МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ СЕМЕНА КУЗНЕЦЯ

"ЗАТВЕРДЖУЮ"
Заступник керівника
(проректор з науково-педагогічної роботи)
М.В. Афанасьєв

МАТЕМАТИЧНІ ОСНОВИ КРИПТОЛОГІЇ

робоча програма навчальної дисципліни

Галузь знань	**12 “ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ”**
Спеціальність	**125 “КІБЕРБЕЗПЕКА”**
Освітній рівень	**перший (бакалаврський)**
Освітня програма	**”КІБЕРБЕЗПЕКА”**

Вид дисципліни	**базова**
Мова викладання, навчання та оцінювання	**українська**

Завідувач кафедри *кібербезпеки та інформаційних технологій* Євсеєв С.П.

Харків
ХНЕУ ім. С. Кузнеця
2019

ЗАТВЕРДЖЕНО
на засіданні кафедри кібербезпеки
та інформаційних технологій
Протокол № 6 від 10.12.2019 р.

Розробник(-и):
Мілов О.В., к.т.н., проф. кафедри КІТ

Лист оновлення та перезатвердження
робочої програми навчальної дисципліни

Навчальний рік	Дата засідання кафедри – розробника РПНД	Номер протоколу	Підпис завідувача кафедри

1. Вступ

Анотація навчальної дисципліни:

Дисципліна «Математичні основи криптології» забезпечує підготовку бакалаврів відповідно до вимог і навчального плану спеціальності «кібербезпека», ознайомлення студентів з математичними основами криптології, а саме – основами теорії чисел, лінійною алгеброю, основами дискретної математики, комбінаторики та ін. Дисципліна «Математичні основи криптології» розглядається як теоретична і прикладна дисципліна, що дає уявлення про основні математичні методи та підходи, що застосовуються для забезпечення криптографічного захисту інформації в процесі зберігання та передачі інформації, представленої в двійкових кодах. Дисципліна присвячена вивченню математичних основ криптології та криптографічного аналізу, що застосовуються до захисту інформації в інформаційних системах. Дисципліна розкриває поняття шифрів, симетричної та асиметричної криптографії, електронного підпису, гешування та інші математичні об'єкти криптографії. Вивчаються відповідні криптографічні стандарти, що застосовуються сьогодні в захисті інформації в Україні та за кордоном. Докладно розглядаються: стандарти RSA. DES. GOST1989. та інші. Також приділено увагу перспективним напрямам в криптології: криптографічним протоколам з розголошенням і без розголошення, теорії алгоритмічної складності і одностороннім функціям, схемам поділу секрету і деяким їх застосуванням в задачах ідентифікації і аутентифікації.

Мета навчальної дисципліни:

Метою вивчення дисципліни «Математичні основи криптології» є:

- ознайомлення з основами математичної теорії криптології:
- придбання навичок в практичному використанні, постановці і вирішенні задач шифрування інформації:
- розуміння суті інформаційних процесів в криптографічних системах;
- застосування комп'ютерів для вирішення завдань шифрування і дешифрування:
- розробка і використання математичних і обчислювальних моделей процесів шифрування інформації, їх оптимізація та вироблення напрямків вдосконалення.

Курс	**3**	
Семестр	**1**	
Кількість кредитів ECTS	**5**	
Аудиторні навчальні заняття	**лекції**	**30**
	семінарські, практичні	
	лабораторні	**30**
Самостійна робота		**90**
Форма підсумкового контролю	**залік**	

Структурно-логічна схема вивчення навчальної дисципліни:

Попередні дисципліни	Наступні дисципліни
Математичний аналіз Лінійна алгебра Математичне моделювання Теорія ризику Теорія ймовірностей і математична статистика Дискретна математика Основи теорії систем та системний аналіз; Теорія інформації та кодування Інформатика Програмування Менеджмент інформаційної безпеки	Основи криптографічного захисту Основи інформаційної безпеки Теорія прийняття рішень; Проектування захищених телекомунікаційних систем Програмно-апаратні засоби забезпечення інформаційної безпеки Системи аналізу захищеності Технічний захист інформації Забезпечення інформаційної безпеки

