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

Кафедра інформаційних технологій в телекомунікаціях

Основи криптографічного захисту інформації

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 18 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

Значна увага приділяється вивченню математичної основам теорії множин, теорії кілець та полів Галуа, теорії ймовірностей, теорії статистики та теорії перетворень у підгрупі точок еліптичних кривих. Вивчається математичний апарат який використовується під час побудови сучасних алгоритмів та протоколів шифрування, перевірки цілісності та автентифікації, а також вивченні їх ефективності та спеціальних властивостей.

Цілі дисципліни	Метою навчальної дисципліни є: - підготовка фахівця, який має базові компетенції, що засновані на знаннях математичного апарату, який використовується для розробки криптографічних методів та засобів захисту інформації; - 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 математичного апарату криптографічних систем захисту даних в телекомунікаційних системах та мережах.
Предмет навчальної дисципліни	Предметом вивчення навчальної дисципліни є: 1. Практичні навички із застосування математичного апарату для реалізації та обслуговування сучасних систем захисту інформації в телекомунікаційних системах. 2. Загальні принципи побудови прикладних методів криптографічного захисту інформації. 3. Основні шляхи забезпечення цілісності, конфіденційності, доступності інформації в телекомунікаційних мережах. 4. Методи гешування даних та електронного цифрового підпису.
Компетентності	Здатність до абстрактного мислення, аналізу та синтезу (ЗК1); Здатність вчитися і оволодівати сучасними знаннями (ЗК7); Вміння виявляти, ставити та вирішувати проблеми (ЗК8); Здатність розуміти сутність і значення інформації в розвитку сучасного інформаційного суспільства (ФК1); Здатність вирішувати стандартні завдання професійної діяльності на основі інформаційної культури із застосуванням інформаційно-комунікаційних технологій і з урахуванням основних вимог інформаційної безпеки (ФК2); Здатність використовувати базові методи, способи та засоби отримання, передавання, обробки та зберігання інформації (ФК3); Володіння сучасними підходами та технологіями для планування, проектування, використання та створення засобів для адміністрування інформаційно-комунікаційних мереж з використанням методів прихованої передачі інформації в телекомунікаційних мережах за рахунок вбудовування інформації в відео, аудіо, нерухомі зображення та мережеві заголовки (RTP, TCP та інші). (ФК19).
Програмні результати навчання	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); Мати навички оцінювання, інтерпретації та синтезу інформації і даних (ПРН 5); 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); Здійснювати обґрунтований вибір методу приховування в залежності від вимог замовника та реалізовувати програмно чи апаратно обрані методи приховування інформації в текстах, нерухомих зображеннях, відео- та аудіофайлах (ПРН 17); Забезпечувати надійну та якісну роботу інформаційно-комунікаційних мереж, телекомунікаційних та радіотехнічних систем (ПРН 21); Бути ознайомленими з принципами дії та можливостями сучасних технологій і систем прихованої передачі інформації та мати навички роботи з прихованими каналами передачі даних у телекомунікаційних системах та визначення методів їх виявлення (ПРН 23).

В результаті вивчення курсу студент повинен знати властивості послідовностей чисел та множин, вміти застосовувати симетричні та асиметричні шифри, використовувати модулярну арифметику, будувати прості алгоритми криптоперетворювань та гешування.

За результатом вивчання дисципліни студенти повинні:

ЗНАТИ:

– історію криптології;
– основні методи, які використовуються криптологією;
– властивості спеціальних послідовностей чисел;
– основні поняття теорії груп, кілець, полів та поліномів;
– основні поняття теорії ймовірностей;
– способи подання інформації в криптосистемах;
– основні симетричні криптоалгоритми;
– основні асиметричні криптоалгоритми;
– способи застосування алгоритмів шифрування.

ВМІТИ:

– класифікувати криптосистеми на основі декількох критеріїв;
– використовувати основні алгебраїчні структури для побудови криптоперетворювань;
– аналізувати обчислювальну складність алгоритмів криптоперетворювань;
– будувати генератори псевдовипадкових послідовностей чисел;
– розраховувати симетричні криптосистеми та криптосистеми, що побудовані на основі проблеми дискретного логарифмування.

