Міністерство освіти і науки України

Харківський національний університет імені В.Н. Каразіна

Кафедра безпеки інформаційних систем і технологій

"ЗАТВЕРДЖУЮ"

Проректор з науково-педагогічної роботи

Антон ПАНТЕЛЕЙМОНОВ

"_____" _____ 2020 р.

Робоча програма навчальної дисципліни

Теорія чисел, груп, полів, кілець

рівень вищої освіти перший (бакалаврський)

галузь знань 12 «Інформаційні технології»

спеціальність 125 – «Кібербезпека»

освітня програма Кібербезпека

спеціалізація

вид дисципліни обов'язкова

факультет комп'ютерних наук

2020 / 2021 навчальний рік

Програму рекомендовано до затвердження вченою радою факультету (інституту, центру)
"31" серпня 2020 року, протокол № 12

РОЗРОБНИКИ ПРОГРАМИ: Кузнецов Олександр Олександрович, доктор технічних наук, професор, професор кафедри безпеки інформаційних систем і технологій.

Програму схвалено на засіданні кафедри безпеки інформаційних систем і технологій
Протокол від "31" серпня 2020 року № 1

Завідувач кафедри безпеки інформаційних систем і технологій

_____ Рассомахін С.Г.

Програму погоджено з гарантом освітньої (професійної/наукової) програми (керівником проектної групи) Кібербезпека
назва освітньої програми

Гарант освітньої (професійної/наукової) програми

(керівник проектної групи) Рассомахін Сергій Геннадійович

_____ Рассомахін С.Г.
(підпис) (прізвище та ініціали)

Програму погоджено методичною комісією факультету комп'ютерних наук

Протокол від "31" серпня 2020 року № 1

Голова методичної комісії факультету комп'ютерних наук

_____ Бердніков А. Г.

Додаток до робочої програми навчальної дисципліни "Теорія чисел, груп, полів, кілець".

Дію робочої програми продовжено: на 2021/2022 н. р.

Заступник декана факультету з навчальної роботи

_____ Євгенія КОЛОВАНОВА

« » серпня 2021 р.

Голова методичної комісії факультету комп'ютерних наук

_____ Анатолій БЕРДНІКОВ

« » серпня 2021 р.

Програму погоджено з гарантом освітньої програми 125 «Кібербезпека»
Гарант освітньої програми 125 «Кібербезпека»

_____ Сергій РАССОМАХІН

ВСТУП

Програма навчальної дисципліни "Теорія чисел, груп, полів, кілець" складена відповідно до освітньо-професійної програми підготовки першого (бакалаврського) рівня за спеціальністю 125 «Кібербезпека», освітня програма «Кібербезпека».

1. Опис навчальної дисципліни

1.1. Мета викладання навчальної дисципліни

Метою викладання навчальної дисципліни є вивчення основних понять та положень теорії чисел, теорії груп, полів, кілець, що є математичною основою сучасних методів та обчислювальних алгоритмів перешкодостійкого кодування та криптографічного захисту інформації.

1.2. Основні завдання вивчення дисципліни

У цьому курсі передбачається формування у студентів певних знань теорії чисел, теорії груп, полів, кілець, елементів алгебраїчної теорії блокових кодів та теорії алгебраїчних кривих, зокрема кінцевих груп над точками еліптичних кривих, які використовуються у сучасних криптоперетвореннях з відкритими ключами

1.3. Кількість кредитів 6

1.4. Загальна кількість годин 180

1.5. Характеристика навчальної дисципліни	
Нормативна	
Денна форма навчання	Заочна (дистанційна) форма навчання
Рік підготовки	
2-й	-й
Семестр	
4-й	-й
Лекції	
52 год.	год.
Практичні, семінарські заняття	
30 год.	год.
Лабораторні заняття	
14 год.	год.
Самостійна робота	
84 год.	год.
Індивідуальні завдання	
розрахункова робота 10 год.	

