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

Кафедра інформаційних технологій в телекомунікаціях

Захист інформації у телекомунікаційних системах

Робоча програма навчальної дисципліни (Силабус)

Реквізити навчальної дисципліни	
Рівень вищої освіти	**Перший (бакалаврський)**
Галузь знань	17 Електроніка та телекомунікації
Спеціальність	172 Телекомунікації та радіотехніка
Освітня програма	Інформаційно-комунікаційні технології
Статус дисципліни	вибіркова
Форма навчання	очна(денна)/заочна
Рік підготовки, семестр	рік третій, весняний семестр
Обсяг дисципліни	4 кредити ЄКТС, з них лекції 36 годин, практичні заняття 36 годин
Семестровий контроль/ контрольні заходи	Модульна контрольна робота залік
Розклад занять	Згідно з розкладом
Мова викладання	Українська
Інформація про керівника курсу / викладачів	Лектор: к.т.н., доцент, Астраханцев А.А., 063-707-78-63, andrii.astrakhantsev@nure.ua Практичні / Семінарські: к.т.н., доцент, Астраханцев А.А Лабораторні: к.т.н., доцент, Астраханцев А.А
Розміщення курсу	

Програма навчальної дисципліни

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

Сучасна телекомунікаційна сфера людської діяльності, що спрямована на обмін інформаційними повідомленнями, потребує захисту та збереження конфіденційності цієї інформації. Тому ця дисципліна, розглядає існуючі сучасні методи та засоби забезпечення цілісності, конфіденційності й доступності інформаційного обміну в телекомунікаційних системах, і є практичною основою сукупності знань і вмінь, що суттєво розширюють і доповнюють телекомунікаційний профіль фахівця в області систем та мереж зв'язку.

Цілі дисципліни	Метою навчальної дисципліни є: - підготовка фахівця, який має базові компетенції, що засновані на системи знань в області апаратних та програмних засобів захисту інформації в телекомунікаційних системах; - формування та розвиток загальних і професійних компетентностей з впровадження та застосування технологій телекомунікацій і радіотехніки, що сприяють соціальній стійкості та мобільності випускника на ринку праці; - формування у здобувачів освіти логічного мислення, розвиток їх інтелекту та здібностей; - формування знань, вмінь і навичок, необхідних для розуміння сучасних концепцій, методів та технологій захисту даних, які циркулюють в існуючих телекомунікаційних системах та мережах.
Предмет навчальної дисципліни	Предметом вивчення навчальної дисципліни є: 1. Загальні принципи побудови апаратних та програмних засобів захисту інформації. 2. Концептуальні та нормативно-правові засади забезпечення захисту інформації в Україні. 3. Практичні навички, уміння дослідження і виявлення технічних каналів витоку інформації. 4. Основні загрози та методи протидії їм у телефонних та компьютерних мережах. 5. Методи захисту інформації у мобільних мережах 4-го та 5-го поколінь.
Компетентності **(ЗК1, ЗК7, ЗК8, ФК2, ФК5, ФК15, ФК18)**	Здатність до абстрактного мислення, аналізу та синтезу (ЗК1); Здатність вчитися і оволодівати сучасними знаннями (ЗК7); Вміння виявляти, ставити та вирішувати проблеми (ЗК8); Здатність вирішувати стандартні завдання професійної діяльності на основі інформаційної та бібліографічної культури із застосуванням інформаційно-комунікаційних технологій і з урахуванням основних вимог інформаційної безпеки (ФК2); Здатність використовувати нормативну та правову документацію, що стосується інформаційно-телекомунікаційних мереж, телекомунікаційних та радіотехнічних систем (закони України, технічні регламенти, міжнародні та національні стандарти, рекомендації Міжнародного союзу електрозв'язку і т.п.) для вирішення професійних завдань (ФК5); Здатність проводити розрахунки у процесі проектування пристроїв і засобів інформаційно-телекомунікаційних мереж, телекомунікаційних та радіотехнічних систем відповідно до технічного завдання з використанням як стандартних, так і самостійно створених методів, прийомів і програмних засобів автоматизації проектування (ФК15); Здатність розробляти на базі сучасних телекомунікаційних технологій відповідні програмно-апаратні платформи для безпроводових і мобільних мереж інфокомунікацій, здійснювати їх інтеграцію з іншими інфокомунікаційними мережами, зокрема мережами мобільного зв’язку 4-го і 5-го покоління (ФК18).