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, • дискретна математика	• захист інформації в телекомунікаційних системах, • технології обслуговування телекомунікаційних систем

3. Зміст навчальної дисципліни

Змістовий модуль 1. Історичні шифри. Основи математичного апарату.

Тема 1. Основні терміни та визначення. Історичні шифри.

Предмет, ціль і задачі курсу. Історія криптології. Основні методи криптології. Традиційні криптосистеми. Поняття криптоаналізу.

Тема 2. Основи теорії множин. Основи теорії чисел.

Поняття множини. Задання належності до множини. Юніверсум та пуста множина. Перетин, об'єднання, різниця, симетрична різниця, доповнення множин. Поняття булеану. Декартов добуток множин. Поняття відображення. Група, моноїд, кільце, поле та їх властивості.

Тема 3. Подання інформації в криптографічних системах.

Системи числення. Подання чисел у різних системах числення. Формування чисел довільної довжини на основі бітів, байтів, слів та масивів слів. Поняття кодування. Кодові таблиці в інформаційних системах. Стандарти ASCII та UNICODE.

Змістовий модуль 2. Модулярна арифметика. Основні перетворення в криптології.

Тема 1. Модулярна арифметика.

Віднімання за модулем. Порівняння. Рішення Діофантових рівнянь. Теореми Ейлера та Ферма. Властивості ступеневих порівнянь. Квадратичні віднімання.

Тема 2. Основи теорії інформації і кодування джерела.

Поняття події, імовірності події та ансамблю. Неможливі та несумісні події. Підрахування імовірностей. Основні теореми теорії імовірностей. Формула повної імовірності. Предмет та завдання теорії інформації. Поняття ентропії системи. Джерело дискретних повідомлень. Ентропія складної системи. Умовна ентропія та об'єднання залежних систем. Визначення інформації через ентропію. Характеристики стисненої інформації. Стійкість криптосистем.

Тема 3. Математичні перетворення в симетричних шифрах.

Приклади математичних перетворень у симетричних шифрах. Мережа Фейстеля. Режими роботи симетричних шифрів. Криптоперетворення в алгоритмах DES та AES. Шифрування даних – блочні шифри. Забезпечення шифрування під час дзвінка або розмови – поточні шифри.

Тема 4. Математичні перетворення в асиметричних шифрах.

Математичні перетворення у асиметричних криптосистемах. Криптосистеми RSA, El-Gamal, DH. Основні математичні перетворення в криптосистемах на еліптичних кривих. Застосування асиметричної криптографії для взаємної автентифікації користувачів.

Тема 5. Математичні перетворення над криптографічними примитивами.

Математичні перетворення під час створення електронного цифрового підпису. Математичні перетворення при формуванні Геш-функції. Методи генерації псевдовипадкових послідовностей. Послідовності чисел. Лінійні конгруентні генератори. Лінійні рекурентні генератори.

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. 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.
4. Effective Cybersecurity: A Guide to Using Best Practices and Standards. / W. Stallings; Addison-Wesley Professional; 1st edition (2018). – 800 p.
5. Остапов С.Е., Євсеєв С.П. , Король О.Г. Технології захисту інформації : Навчальний посібник. – Л.: Новий світ-2000, 2021. – 678 с.

6. Wenbo Mao. Modern Cryptography: Theory and Practice – Williams, 2005. – 768 p.
7. Schnaier B. Fergusson N. Practical Cryptography: Designing and Implementing Secure Cryptographic Systems, 2004. – 432 p.

Навчальний контент

5. Методика опанування навчальної дисципліни (освітнього компонента)

5.1 Лекційні заняття – 36 годин

Змістовий модуль 1. Історичні шифри. Основи математичного апарату.

Тема 1. Основні терміни та визначення. Історичні шифри.

Лекція 1,2. Предмет, ціль і задачі курсу. Історія криптології. Основні методи криптології. Традиційні криптосистеми. Поняття криптоаналізу.

Лекція 3. Історичні шифри. Етапи розвитку методів шифрування. Шифри підстановки та перестановки.