2. Компетентності та результати навчання за дисципліною:

Компетентності	Результати навчання
Здатністю застосовувати відповідний математичний апарат для вирішення професійних завдань	Знати: моделі шифрів і математичні методи їх дослідження Вміти: застосовувати математичні методи опису і дослідження криптографічних систем Володіти: навичками математичного моделювання в криптографії.
Здатністю здійснювати раціональний вибір засобів забезпечення інформаційної безпеки телекомунікаційних систем з урахуванням пред'явлених до них вимог якості обслуговування і якості функціонування	Знати: основні завдання та поняття криптографічних методів захисту інформації; основні криптографічні методи захисту інформації; вимоги до шифрів і основні характеристики шифрів вміти: здійснювати раціональний вибір криптографічних методів і засобів захисту інформації в телекомунікаційних системах; реалізовувати типові криптографічні перетворення; володіти: навичками використання типових криптографічних перетворень; навичками застосування інженерно-криптографічних механізмів для виявлення несправностей криптографічних засобів захисту інформації

3. Програма навчальної дисципліни

Змістовій модуль 1. Традиційне шифрування
Тема 1. Вступ.
Цілі підтримки безпеки (конфіденційність, цілісність, готовність).

Атаки. Атаки, які загрожують конфіденційності: втручання, спостереження за трафіком і його аналіз. Атаки, які загрожують цілісності: модифікація, імітація джерела, повторна передача інформації, відмова від повідомлення. Атаки, які загрожують готовності: відмова в обслуговуванні. Пасивні і активні атаки: пасивні нападу, активні атаки.

Послуги та механізми. Послуги інформаційної безпеки: конфіденційність даних, цілісність даних, встановлення дійсності (аутентифікація), виняток відмови від повідомлень, управління доступом. Механізми безпеки: шифрування, цілісність даних, цифровий підпис, обмін повідомленнями для впізнання, заповнення трафіку, управління маршрутизацією, довіреність, контроль доступу. Співвідношення між послугами та механізмами.

Методи. Криптографія: шифрування симетричними ключами, шифрування асиметричними ключами, хешування, стеганографія. Історичні приклади використання. Сучасне використання.

Тема 2. Модульна арифметика.

Арифметика цілих чисел. Множина цілих чисел: бінарні операції, розподіл цілих чисел, два обмеження, граф рівняння поділу.

Теорія подільності. Властивості. Всі подільники. Найбільший спільний дільник. Алгоритм Евкліда. Розширений алгоритм Евкліда. Лінійні діофантові рівняння. Частне рішення. Загальні рішення.

Модульна арифметика. Операції по модулю. Система відрахувань: Zn. Порівняння. Система відрахувань. Кругова система позначень. Операції в Zn. Властивості. Інверсії. Адитивна інверсія. Мультиплікативна інверсія. Додавання і множення таблиць. Різні множини для додавання і множення.

Тема 3. Матриці.

Визначення. Операції і рівняння. Рівність. Складання і віднімання. Множення. Скалярний множення. Детермінант.

Інверсії. Адитивна інверсія. Мультиплікативна інверсія.

Матриці відрахувань. Порівняння.

Лінійне рівняння. Лінійні рівняння з одним невідомим, що містять порівняння. Система лінійних рівнянь, що містять порівняння.

Тема 4. Традиційні шифри з симетричним ключем

Принципи Керкгоффса. Криптоаналіз. Атака тільки на зашифрований текст. Атака грубої сили. Статистична атака. Атака за зразком. Атака знання вихідного тексту. Атака з вибіркою вихідного тексту. Атака з вибором зашифрованого тексту.