Програмні результати навчання **(ПРН1, ПРН2, ПРН6, ПРН9, ПРН15, ПРН18, ПРН21, ПРН25)**	Аналізувати, аргументувати, приймати рішення при розв'язанні спеціалізованих задач та практичних проблем телекомунікацій та радіотехніки, які характеризуються комплексністю та неповною визначеністю умов (ПРН 1); Застосовувати результати особистого пошуку та аналізу інформації для розв'язання якісних і кількісних задач подібного характеру в інформаційно-комунікаційних мережах, телекомунікаційних і радіотехнічних системах (ПРН 2); Адаптуватись в умовах зміни технологій інформаційно-комунікаційних мереж, телекомунікаційних та радіотехнічних систем (ПРН 6); Спілкуватись з професійних питань, включаючи усну та письмову комунікацію державною мовою та однією з поширених європейських мов (ПРН 9); Розуміння та дотримання вітчизняних і міжнародних нормативних документів з питань розроблення, впровадження та технічної експлуатації інформаційно-телекомунікаційних мереж, телекомунікаційних і радіотехнічних систем (ПРН 15); Здійснювати обґрунтований вибір обладнання при проектуванні системи захисту інформації та перевіряти на відповідність нормативно-правовим документам структуру системи захисту інформації банківських установ (ПРН 18); Забезпечувати надійну та якісну роботу інформаційно-комунікаційних мереж, телекомунікаційних та радіотехнічних систем (ПРН 21); Вільно орієнтуватися в системі правового забезпечення телекомунікацій, використовувати знання законодавчих та нормативних актів для організації діяльності в галузі телекомунікацій і радіотехніки, вміти бачити перспективи розвитку правового регулювання в галузі телекомунікаційних технологій (ПРН 25);

Завданнями вивчення навчальної дисципліни є:

- оволодіння методами аналізу функціонування телекомунікаційних систем, як об'єктів захисту інформації;
- набуття навичок в оцінюванні загроз витоку інформації в телекомунікаційних системах;
- дослідження сучасних пристроїв перехоплення інформації;
- оволодіння методами аналізу та застосування засобів захисту інформації;
- оволодіння навичками використання криптографічних перетворень для захисту мовних сигналів.

У результаті вивчення даної навчальної дисципліни студент повинен:

знати:

- основні канали витоку інформації в телекомунікаційних системах;
- характеристики, принципи побудови і функціонування пристрої перехоплення інформації;
- основи криптографії та шифрування;
- методи закриття мовних повідомлень,

вміти:

- застосовувати одержані з дисципліни знання на практиці;
- самостійно аналізувати телекомунікаційні системи та визначати канали витоку інформації в них;
- самостійно здійснювати аналіз пристроїв перехоплення інформації та її захисту;
- самостійно проводити обґрунтування вибору пристроїв закриття мовних повідомлень.

2. Пререквізити та постреквізити дисципліни

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 базуючись на знаннях таких дисциплін: • вища математика • основи теорії імовірностей, • основи інформаційно-комунікаційних технологій, • сигнали та процеси в телекомунікаційних системах, • теорія передачі інформації та кодування.	• Наукова робота за темою бакалаврської дисертації • Практика

3. Зміст навчальної дисципліни

Тема 1. Концептуальні засади забезпечення інформаційної безпеки України. Нормативно-правові основи захисту інформації в Україні. Концепція інформаційної безпеки України. Основні поняття захисту інформації: конфіденційність, цілісність, доступність, авторизація та способи їх забезпечення.

Тема 2. Технічні канали витоку інформації. Місце технічного захисту інформації у системі інформаційної безпеки. Сутність та завдання технічного захисту інформації. Основні поняття, терміни та визначення технічного захисту інформації. Види інформації, яка може стати об'єктом злочинних посягань. Типи каналів витоку інформації. Основні засоби/способи отримання інформації та засоби протидії ним. Засоби захисту приміщень. Акустичні засоби захисту. Пристрої виявлення небезпечних випромінювань. Функції індикаторів поля та скануючих приймачів. Багатофункціональні пошукові системи. Пристрої виявлення та придушення диктофонів.

Тема 3. Захист телефонних мереж загального кристування. Аналізатори телефонних ліній. Методи виявлення підключень до телефонних ліній. Методи та засоби захисту телефонних ліній. Методи підключення до оптичних каналів зв'язку та методи їх виявлення. Аналогові скремблери. Пристрої з частотною та часовою інверсією. Комбіновані скремблери. Дискретизація мови з подальшим шифруванням.