Тема 2. Основи теорії множин та теорії чисел

Лекція 4. Поняття множини. Задання належності до множини. Юніверсум та пуста множина. Перетин, об'єднання, різниця, симетрична різниця, доповнення множин. Поняття булеану. Декартов добуток множин. Поняття відображення.

Лекція 5. Поняття відображення. Група, моноїд, кільце, поле та їх властивості. Використання в системах захисту інформації.

Тема 3. Подання інформації в криптографічних системах

Лекція 6. Системи числення. Подання чисел у різних системах числення. Формування чисел довільної довжини на основі бітів, байтів, слів та масивів слів. Поняття кодування. Кодові таблиці в інформаційних системах. Стандарти ASCII та UNICODE.

Змістовий модуль 2. Модулярна арифметика. Основні перетворення в криптології.

Тема 1. Модулярна арифметика.

Лекція 7,8,9. Віднімання за модулем. Порівняння. Рішення Діофантових рівнянь. Теореми Ейлера та Ферма. Властивості ступеневих порівнянь. Квадратичні віднімання.

Тема 2. Основи теорії інформації і кодування джерела.

Лекція 10. Поняття події, імовірністі події та ансамблю. Неможливі та несумісні події. Підрахування імовірностей. Основні теореми теорії імовірностей. Формула повної імовірності.

Лекція 11,12. Предмет та завдання теорії інформації. Поняття ентропії системи. Джерело дискретних повідомлень. Ентропія складної системи. Умовна ентропія та об'єднання залежних систем. Визначення інформації через ентропію.

Лекція 13. Кодування джерела. Рівномірне кодування. Ентропійне кодування. Коди Хафмана та Шенона-Фано. Характеристики стисненої інформації. Стійкість криптосистем.

Тема 3. Математичні перетворення в симетричних шифрах.

Лекція 14. Приклади математичних перетворень у симетричних шифрах. Режими роботи симетричних шифрів.

Лекція 15. Криптографічні хеш-функції

Тема 4. Математичні перетворення в асиметричних шифрах.

Лекція 16,17. Математичні перетворення у асиметричних криптосистемах. Криптосистеми RSA, El-Gamal, DH. Основні математичні перетворення в криптосистемах на еліптичних кривих.

Тема 5. Математичні перетворення над криптографічними примитивами.
Лекція 18. Математичні перетворення під час створення електронного цифрового підпису. Математичні перетворення при формуванні Геш-функції. Методи генерації псевдовипадкових послідовностей. Послідовності чисел. Лінійні конгруентні генератори. Лінійні рекурентні генератори.

5.2 Практичні заняття – 18 годин

Основні завдання циклу практичних занять:

- засвоєння математичного апарату, що використовується в криптографії
- вивчення способів подання інформації в інформаційно-телекомунікаційних системах
- вивчення сучасних методів шифрування данних
- вивчення методів формування цифрового підпису та гешування данних

Змістовий модуль 1. Історичні шифри. Основи математичного апарату.
Тема 1. Основні терміни та визначення. Історичні шифри.
Практичне заняття 1. Основні методи та поняття криптології. Основні принципи та види криптоаналізу.
Практичне заняття 2. Історія розвитку шифрування

Тема 2. Основи теорії множин та чисел
Практичне заняття 3. Рішення задач теорії множин

Тема 3. Подання інформації в криптографічних системах
Практичне заняття 4. Системи числення. Подання чисел у різних системах зчислення.
Практичне заняття 5. Формування чисел довільної довжини на основі бітів, байтів, слів та масивів слів. Формування чисел збільшеної розрядності в інформаційних системах різного типу

Змістовий модуль 2. Модулярна арифметика. Основні перетворення в криптології.
Тема 1. Модулярна арифметика.
Практичне заняття 6. Віднімання за модулем. Порівняння
Практичне заняття 7. Рішення Діофантових рівнянь. Квадратичні віднімання.

Тема 3. Математичні перетворення в симетричних шифрах.
Практичне заняття 8. Приклади математичних перетворень у симетричних шифрах. Режими роботи симетричних шифрів.