Категорії традиційних шифрів. Шифри підстановки. Моноалфавітні шифри. Адитивний шифр. Шифр зсуву. Шифр Цезаря. Криптоаналіз. Статистичні атаки. Мультиплікативні шифри. Криптоаналіз афінного шифру. Моноалфавітни шифр підстановки. Криптоаналіз. Багатоалфавітні шифри. Автоключевий шифр. Криптоаналіз. Шифр Плейфера. Криптоаналіз шифру Плейфера. Шифр Віженера. Список Віженера. Криптоаналіз шифру Віженера. Шифр Хілла. Криптоаналіз шифрів Хілла. Одноразовий блокнот. Роторний шифр. Машина "Енігма". Кодова книга - довідник шифрів. Процедура зашифрованих повідомлень. Процедура для розшифровки повідомлення. Криптоаналіз.

Шифри перестановки. Шифри перестановки без використання ключа. Ключові шифри перестановки. Об'єднання двох підходів. Ключі. Використання матриць. Криптоаналіз шифрів перестановки. Статистична атака. Атака грубої сили. Атака за зразком. Шифри с подвійною перестановкою.

Шифри потоку і блокові шифри. Шифри потоку. Блокові шифри. Комбінація.

Тема 5. Алгебраїчні структури.

Группи. Поле. Поля GF(2n). Поліноми. Операції. Модуль. Додавання. Множення. Множення, що використовує комп'ютер. Використання генератора. Інверсії. Адитивні інверсії. Мультиплікативні інверсії. Додавання і віднімання. Множення і ділення.

Тема 6. Сучасні блокові шифри.

Підстановка, або транспозиція. Блокові шифри як групові математичні перестановки. Повнорозмірні ключові шифри. Шифри ключа часткового розміру. Шифри без ключа. Компоненти сучасного блокового шифру. S-блоки. Циклічний зсув. Заміна. Розбиття і об'єднання. Складові шифри. Розсіювання і перемішування. Раунди. Два класу складових шифрів. Шифри Файстеля. Шифри НЕ-Файстеля. Атаки на блокові шифри. Диференціальний криптоаналіз. Лінійний криптоаналіз.

Сучасні шифри потоку. Синхронні шифри потоку. Одноразовий блокнот. Регістр зсуву зі зворотним зв'язком. Несинхронні шифри потоку.

Тема 7. DES

Загальні положення. Структура DES. Початкові і кінцеві перестановки. Раунди. Функція DES. Шифр і зворотний шифр. Перший спосіб. Алгоритм. Альтернативний спосіб. Генерація ключів. Видалення бітів перевірки. Зрушення вліво. Перестановка стиснення. Алгоритм.

Аналіз DES. Властивості. Лавинний ефект. Ефект повноти. Критерії розробок DES. S-блоки. P-блоки. Число раундів. Слабкості DES. Слабкість в ключі шифру.

Багаторазове застосування DES. Дворазовий DES. Триразовий DES. Триразовий DES з двома ключами. Триразовий DES з трьома ключами.

Безпека DES. Атака грубої сили. Диференціальний криптоаналіз. Лінійний криптоаналіз.

Змістовій модуль 2. Сучасні методи шифрування

Тема 8. Перетворення.

Критерії. Безпека. Вартість. Реалізація. Раунди. Одиниці даних. Біт. Байт. Слово. Блок. Матриця станів. Структура кожного раунду.

Підстановка. SubBytes. InvSubBytes. Перетворення з використанням поля GF. Алгоритм. Нелінійність. Перестановка. ShiftRows. InvShiftRows. Алгоритм. Змішування. MixColumns. InvMixColumns. Алгоритм. Додавання ключів. AddRoundKey. Алгоритм.

Тема 9. Розширення ключів.

Розширення ключів в AES-128. RotWord. SubWord. RoundConstants. Алгоритм. Розширення ключа в AES-192 і AES-256. Аналіз розширення ключа.

Шифри. Початковий проект. Алгоритм. Альтернативний проект. Пари SubBytes / ShiftRows. Пара MixColumns / AddRoundKey. Зміна алгоритму розширення ключів. Приклади.

Аналіз AES. Безпека. Атака грубої сили. Статистичні атаки. Диференціальні та лінійні атаки. Реалізація. Простота і вартість.

Тема 10. Застосування сучасних блокових шифрів.