Тема 4. Захист інформації в компьютерних мережах. Протоколи захисту інформації : L2TP, IPSec, SSL/TLS та інші. Програмно-технічні засоби захисту: файрволи, міжмережні екрани, фільтруючі маршрутизатори, проксі-системи. Проектування комплексної системи захисту інформації. Забезпечення антивірусного захисту.

Тема 5. Захист інформації в мобільних мережах. Способи забезпечення захищеності в мережах 2G/3G/4G/5G. Способи забезпечення захисту на пристроях користувачів. Основи біометричної автентифікації.

4. Навчальні матеріали та ресурси

4.1. Базова література

1. Кузнецов О. О. Захист інформації в інформаційних системах. Методи традиційної криптографії / О.О. Кузнецов, С.П. Євсеєв, О.Г. Король. – Х.: Вид. ХНЕУ, 2011. – 510 с.
2. Юдін О.К., Корченко О.К., Конахович Г.Ф. Захист інформації в мережах передачі даних : Підручник. — К.: «НВП ІТЕРСЕРВІС», 2009. – 716 с.
3. Остапов С.Е., Євсеєв С.П. , Король О.Г. Технології захисту інформації : Навчальний посібник. – Л.: Новий світ-2000, 2021. – 678 с.
4. Захист інформації в комп'ютерних системах : підручник / уклад. О. М. Гапак, С. І. Балога; рец. : М. І. Глебена. – Ужгород : ПП "АУТДОР-ШАРК, 2021. – 184 с.
5. Ю.А.Тарнавський. Технології захисту інформації. К.: КПІ ім. Ігоря Сікорського, 2018. – 162 с.

4.2. Додаткова література

1. ДСТУ 7624:2014. Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення. – Чинний з 29.12.2014 р. ПАТ «Інститут інформаційних технологій» Мінекономрозвитку України, 2016. – 228 с..
2. ДСТУ 4145-2002. Інформаційні технології. Криптографічний захист інформації. Електронний цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння. К. : Держстандарт України, 2003.
3. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. – Чинний з 28.04.1999. – К.: ДСТСЗІ СБ України, 1999. – 14 с.
4. Інформаційна безпека: навч. посіб. / С. В. Кавун, В. В. Носов, О. В. Манжай. Харків: Вид. ХНЕУ, 2008. – 352 с
5. Хорошко В.О. Основи інформаційної безпеки: підручник /В.О. Хорошко, В.С. Чередниченко, М.Є. Шелест; за ред.В.О. Хорошка. – К.: ДУІКТ, 2008. – 186 с.
6. Effective Cybersecurity: A Guide to Using Best Practices and Standards. / W. Stallings; Addison-Wesley Professional; 1st edition (2018). – 800 p.

Навчальний контент

5. Методика опанування навчальної дисципліни (освітнього компонента)

5.1 Лекційні заняття – 36 годин

Тема 1. Концептуальні засади забезпечення інформаційної безпеки України.
Лекція 1. Нормативно-правові основи захисту інформації в Україні. Концепція інформаційної безпеки України.
Лекція 2. Основні поняття захисту інформації: конфіденційність, цілісність, доступність, авторизація та способи їх забезпечення.

Тема 2. Технічні канали витоку інформації.
Лекція 3. Місце технічного захисту інформації у системі інформаційної безпеки. Сутність та завдання технічного захисту інформації. Основні поняття, терміни та визначення технічного захисту інформації. Види інформації, яка може стати об'єктом злочинних посягань.
Лекція 4. Типи каналів витоку інформації. Основні засоби/способи отримання інформації та засоби протидії ним. Засоби захисту приміщень.
Лекція 5. Акустичні засоби захисту. Пристрої виявлення небезпечних випромінювань. Функції індикаторів поля та скануючих приймачів. Багатофункціональні пошукові системи. Пристрої виявлення та придушення диктофонів.

Тема 3. Захист телефонних мереж загального кристування

Лекція 6. Аналізатори телефонних ліній. Методи виявлення підключень до телефонних ліній. Методи та засоби захисту телефонних ліній. Методи підключення до оптичних каналів зв'язку та методи їх виявлення.
Лекція 7. Аналогові скремблери. Пристрої з частотною та часовою інверсією. Комбіновані скремблери. Дискретизація мови з подальшим шифруванням.

Тема 4. Захист інформації в компьютерних мережах.
Лекція 8,9. Протоколи захисту інформації : L2TP, IPSec, SSL/TLS.
Лекція 10. Програмно-технічні засоби захисту: файрволи, міжмережні екрани, фільтруючі маршрутизатори, проксі-системи.
Лекція 11. Проектування комплексної системи захисту інформації. Забезпечення антивірусного захисту.

