспорту є серйозним порушенням, навіть якщо воно є ненавмисним. Кодекс доступний за посиланням:

<http://kart.edu.ua/documentu-zvo-ua>

Зокрема, дотримання Кодексу академічної доброчесності УкрДУЗТ означає, що вся робота на іспитах та заліках має виконуватися індивідуально. Під час виконання самостійної роботи студенти можуть консультуватися з викладачами та з іншими студентами, але повинні самостійно розв'язувати завдання, керуючись власними знаннями, уміннями та навичками. Посилання на всі ресурси та джерела (наприклад, у звітах, самостійних роботах чи презентаціях) повинні бути чітко визначені та оформлені належним чином. У разі спільної роботи з іншими студентами над виконанням індивідуальних завдань, ви повинні зазначити ступінь їх залученості до роботи.

## Інтеграція студентів із обмеженими можливостями

Вища освіта є провідним чинником підвищення соціального статусу, досягнення духовної, матеріальної незалежності і соціалізації молоді з обмеженими функціональними можливостями й відображає стан розвитку демократичних процесів і гуманізації суспільства.

Для інтеграції студентів із обмеженими можливостями в освітній процес Українського державного університету залізничного транспорту створена система дистанційного навчання на основі сучасних педагогічних, інформаційних, телекомунікаційних технологій.

Доступ до матеріалів дистанційного навчання з цього курсу можна знайти за посиланням: <http://do.kart.edu.ua/>

## Інформаційні матеріали

1. Лістровий С.В. Інформаційно-управляючі системи та організації паралельних обчислень / С. В. Лістровий, О. С. Лістрова, М. А. Мірошник; за ред. С. В. Лістрового. Х. : УкрДУЗТ ; Діса плюс, 2015.

2. Кавун С. В. Інформаційна безпека. Навчальний посібник / С. В. Кавун, В. В. Носов, О. В. Манжай. - Харків: Вид. ХНЕУ, 2008. - 352 с.

3. Бурячок В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. - К.: ДУТ, 2015. - 288 с.

4. <http://metod.kart.edu.ua/>

5. <http://www.e-helper.com.ua/node/120>

6. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.

7. НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.

8. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.

9. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.

10. НД ТЗІ 2.7-009-09 Методичні вказівки з оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу.

11. НД ТЗІ 2.7-010-09 Методичні вказівки з оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації від несанкційованого доступу.

12. ISO/IEC 27001:2005 Information technology — Security techniques — Information security management systems — Requirements.

13. ISO/IEC 27002:2007 Information technology — Security techniques — Code of practice for information security management.

14. ISO/IEC 27005:2008 Technologies de l'information — Techniques de sécurité – Gestion du risque en sécurité de l'information.

15. В.В. Домарев, Д.В. Домарев. Управління інформаційною безпекою в банківських установах (Теорія і практика впровадження стандартів серії ISO 27k), Донецьк: Велстар, 2012. – 146 с.