Режим електронної кодової книги. Проблеми безпеки. Поширення помилки. Алгоритм. Захоплення зашифрованого тексту. Додатки. Режим зчеплення блоків шифрованого тексту (CBC). Вектор ініціалізації (IV). Проблеми безпеки. Поширення помилки. Алгоритм. Захоплення зашифрованого тексту. Додатки. Режим кодованої зворотного зв'язку (CFB). CFB як шифр потоку. Алгоритм. Проблеми безпеки. Поширення помилки. Додаток. Спеціальний випадок. Режим зовнішнього зворотного зв'язку (OFB). OFB як шифр потоку. Алгоритм. Проблеми безпеки. Поширення помилки. Спеціальний випадок. Режим лічильника (CTR). CTR як шифр потоку. Алгоритм. Безпека. Поширення помилки. Порівняння різних режимів.

Використання шифрів потоку. RC4. Матриця станів. Ідея. Алгоритм. Проблеми безпеки. A5 / 1. Генератор ключів. Шифрування / дешифрування. Проблеми безпеки. Управління ключами. Генерування ключів.

Тема 11. Прості числа.

Визначення. Взаємно прості числа. Кількість простих чисел. Число простих чисел. Число простих чисел, менших n. Перевірка на просте число. Решето Ератосфена. Phi-функція Ейлера. Мала теорема Ферма. Перша версія. Друга версія. Додатки. Теорема

Ейлера. Перша версія. Друга версія. Додатки. Генерація простих чисел. Прості числа Мерсенна. Прості числа Ферма.

Випробування простоти чисел. Детерміновані алгоритми. Алгоритм теорії подільності. AKS-алгоритм. Імовірнісні алгоритми. Тест Ферма. Випробування квадратним коренем. Тест Міллера-Рабіна. Ініціалізація. Рекомендовані тести простоти чисел.

Розкладання на множники. Основна теорема арифметики. Найбільший спільний дільник. Найменше спільне кратне. Методи розкладання на множники. Метод перевірки розподілом. Метод Ферма. Метод Полларда. PB (Rho) - метод Полларда. Більш ефективні методи. Квадратичне решето. Решето поля чисел. Інші проблеми. Китайська теорема про залишки.

Тема 12. Квадратичне порівняння з модулем.

Квадратичне порівняння з модулем у вигляді простого числа. Квадратичні відрахування і невирахування. Критерій Ейлера. Рішення квадратичного порівняння з модулем у вигляді простого числа. Квадратичне порівняння по складеному модулю. Складність.

Піднесення до ступеню і логарифми. Швидке піднесення в ступінь. Логарифм. Повний перебір. Дискретний логарифм. Рішення модульного логарифма з використанням дискретних логарифмів.

Тема 13. Криптографічна система RSA.

Вступ. Ключі. Загальна ідея. Оригінальний текст / зашифрований текст. Шифрування / дешифрування. Потреба в обох криптосистемах. "Лазівка" в односторонньої функції. Функції. "Лазівка" в односторонньої функції. Ранцева криптосистема. Визначення. Супербільшення кортежу. Секретна зв'язок з використанням ранця. Генерація ключів. Шифрація. Дешифрація. Лазівка.

Криптографічний система RSA. Введення. Процедура. Дві алгебраїчні структури. Генерація ключів. Шифрування. Дешифрування. Доказ RSA. Деякі тривіальні приклади. Атаки RSA. Атака розкладання на множники. Атака з вибіркою зашифрованого тексту. Атаки на показник ступеня шифрування. Атаки показника ступеня дешифрування. Атаки вихідного тексту. Атаки модуля. Атаки реалізації. Рекомендації. Оптимальне асиметричне додаток шифрування (OAEP - Optimal Assimetric Encryption Padding). Помилка в передачі.

Тема 14. Криптосистема Рабина.

Процедура. Генерація ключів. Шифрування. Дешифрування. Безпека криптографічного системи Рабина.