1.6. Заплановані результати навчання

Згідно з вимогами освітньо-професійної програми студенти повинні досягти таких результатів навчання:

ЗНАТИ:

- основні поняття і теореми теорії чисел;
- основні положення теорії порівнянь, зокрема системи вирахувань та модулярні системи обчислень;
- обчислювальні методи перетворень та порівнянь по простому та складеному модулю;
- методи та алгоритми перетворень нянь у системах вирахувань та модулярних системах обчислень;
- основні поняття та визначення теорії груп, полів, кілець та елементів лінійної алгебри;
- основні властивості та структуру кінцевих полів, арифметику та основні перетворення в кінцевих полях;
- обчислювальні методи спектральних перетворень в кінцевих полях, зокрема обмеження спряженості та ідемпотенти;
- елементи алгебраїчної теорії блокових кодів, зокрема визначення та групову структуру циклічних кодів, кодів Ріда-Соломона, Боуза-Чоудхурі-Хоквінгема (БЧХ), Хемінга, методи спектрального опису циклічних кодів;
- математичні перетворення у групі точок еліптичної кривої, зокрема перетворення відповідно до ДСТУ 4145-2002, ГОСТ Р 34.10-2001 та FIPS-186.

ВМІТИ:

- виконувати практичні обчислення за відповідними алгоритмами теорії чисел (ділення із залишком, обчислення найбільшого спільогой дільника, обчислення за алгоритмом Евкліда);
- виконувати практичні обчислення для виконання перетворень та порівнянь по простому та складеному модулю, аналізувати та оцінювати складність виконання відповідних перетворень;
- досліджувати властивості чисел та послідовностей чисел, зокрема с символу Лежандра;
- розробляти схеми алгоритмів та прості програмні засоби для виконання відповідних обчислень у системах вирахувань та модулярних системах;
- виконувати практичні обчислення за відповідними алгоритмами теорії груп, полів, кілець та елементів лінійної алгебри, досліджувати властивості та структуру кінцевих полів, реалізовувати арифметику та основні перетворення в кінцевих полях;
- виконувати практичні обчислення для виконання спектральних перетворень в кінцевих полях, зокрема користуватися обмеженнями спряженості та обчислювати ідемпотенти;
- практично реалізовувати обчислення основних алгебраїчних конструкцій групових кодів, зокрема досліджувати групову структуру циклічних кодів, кодів Ріда-Соломона, БЧХ та Хемінга;
- реалізовувати обчислювальні алгоритми та методи спектрального опису циклічних кодів;
- досліджувати властивості математичних перетвореннь у групі точок еліптичної кривої, зокрема відповідно до ДСТУ 4145-2002, ГОСТ Р 34.10-2001 та FIPS-186.

2. Тематичний план навчальної дисципліни

Розділ 1. Основи теорії чисел

Теорія подільності

Тема 1. Основні поняття та теореми теорії подільності

Тема 2. Ланцюгові дроби

Тема 3. Найважливіші функції теорії чисел

Теорія порівнянь

Тема 4. Основні поняття та властивості порівнянь

Тема 5. Теорема Ейлера і теорема Ферма. Порівняння першого ступеня. Китайська теорема про залишки

Тема 6. Символ Лежандра та його властивості. Закон взаємності Гауса. Послідовності Лежандра. Символ Якобі

Тема 7. Первісні корені та індекси. Характери

Тема 8. Застосування методів теорії чисел для захисту інформації

Розділ 2. Основи теорії груп, полів, кілець

Арифметика та основні властивості груп, полів, кілець

Тема 9. Основні поняття та визначення теорії груп, полів, кілець

Тема 10. Арифметика полів Галуа

Тема 11. Структура та основні властивості кінцевих полів

Спектральні перетворення в кінцевих полях та елементи алгебраїчної теорії блокових кодів

Тема 12. Векторні простори та елементи лінійної алгебри. Основні поняття та визначення теорії групових кодів

Тема 13. Спектральні перетворення в кінцевих полях. Обмеження спряженості та ідемпотенти

Тема 14. Елементи алгебраїчної теорії блокових кодів

Математичні перетворення у групі точок еліптичної кривої

Тема 15. Визначення та основні властивості групи точок еліптичної кривої. Перетворення у групі точок еліптичної кривої