Тема 5. Захист інформації в мобільних мережах
Лекція 12,13,14. Способи забезпечення захищеності в мережах 2G/3G/4G/5G.
Лекція 15,16. Способи забезпечення захисту на пристроях користувачів. Пін-коди, скрін-локери.
Лекція 17,18. Основи біометричної автентифікації.

5.2 Практичні заняття – 18 годин

Основні завдання циклу практичних та лабораторних занять:

- вивчення способів несанкціонованого отримання інформації в інформаційно-телекомунікаційних системах та методів протидії;
- вивчення методів захисту інформації в мобільних, компьютерних мережах та мережах передачі даних.

Тема 1. Концептуальні засади забезпечення інформаційної безпеки України.
Практичне заняття 1. Аналіз методів забезпечення цілісності, конфіденційності, доступності та вторизації

Тема 2. Технічні канали витоку інформації.
Практичне заняття 2. Аналіз ефективності зняття інформації з різних типів кабелів.
Практичне заняття 3. Розрахунок рівня сигналу в технічним каналах витоку.

Тема 4. Захист інформації в компьютерних мережах
Практичне заняття 4. Методи формування цифрового підпису
Практичне заняття 5. Методи формування геш-функції
Практичне заняття 6. Методи прихованої передачі інформації в компьютерних мережах. Основи стеганографії.

Тема 5. Захист інформації в мобільних мережах.
Практичне заняття 7. Захист мовної інформації в GSM. Лінійні рекурентні регістри (LFSR).
Практичне заняття 8. Аналіз стійкості алгоритмів захисту інформації у мобільних мережах.
Практичне заняття 9. Розрахунок параметрів біометричної автентифікації.

5.3 Лабораторні заняття – 27 годин

Тема 1. Концептуальні засади забезпечення інформаційної безпеки України.
Лабораторне заняття 1 (4 год). Правове забезпечення безпеки телекомунікаційних систем.
Лабораторне заняття 2 (4 год). Застосування нормативно-правової бази при організації захисту інформації у фінансових установах

Тема 2. Технічні канали витоку інформації.
Лабораторне заняття 3 (4 год). Забезпечення захисту зовнішнього периметру за допомогою датчиків.

Тема 3. Захист телефонних мереж загального кристування
Лабораторне заняття 4 (4 год). Системи закриття мови в каналах зв'язку. Скремблери.

Тема 4. Захист інформації в компьютерних мережах
Лабораторне заняття 5 (4 год). Побудова захищеної комп'ютерної мережі за допомогою IPSec.
Лабораторне заняття 6 (4 год). Шифрування данних з використанням OpenSSL
Лабораторне заняття 7 (3 год). Тестування захищеності транспортного рівня за допомогою OpenSSL.

6. Самостійна робота студента

Самостійна робота є важливою складовою вивчення дисципліни та спрямована на вивчення основних понять дисципліни «Захист інформації в телекомунікаційних системах».

Самостійна робота включає:

- підготовку до аудиторних занять;
- пошук (підбір) і вивчення літератури та електронних джерел інформації за заданою проблемою дисципліни;
- самостійну роботу за окремими темами навчальної дисципліни;
- домашнє завдання, що передбачає вивчення тих чи інших розділів дисципліни;
- підготовка до заліку.

Види самостійної роботи:

- самостійна робота студента з викладачем включає в себе індивідуальні консультації протягом семестру та складання контрольних заходів;
- самостійна робота студента в складі групи включає в себе консультації перед заліком;
- самостійна робота студента без викладача.

Під час самостійного вивчення теоретичного курсу студентам необхідно:

- самостійно вивчати теми теоретичного курсу відповідно до програми дисципліни;
- проробити та підготувати відповіді на запитання, що наведені після кожної теми.

Самостійну роботу виконують студенту на підставі навчально-методичних матеріалів дисципліни. Самостійна робота студента оцінюється викладачем за результатами:

- опитувань:
- виконання лабораторних робіт;
- виконання практичних занять;
- відповідей під час проведення іспиту.

Політика та контроль

7. Політика навчальної дисципліни (освітнього компонента)

1. Лекційні заняття

Ваговий бал – 1:

– бал за присутність на лекції та написання конспекту – 1.35;

За семестр проводиться 18 лекційних занять, кожен студент має можливість бути присутнім на кожному з занять

Максимальна кількість балів: 18 ×1.35 = 24

2. Практичні роботи

Ваговий бал – 4:

– бал за повну відповідь на запитання – 2,5…4;
– бал за часткову відповідь на запитання – 1...2;
– бал за невірну відповідь або відмову відповідати – 0.