Криптографічна система Ель-Гамаля. Процедура. Генерація ключів. Шифрування. Дешифрування. Доказ. Аналіз. Безпека криптосистеми Ель-Гамаля. Атаки малого модуля. Атака знання вихідного тексту. Додаток

Криптосистеми на основі методу еліптичних кривих. Еліптичні криві в дійсних числах. Абелева група. Група і поле. Еліптичні криві в GF(p). Знаходження інверсії. Знаходження точок на кривій. Складання двох точок. Множення точки на константу. Еліптичні криві в GF. Знаходження інверсії. Знаходження точок на кривій. Складання двох точок. Множення точок на константу. Криптографія еліптичної кривої, що моделює криптосистему Ель-Гамаля. Генерація загальнодоступних і приватних ключів. Шифрування. Дешифрування. Порівняння. Безпека методу з використанням еліптичної кривої. Розмір модуля.

Теми лабораторних робіт

Лабораторна робота № 1. Найпростіші шифри.

Лабораторна робота № 2. Блочно симетричні шифри.

Лабораторна робота № 3. Асиметричні криптосистеми.

Лабораторна робота № 4. Алгоритм цифрового підпису.

Лабораторна робота № 5. Стеганографічні методи захисту інформації.

Лабораторна робота № 6. Використання програми PGP для шифрування повідомлень електронної пошти.

Лабораторна робота № 7. Статистичні дослідження генераторів випадкових та псевдовипадкових послідовностей за методикою NISTSTS.

4. Порядок оцінювання результатів навчання

Система оцінювання сформованих компетентностей у студентів враховує види занять, які згідно з програмою навчальної дисципліни передбачають лекційні, лабораторні заняття, а також виконання самостійної роботи. Оцінювання сформованих компетентностей у студентів здійснюється за накопичувальною 100-бальною системою. Відповідно до Тимчасового положення “Про порядок оцінювання результатів навчання студентів за накопичувальною бально-рейтинговою системою” ХНЕУ ім. С. Кузнеця, контрольні заходи включають:

поточний контроль, що здійснюється протягом семестру під час проведення лекційних, лабораторних занять і оцінюється сумою набраних балів (максимальна сума – 60 балів; мінімальна сума, що дозволяє студенту складати залік, – 35 балів);

модульний контроль, що проводиться у формі контрольної роботи з ініціативи викладача з урахуванням поточного контролю за відповідний змістовий модуль і має на увазі інтегровану оцінку результатів навчання студента після вивчення матеріалу з логічно завершеної частини дисципліни – змістового модуля;

підсумковий/семестровий контроль, що проводиться у формі семестрового заліку, відповідно до графіку навчального процесу.

Порядок проведення поточного оцінювання знань студентів. Оцінювання знань студента під час лабораторних занять та виконання індивідуальних завдань проводиться за такими критеріями:

- здатністю застосовувати відповідний математичний апарат для вирішення професійних завдань;
- здатністю здійснювати раціональний вибір засобів забезпечення інформаційної безпеки інформаційно-комунікаційних систем з урахуванням пред'явлених до них вимог якості обслуговування і якості функціонування.

Загальними критеріями, за якими здійснюється оцінювання позааудиторної самостійної роботи студентів, є:

- знання моделей шифрів і математичних методів їх дослідження, основних задач та понять криптографічних методів захисту інформації, основних криптографічних методів захисту інформації, вимог до шифрів і основних характеристик шифрів;
- вміння застосовувати математичні методи опису і дослідження криптографічних систем, здійснювати раціональний вибір криптографічних методів і засобів захисту інформації в телекомунікаційних системах та реалізовувати типові криптографічні перетворення;
- володіння навичками математичного моделювання в криптографії, навичками використання типових криптографічних перетворень, застосування інженерно-криптографічних механізмів для виявлення уразливостей криптографічних засобів захисту інформації.

Студента слід вважати атестованим, якщо сума балів, одержаних за результатами підсумкової/семестрової перевірки успішності, дорівнює або перевищує

60. Підсумкова оцінка з навчальної дисципліни розраховується з урахуванням балів, отриманих під час заліку, та балів, отриманих під час поточного контролю за накопичувальною системою. Сумарний результат у балах за семестр складає: “60 і більше балів – зараховано”, “59 і менше балів – не зараховано” та заноситься у залікову "Відомість обліку успішності" навчальної дисципліни.