3. Структура навчальної дисципліни

Назви розділів і тем	Кількість годин											
	Денна форма						Заочна форма					
	Усього	у тому числі					Усього	у тому числі				
		л	п	лаб.	сем	ср		л	п	лаб	сем	ср
Розділ 1. Теорія чисел												
Тема 1. Основні поняття та теореми теорії подільності	8	4				4						
Тема 2. Ланцюгові дроби	10	4	2			4						
Тема 3. Найважливіші функції теорії чисел	10	4	2			4						
Контрольна робота №1												

Назви розділів і тем	Кількість годин											
	Денна форма						Заочна форма					
	Усього	у тому числі					Усього	у тому числі				
		л	п	лаб.	сем	ср		л	п	лаб	сем	ср
Тема 4. Основні поняття та властивості порівнянь	8	4				4						
Тема 5. Теорема Ейлера і теорема Ферма. Порівняння першого ступеня. Китайська теорема про залишки	10	4	2			4						
Тема 6. Символ Лежандра та його властивості. Закон взаємності Гауса	8	2	2			4						
Тема 7. Первісні корені та індекси. Характери	8	2	2			4						
Тема 8. Застосування методів теорії чисел для захисту інформації	12	2	2	4		4						
Контрольна робота №2												
Разом за розділом 1	74	22	16	4		32						
Розділ 2. Теорія груп, полів, кілець												
Тема 9. Основні поняття та визначення теорії груп, полів, кілець	10	4				6						
Тема 10. Арифметика полів Галуа	14	4	4			6						
Тема 11. Структура та основні властивості кінцевих полів	16	4	2	4		6						
Контрольна робота №3												
Тема 12. Векторні простори та елементи лінійної алгебри. Основні поняття та визначення теорії групових кодів	14	6	2			6						
Тема 13. Спектральні перетворення в кінцевих полях. Обмеження спряженості та ідемпотенти	12	4	2			6						
Тема 14. Елементи алгебраїчної теорії блокових кодів	16	4	2	4		6						
Контрольна робота №4												
Тема 15. Визначення та основні властивості групи точок еліптичної кривої. Перетворення у	14	4	2	2		6						

Назви розділів і тем	Кількість годин											
	Денна форма						Заочна форма					
	Усього	у тому числі					Усього	у тому числі				
		л	п	лаб.	сем	ср		л	п	лаб	сем	ср
групі точок еліптичної кривої												
Контрольна робота №5												
розрахункова робота						10						
Разом за розділом 2	106	30	14	10		52						
Усього годин	180	52	30	14		84						

4. Теми семінарських (практичних, лабораторних) занять та контрольних робіт

Розділ 1. Основи теорії чисел

Практичне заняття (тема) №1. Теорія подільності (4 години)

1. Вирішення лінійних діофантових рівнянь
2. Розкладання дійсних чисел в ланцюгові дроби
3. Обчислення придатних дробів
4. Контінуанти та аналіз алгоритму Евкліда
5. Ціла та дробова частина дійсного числа
6. Кількість та сума дільників позитивного цілого числа. Досконалі числа
7. Функція Мебіуса та функція Ейлера

Контрольна робота №1 за темою «Теорія подільності» (4 години консультацій)

Практичне заняття (тема) №2. Теорія порівнянь (4 години)

1. Повна і приведена система відрахувань
2. Комплексні корені m-го ступеня з одиниці та їх зв'язок з системою відрахувань
3. Многочлени ділення кола
4. Вирішення порівняння першого ступеня (4 способи)
5. Китайська теорема про залишки
6. Порівняння другого ступеня, символ Лежандра та закон взаємності Гауса
7. Символ Якобі

Практичне заняття (тема) №3. Застосування методів теорії чисел для захисту інформації (4 години)

1. Схема розподілу секрету із застосуванням китайської теореми про залишки
2. Алгоритм обміну ключами Діффі-Хелмана
3. Алгоритм RSA (шифрування та ЕЦП)
4. Алгоритм Ель-Гамаля (шифрування та ЕЦП)
5. Алгоритм шифрування із правдоподібним запереченням

Лабораторне заняття (тема) №1. Застосування методів теорії чисел для захисту інформації (4 години)

1. Реалізація схеми розподілу секрету із застосуванням китайської теореми про залишки (для чисел довжиною щонайменше 4096 бітів)
2. Реалізація алгоритму обміну ключами Діффі-Хелмана (для чисел довжиною щонайменше 4096 бітів)
3. Реалізація алгоритму RSA для шифрування та ЕЦП (для чисел довжиною щонайменше 4096 бітів)