Максимальна кількість балів: 4 × 9 = 36.

3. Лабораторні роботи

Ваговий бал – 5:

– бал за одну повну вірно виконану лабораторну роботу зі звітом–5;
– бал за не здану лабораторну роботу – 0;
За здану лабораторну без звіту – 1 штрафний бал;
Максимальна кількість балів: 5 × 4 = 20.

4. Модульна контрольна робота

1 модульна контрольна робота, за яку можна отримати до 20 балів
1 домашня контрольна робота, за яку можна отримати до 9 балів

5. Критерії екзаменаційного оцінювання

1. Повні відповіді на теоретичні запитання та вірний розв'язок задачі – 40;
2. Повні відповіді на теоретичні запитання, задача розв'язана невірно – 35;
3. Часткові відповіді на теоретичні запитання при розв'язаній задачі – 25;
4. Відсутня відповідь на одне з теоретичних питань – 10;
5. Відсутні відповіді – 0.

Заохочувальні бали:

– за участь у факультетській олімпіаді з дисципліни, модернізації лабораторних робіт, виконання завдань із удосконалення дидактичних матеріалів з дисципліни надається + 0 ... + 3 (заохочувальних) балів.

Студенти, які набрали протягом семестру рейтинг з кредитного модуля менше 0,5*R,* зобов'язані виконувати контрольну роботу.

Студенти, які набрали протягом семестру необхідну кількість балів (*RD* < 0,4R) мають можливість:

Отримати підсумкову оцінку так званим «автоматом» відповідно до набраного рейтингу;

Виконувати підсумкову контрольну роботу з метою підвищення оцінки;

У разі отримання оцінки, більшої ніж «автомат» з рейтингу, студент отримує оцінку за результатами підсумкової контрольної роботи;

Підвищувати оцінку шляхом написання письмового іспиту.

8. Політика університету

8.1. 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

8.2. 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

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

Поточний контроль: опитування за темою заняття, МКР
Календарний контроль: провадиться двічі на семестр як моніторинг поточного стану виконання вимог силабусу.
Семестровий контроль: залік
Умови допуску до семестрового контролю: семестровий рейтинг більше 50 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

10.Додаткова інформація з дисципліни (освітнього компонента)

10.1 Інформаційні ресурси

1. ЗАКОН УКРАЇНИ Про національну безпеку України (Відомості Верховної Ради (ВВР), 2018, № 31, ст.241) [Електронний ресурс] – Режим доступу: http://zakon.rada.gov.ua/laws/show/2469-19
2. ЗАКОН УКРАЇНИ про внесення змін до Закону України "Про захист інформації в автоматизованих системах" [Електронний ресурс] – Режим доступу: http://zakon.rada.gov.ua/laws/show/2594-15
3. АДМІНІСТРАЦІЯ ДЕРЖАВНОЇ СЛУЖБИ СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ [Електронний ресурс] – Режим доступу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=81998&cat_id=38835

10.2 Нормативна література

1. ДСТУ ГОСТ 28147: 2009 Система обробки інформації. Захист криптографічний. Алгоритм криптографічного перетворення (ГОСТ 28147-89) ДСТУ 2396-94 Системи оброблення інформації. Теорія інформації. Терміни та визначення
2. ДСТУ 4145-2002 "Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння";
3. ДСТУ ISO/IEC 11770-3:2002 "Інформаційні технології. Методи захисту. Управління ключовими даними. Частина 3. Протоколи, що ґрунтуються на асиметричних криптографічних перетвореннях";
4. ДСТУ ISO/IEC 15946-3:2002 "Інформаційні технології. Методи захисту. Криптографічні методи, що ґрунтуються на еліптичних кривих. Частина 3. Установлення ключів";

5. ДСТУ ГОСТ 28147-2009 “Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования”;
6. ДСТУ ISO/IEC 10118-3:2005 “Інформаційні технології. Методи захисту. Гешфункції. Частина 3. Спеціалізовані геш-функції”.
7. ДСТУ 2481-94 Системи оброблення інформації. Інтелектуальні інформаційні технології. Терміни та визначення
8. ДСТУ 2505-94 Системи оброблення інформації. Організація даних. Терміни та визначення.

Робочу програму навчальної дисципліни (силабус):

Складено доцент, к.т.н., доцент, Астраханцев А.А.

Ухвалено кафедрою ІТТ (протокол № 13 від 24.05.2024)

Погоджено Методичною комісією НН ІТС (протокол № 4 від 13.06.2024)