Розподіл балів за тижнями

Теми змістового модуля			**Лекційні заняття**	**Лабораторні заняття**	**Письмова контрольна робота**	**Усього**
Змістовий модуль 1.	**Тема 1**	1 тиждень	1	3		4
	Тема 2	2 тиждень	1	3		4
	Тема 3	3 тиждень	1	3		4
	Тема 4	4 тиждень	1	3		4
	Тема 5	5 тиждень	1	3		4
	Тема 6	6 тиждень	1	3		4
	Тема 7	7 тиждень	1	3		4
	Тема 8	8 тиждень	1	3	10	14
Змістовий модуль 2.	**Тема 9**	9 тиждень	1	3		4
	Тема 10	10 тиждень	1	3		4
	Тема 11	11 тиждень	1	3		4
	Тема 12	12 тиждень	1	3		4
	Тема 13	13 тиждень	1	3		4
	Тема 14	14 тиждень	1	3		4
	Тема 15	15 тиждень	1	3	10	14
	Залік					20
Усього			15	45	20	100

Шкала оцінювання: національна та ЄКТС

Сума балів за всі види навчальної діяльності	Оцінка ЄКТС	Оцінка за національною шкалою	
		для екзамену, курсового проекту (роботи), практики	для заліку
90 – 100	A	відмінно	зараховано
82 – 89	B	добре	

74 – 81	C		
64 – 73	D	задовільно	
60 – 63	E		
35 – 59	FX	незадовільно	не зараховано
1 – 34	F		

5. Рекомендована література

5.1. Основна

1. В. Мао. Современная криптография: теория и практика. - СПб.: Вильямс, 2005, Д 85с.
2. Аграновский А. В., Хади Р. А. Практическая криптография: алгоритмы и их программирование - М.: СОЛОН-ПРЕСС, 2009
3. Бирюков А. А. Информационная безопасность: защита и нападение - М.: ДМК Пресс, 2012
4. Виега Д., Лебланк Д., Ховард М. 19 смертных грехов, угрожающих безопасности программ : Как не допустить типичных ошибок - М.: ДМК Пресс, 2009 v

5.2. Додаткова

5. Вернет, Пэйн. Криптография. Официальное руководство RSA Security. - М.: Бином, 2002,342с.
6. Грэм, Кнут, Паташник. Конкретная математика. - М.: Мир, 1998, 145с.
7. П.Н. Девянин, О.О. Михальский, Д.И. Правиков, А.Ю. Щербаков. Программно-аппаратные средства обеспечения информационной безопасности. Теоретические основы компьютерной безопасности. - М.: Радио и связь, 2000, 176с.
8. А.А. Малюк, С.В. Пазизин, Н.С. Погожин. Введение в защиту информации в автоматизированных системах. - М.: Горячая Линия - Телеком, 2001, 126с.
9. А.А. Молдовян, Н.А. Молдовян, Гуц, Изотов. - Криптография: скоростные шифры. - СПб.: БХВ, 2002, 222 с.
10. Ноден, Ките. Алгебраическая алгоритмика. - М.: Мир, 1999, 192с.

5.3. Інформаційні ресурси в мережі Інтернеті

11. www.cyberpol.ru - Комп'ютерна злочинність і способи боротьби.
12. www.iso27000.ru - Інформаційний портал, присвячений питанням управління інформаційною безпекою.
13. www.itsec.ru - Інтернет-журнал «Інформаційна безпека».
14. www.inside-zi.ru - Інформаційно-методичний журнал «Захист інформації. Інсайд».
15. www.kaspersky.ru - Лабораторія Касперського.
16. www.drweb.com – Лабораторія DrWeb.
17. Сайт персональних навчальних систем ХНЕУ ім. С. Кузнеця навчальної дисципліни “Математичні основи криптології” https://pns.hneu.edu.ua/course/view.php?id=5678