4. Реалізація алгоритму шифрування із правдоподібним запереченням (для чисел довжиною щонайменше 4096 бітів)

Контрольна робота №2 за темами «Теорія порівнянь», «Застосування методів теорії чисел для захисту інформації» (4 години консультацій)

Всього за першим розділом: 16 годин (12 годин ПЗ; 4 годин ЛР)

Розділ 2. Основи теорії груп, полів, кілець

Практичне заняття (тема) №4. Арифметика та основні властивості груп (4 години) – за лекціями 13, 14

1. Група класів відрахувань за модулем
2. Підгрупи, цикли та класи суміжності
3. Приклади застосування теорем Келі та Лагранжа в теорії груп
4. Теорема о гомоморфізмі груп
5. Властивості симетричної групи (цикли, зростання, інверсії)

Практичне заняття (тема) №5. Арифметика та основні властивості кілець та полів (4 години) – за лекціями 15, 16, 17

1. Скінченні поля, побудовані за кільцем цілих чисел
2. Скінченні поля, побудовані за кільцем многочленів
3. Лінійні рекурентні регістри в конфігурації Галуа
4. Лінійні рекурентні регістри в конфігурації Фібоначчі
5. Примітивні елементи, мінімальні многочлени та алгебраїчна структура скінчених полів

Лабораторне заняття (тема) №2. Арифметика та основні властивості кілець та полів (4 години)

1. Реалізація лінійних рекурентних регістрів в конфігурації Галуа
2. Реалізація лінійних рекурентних регістрів в конфігурації Фібоначчі
3. Реалізація нелінійних рекурентних регістрів
4. Реалізація лінійних рекурентних регістрів для сучасних симетричних шифрів (в тому числі алгоритму Струмок)

Контрольна робота №3 за темою «Арифметика та основні властивості груп, кілець та полів» (4 години консультацій)

Практичне заняття (тема) №6. Векторні простори та елементи лінійної алгебри (4 години) – за лекціями 18, 19

1. Векторні простори, базиси, ортогональні доповнення
2. Лілійні блокові коди як векторні простори
3. Відстань упаковки та відстань покриття. Досконалі коди
4. Матричний опис лінійних кодів

Практичне заняття (тема) №7. Спектральні перетворення в скінченних полях (4 години) – за лекціями 20, 21, 22, 23

1. Дискретне перетворення Фурье та перетворення Фурье в полях Галуа
2. Властивості зсуву, згортки та коренів при перетворенні Фурье в полях Галуа
3. Обмеження спряженості та ідемпотенти
4. Поліноміальний опис алгебраїчних кодів
5. Теорема БЧХ та побудова кодів у спектральній області

Лабораторне заняття (тема) №3. Алгебраїчні коді та спектральні перетворення в кінцевих полях (4 години)

1. Реалізація двійкових кодів БЧХ у просторовій області
2. Реалізація двійкових кодів БЧХ у спектральній області
3. Дослідження властивостей зсуву, згортки та коренів при перетворенні Фурье в полях Галуа

Контрольна робота №4 за темами «Векторні простори та елементи лінійної алгебри», «Спектральні перетворення в скінченних полях» (4 години консультацій)

Практичне заняття (тема) №8. Математичні перетворення у групі точок еліптичної кривої (2 години) – за лекцією 24

1. Групи точок еліптичної кривої та завдання дискретного логарифмування у групі точок
2. Цикли та порядки точок еліптичної кривої

Лабораторне заняття (тема) №4. Математичні перетворення у групі точок еліптичної кривої (2 години)

4. Реалізація арифметичних перетворень у групі точок еліптичної кривої зі стандарту ДСТУ 4145. Реалізація алгоритму формування та перевірки ЕЦП
5. Реалізація арифметичних перетворень у групі точок еліптичної кривої зі стандартів ГОСТ Р 34.10-2001 та FIPS-186. Реалізація алгоритму формування та перевірки ЕЦП

Контрольна робота №5 за темою «Математичні перетворення у групі точок», (2 години консультацій)