Тема 4. Математичні перетворення в асиметричних шифрах.
Практичне заняття 9. Криптосистема RSA, El-Gamal, DH. Основні математичні перетворення в криптосистемах на еліптичних кривих.

6. Самостійна робота студента

Самостійна робота є важливою складовою вивчення дисципліни та спрямована на вивчення основних понять дисципліни «Математичні основи криптології».

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.

Теми, що виносяться на самостійну роботу студентів:

- основні терміни та визначення;
- історичні системи шифрування;
- атаки на традиційні шифри;
- основи теорії множин;
- основи теорії чисел;
- способи подання інформації в криптології: ASCII, UNICODE;
- основи теорії інформації в криптології: кодування джерела;
- основи математичної логіки: основні теореми;
- основні перетворення в симетричних шифрах. Режими роботи шифрів;
- методи розв’язанням Діафантових рівнянь;
- основні математичні перетворення на еліптичних кривих;
- основи побудови та характеристики шифрів на еліптичних кривих.

Політика та контроль

7. Політика навчальної дисципліни (освітнього компонента)

1. Лекційні заняття

Ваговий бал – 1:

– бал за присутність на лекції та написання конспекту – 1.5;

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

Максимальна кількість балів: 18×1.5= 27

2. Практичні заняття

За семестр проводиться 9 практичних занять. В середньому на практичних заняттях студент може відповісти 3 разів

За правильну відповідь на практичному занятті – 5 балів;

За відповідь з помилками – 1…4 балів;

За неправильну відповідь – 0 балів

За присутність на практичному занятті – 1 бал
Максимальна кількість балів: 5х9 = 45

3. Модульна контрольна робота

2 модульні контрольні роботи, за кожну МКР можна отримати до 14 балів

4. 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)

Перелік запитань до заліку:

1. Поняття криптографії, криптоаналізу та криптології. Історія криптології.
2. Традиційні системи шифрування.
3. Вимоги до сучасних шифрів.
4. Поняття криптографічного стійкості.
5. Математична логіка. Висловлювання.
6. Основні види складних висловлювань. Таблиці істинності.
7. Еквівалентні висловлювання. Конверсія, інверсія, контрапозиции, тавтологія.
8. Основні завдання теорії множин. Основні операції теорії множин.
9. Модулярна арифметика.
10. Основні алгебраїчні структури.
11. Послідовності чисел. Лінійні конгруентні генератори.
12. Завдання теорії ймовірності в криптології.
13. Поняття події, ймовірності події та ансамблю.
14. Обчислення ймовірностей. Повна група подій. Поняття статистичної ймовірності.
15. Формула повної ймовірності.
16. Предмет і завдання теорії інформації.
17. Поняття ентропії системи.
18. Ентропія складної системи. Умовна ентропія.
19. Системи числення.
20. Формування чисел довільної розрядності на основі бітів, байтів і слів.
21. Використання чисел збільшеною розрядності.
22. Математичні перетворення в симетричних шифрах
23. Мережа Фейстеля.
24. Види та основні властивості симетричних шифрів
25. Поточне та блочне шифрування. Шифрування голосу.
26. Алгоритми шифрування DES та AES
27. Режими роботи симетричних шифрів
28. Криптографічні хеш-функції. Призначення та характеристики
29. Види хеш-функцій

30. Математичні перетворення в асиметричних криптосистемах
31. Криптосистема RSA.
32. Криптосистема Діффі-Хеллмена.
33. Криптосистема Ель-Гамаля
34. Переваги та недоліки асиметричних шифрів.
35. Формування загального сеансового ключа по Діффі-Хеллмену.
38. Криптосистеми на еліптичних кривих.
39. Поняття кодування. Кодові таблиці в інформаційних системах.
40. Стандарти ASCII і UNICODE.

Робочу програму навчальної дисципліни (силабус):

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

Ухвалено засіданням кафедри ІТТ (протокол №13 від 24 травня 2024р.)

Погоджено Методичною комісією НН ІТС (протокол №4 від 13 червня 2024р.)