Всього за другим розділом: 28 годин (18 годин ПЗ; 10 годин ЛР)
Всього за дисципліною: 44 годин (30 годин ПЗ; 14 годин ЛР)

5. Завдання для самостійної роботи

№ з/п	Назва теми	Кількість годин
1	Основні поняття та теореми теорії подільності	4
2	Ланцюгові дроби	4
3	Найважливіші функції теорії чисел	4
4	Основні поняття та властивості порівнянь	4
5	Теорема Ейлера і теорема Ферма. Порівняння першого ступеня. Китайська теорема про залишки	4
6	Символ Лежандра та його властивості. Закон взаємності Гауса	4
7	Первісні корені та індекси. Характери	4
8	Застосування методів теорії чисел для захисту інформації	4
9	Основні поняття та визначення теорії груп, полів, кілець	4
10	Арифметика полів Галуа	6
11	Структура та основні властивості кінцевих полів	8
12	Векторні простори та елементи лінійної алгебри. Основні поняття та визначення теорії групових кодів	6
13	Спектральні перетворення в кінцевих полях. Обмеження спряженості та ідемпотенти	6

14	Елементи алгебраїчної теорії блокових кодів	6
15	Визначення та основні властивості групи точок еліптичної кривої. Перетворення у групі точок еліптичної кривої	6
	розрахункова робота	10
	Разом	84

6. Індивідуальні завдання

Індивідуальні завдання студентів пов'язані з вивченням окремих, в тому числі іноземних джерел, за тематикою дисципліни, проведенням аналізу існуючих та перспективних засобів захисту інформації, дослідженням рівнів стійкості, розробленням імітаційних моделей та дослідженням ефективності в тому числі із застосуванням принципу масштабування. Теми індивідуальних завдань, як правило, пов'язуються з науковими та науково - методичними дослідженнями, які веде кафедра та інші підрозділи університету чи інші підприємства чи заклади тощо, фірми.

Основними формами реалізації результатів виконання індивідуального завдання є:

- доповідь чи виступ на семінарських чи практичних заняттях;
- доповідь на тематичних науково - практичних конференціях з опублікуванням тез чи доповідей;
- підготовка та опублікування наукових та науково - практичних статей;
- підготовка та подання результатів досліджень для використання в НДР та ДКР кафедри;
- участь в розробці науково - методичних та навчальних матеріалів;
- підготовка патентів на винаходи та корисні моделі;
- розробка та опис програмних продуктів та моделей тощо.

Під час вивчення дисципліни «Теорія чисел, груп, полів, кілець» основною формою **індивідуального завдання** є розробка програмної реалізації наступних алгоритмів:

- вирішення лінійних діофантових рівнянь;
- розкладання дійсних чисел в ланцюгові дроби;
- обчислення придатних дробів;
- обчислення значення функції Мебіуса та функції Ейлера;
- вирішення порівняння першого ступеня (4 способи);
- вирішення системи порівнянь за допомогою Китайської теореми про залишки;
- обчислення значення символу Лежандра та символу Якобі;
- обчислення розподілу секрету із застосуванням китайської теореми про залишки;
- обміну ключами Діффі-Хелмана;
- RSA (шифрування та ЕЦП);
- Ель-Гамаля (шифрування та ЕЦП);
- шифрування із правдоподібним запереченням;
- обчислення властивостей симетричної групи (цикли, зростання, інверсії);
- функціонування лінійних рекурентних регістрів в конфігурації Галуа;
- функціонування лінійних рекурентних регістрів в конфігурації Фібоначчі;
- надмірного кодування через матричне та поліноміальне множення в часовій області;
- дискретного перетворення Фурье в полях Галуа;
- обчислення властивостей зсуву, згортки та коренів при перетворенні Фурье в полях Галуа;
- надмірного кодування із застосуванням властивостей спряженості у спектральній області.

Виконання кожного індивідуального завдання оцінюється викладачем та враховується як результат оперативного контролю степені засвоєння матеріалу.

7. Методи навчання

Як правило лекційні та практичні заняття проводяться аудиторне. В умовах дії карантину заняття проводяться відповідно до Наказу ректора Харківського національного університету імені В.Н. Каразіна (аудиторне або дистанційно за допомогою платформ Google Meet або Zoom).

8. Методи контролю

Вивчення дисципліни передбачає проведення оперативного та поточного контролю в межах загального обсягу годин, а також проведення підсумкового семестрового контролю.

Для оперативного контролю степені засвоєння матеріалу протягом семестру застосовуються наступні заходи:

- контроль присутності студентів (пропуск лекції без поважної причини – "мінус" два бали);
- контроль і оцінка виконання індивідуального завдання – перевірка роботи комп'ютерної програми та усна співбесіда (оцінюється індивідуально викладачем);
- контроль знання відповідей на контрольні питання (оцінюється індивідуально викладачем).

Поточний контроль проводиться у формі письмових контрольних робіт (КР) в межах годин, запланованих на проведення консультацій та лабораторних робіт. Кожна контрольна робота оцінюється за 8-бальною шкалою, кожна лабораторна робота оцінюється за 5 бальною шкалою.

Підсумковий семестровий контроль проводиться з метою оцінки результатів навчання за дисципліну. Він проводиться у формі семестрового екзамену. Семестрові екзамени та заліки проводяться в обсязі навчального матеріалу, визначеного програмою навчальної дисципліни і в терміни, встановлені навчальним планом. Семестрові екзамени проводяться в письмовій формі (припускається використання контролю з використанням комп′ютерів, інформаційно-комунікативних технологій). Екзамени складаються студентами в період екзаменаційних сесій, передбачених навчальним планом. Екзамени проводяться згідно з розкладом, який доводиться до відома викладачів і студентів не пізніше, як за місяць до початку сесії.

Результати складання екзамену оцінюються за 40-бальною шкалою.

Під час проведення підсумкового семестрового контролю виконується перевірка якості конспекту лекцій та практичних занять.

Отримані результати вивчення дисципліни оцінюються за національною шкалою (чотирирівнева: "відмінно", "добре", "задовільно", "незадовільно" або дворівнева: "зараховано", "не зараховано"), кількістю балів 1 … 100 (відповідно до схеми нарахування балів) і вносяться в екзаменаційну відомість та залікову книжку студента.

Схема нарахування балів

Поточний та оперативний контроль										Розрахунково-графічна робота	Разом	Екзамен	Сума
КР1	КР2	КР3	КР4	КР5	ЛР1	ЛР2	ЛР3	ЛР4	контрольна робота 2 шт.		60	40	100
4	4	5	4	4	4	4	4	5	6*2	10			

Примітка:
КР# - поточний контроль у формі письмової контрольної роботи,
ЛР# - поточний контроль у формі лабораторної роботи,
- номер роботи.

До кількості балів, отриманих студентом за кожну КР та ЛР, додається сума балів оперативного контролю, але загальна сума балів оперативного та поточного контролю не може перевищувати 60 балів та бути меншою 0 балів.

Результати складання екзамену оцінюються за 40-бальною шкалою. Сума балів (від 0 до 100 балів включно) є загальним результатом вивчення дисципліни, який вноситься в екзаменаційну відомість та залікову книжку студента відповідно до шкали оцінювання.

9.Критерії оцінювання

Критерії оцінювання знань студентів на експрес - опитування

Визначення	Кількість балів
Відповідь без помилок	2
Виконання відповіді з незначними помилками	1
Відповідь є з певною кількістю помилок, які не заважають достатньо повному висвітленню питання	0,5
Неправильна відповідь, мають місце грубі помилки, нерозуміння суті питання	0

Критерії оцінювання знань студентів за виконання лабораторній роботі

Визначення	Кількість балів
Завдання по лабораторній роботі виконане самостійно в повному обсязі. Звіт оформлений акуратно відповідно до вимог методичних вказівок. При захисті звіту показано розуміння суті і змісту проведених досліджень	4
Завдання по лабораторній роботі виконане самостійно в повному обсязі. Звіт оформлений достатньо акуратно відповідно до вимог методичних вказівок. При захисті звіту були виявлені незначні помилки у знанні теоретичного матеріалу	3
Завдання по лабораторній роботі виконане в повному обсязі. Звіт оформлений достатньо акуратно, в оформленні звіту є незначні недоліки. При захисті звіту були виявлені незначні помилки у знанні теоретичного матеріалу	2
Завдання по лабораторній роботі виконане. Звіт оформлений з помилками і недоліками. При захисті звіту були виявлені суттєві помилки у знанні теоретичного матеріалу	1

Критерії оцінювання знань студентів за виконання контрольній роботи

Визначення	Кількість балів
Дані повні відповіді на кожне практичне питання показано тверде знання навчального матеріалу, розуміння суті поставлених питань, зроблені повні і правильні висновки	6
У відповідях на поставлені практичні питання показано знання навчального матеріалу, розуміння суті поставлених питань за	4-5

наявності незначних помилок зроблені достатньо повні і правильні висновки	
У відповідях на поставлені практичні питання показано достатньо знання навчального матеріалу при наявності суттєвих помилок, зроблені висновки	3
У відповідях показано розуміння суті поставлених питань за наявності принципових помилок при рішенні практичних завдань, відсутні висновки	1
У відповідях на показано слабкі знання навчального матеріалу при наявності принципових помилок при рішенні практичних завдань, відсутні висновки	0,5

Критерії оцінювання знань студентів за виконання курсової роботі (розрахунково-графічної роботи)

Визначення	Кількість балів
Завдання на курсову роботу виконано акуратно в повній відповідності з вимог методичних вказівок. Студент показав тверде знання навчального матеріалу, вміння чітко і стисло викладати основні результати дослідження.	10
Завдання на курсову роботу виконано досить акуратно, але не в повній відповідності з вимогами методичних вказівок. Студент показав достатньо тверде знання навчального матеріалу і вміння стисло викладати основні результати дослідження.	6-8
Завдання на курсову роботу виконано не в повній відповідності з вимогами методичних вказівок. Студент показав не достатньо тверде знання навчального матеріалу і вміння викладати основні результати дослідження.	3-5
Завдання на курсову роботу виконано не в повній відповідності з вимогами методичних вказівок. Студент показав слабке знання навчального матеріалу і невміння викладати основні результати дослідження. У розрахунково-пояснювальній записці є присутніми помилки	0-2

Критерії оцінювання екзаменаційних робіт студентів

Визначення	Кількість балів
При відповіді на екзаменаційний квиток теоретичні питання освітлені повністю, завдання вирішене правильно, зроблені висновки	40
При відповіді на екзаменаційний квиток теоретичні питання достатньо освітлені, завдання вирішене правильно з незначними помилками, зроблені висновки	35-39
При відповіді на екзаменаційний квиток теоретичні питання освітлені з помилками, завдання вирішене правильно з незначними помилками. Зроблені неповні висновки	25-34

При відповіді на екзаменаційний квиток теоретичні питання освітлені з суттєвими помилками, завдання вирішене з помилками. Зроблені неповні висновки	15-24
При відповіді на екзаменаційний квиток теоретичні питання освітлені з суттєвими помилками, завдання вирішене частково або не повністю. Висновки неповні або відсутні	1-14

Шкала оцінювання

Сума балів за всі види навчальної діяльності протягом семестру	Оцінка	
	для чотирирівневої шкали оцінювання	для дворівневої шкали оцінювання
90 – 100	відмінно	зараховано
70-89	добре	
50-69	задовільно	
1-49	незадовільно	не зараховано

10. Рекомендована література

Основна література

1. Єсін В.І., Кузнецов О.О., Сорока Л.С. Безопека інформаційних систем та технологій. Х.:ООО «ЭДЭНА», 2010. – 656с.
2. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Теорія. Практика. Застосування: Підручник для вищих навчальних закладів. – Харків: Вид-во «Форт», 2013. – 880с.
3. FIPS PUB 186-3. FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION. Digital Signature Standard (DSS). – 131 p.
4. ДСТУ 4145-2002 Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння.

11. Посиланная на інформаційні ресурси в Інтернеті, відео-лекції, інше методичне забезпечення

1. www.nist.gov
2. www.eprint.iacr.org
3. www.iso.org
4. www.springerlink.com
5. www.cacr.math.uwaterloo.ca
6. www.financialcryptography.com
7. www.austinlinks.com
8. www.world.std.com/~franl/crypto.html
9. www.cryptonessie.org