Вступ
Тема 1. Теорія інформації та кодування
1.1. Загальні поняття про системи передачі інформації
1.2. Кількість інформації та ентропія
1.2.1. Ентропія випадкового експерименту з рівноймовірними результатами
1.2.2. Ентропія випадкового експерименту з нерівноймовірними результатами
1.2.3. Умови максимізації ентропії джерела повідомлень
1.2.4. Ентропія складного експерименту при взаємозалежності результатів
1.2.5. Ентропія джерел дискретних повідомлень
1.2.6. Надмірність джерел повідомлень
1.2.7. Ентропія джерел неперервних повідомлень. Диференційна ентропія
1.2.8. Ентропія джерела з нормальним та рівномірним законом розподілу
1.3 Канали передачі інформації
1.3.1 Класифікація каналів передачі інформації
1.3.2. Модель дискретного каналу передачі інформації
1.3.3. Кількість інформації, що передається по дискретному каналу передачі інформації
1.3.4. Пропускна здібність дискретного каналу передачі інформації
1.4 Методи ефективного кодування інформації
1.4.1. Ефективне кодування Шеннона – Фано
1.4.2 Ефективне кодування Хаффмана
1.5. Основні визначення та поняття теорії скінченних полів Галуа
1.5.1. Групи
1.5.2. Підгрупи
1.5.3. Кільця
1.5.4. Підполе і суміжні класи
1.5.5. Скінченні поля, побудовані за кільцем цілих чисел
1.5.6. Скінченні поля, побудовані за кільцем многочленів
1.6. Алгебраїчна теорія блокових кодів
1.6.1. Призначення та класифікація завадостійких кодів
1.6.2. Загальні принципи завадостійкого кодування
1.6.3. Кодові межі блокових і безперервних кодів
1.6.4. Лінійні групові коди
1.6.5. Кодуючі і декодуючі пристрої лінійних групових кодів
1.6.6. Лінійні циклічні коди
1.6.7. Вимоги до породжувального многочлену циклічних кодів
1.6.8. Пристрої кодування та декодування циклічних кодів
1.6.9. Коди Боуза–Чхоудхурі–Хоквінгема, коди Ріда–Соломона
1.6.10. Альтернантні коди, коди Гоппи
1.6.11. Алгеброгеометричні коди
1.7. Методи та алгоритми кодування алгеброгеометричних кодів
1.8. Методи та алгоритми декодування алгеброгеометричних кодів
1.8.1. Методи декодування недвійкових блокових кодів
1.8.2. Декодування алгебраїчних кодів методом Берлекемпа
1.8.3. Декодування двійкових кодів БЧХ
1.8.4. Декодування за допомогою алгоритму Евкліда
1.8.5. Алгебраїчне декодування алгеброгеометричних кодів
1.8.6. Переставне декодування алгеброгеометричних кодів
1.8.7. Мажоритарне декодування алгеброгеометричних кодів
1.8.8. Згортувальні коди
1.8.9. Декодування згортувальних кодів. Алгоритм Витербі
1.9. Багаторазова передача кодових комбінацій
1.10. Системи передачі інформації зі зворотним зв’язком
Контрольні запитання до теми 1
Використана література до теми 1
Тема 2. Криптографічні механізми захисту інформації в інформаційних системах
2.1. Математичні основи сучасної теорії захисту інформації
2.1.1. Математичні положення теорії скінченних полів та систем класів лишків
2.1.2. Математичні положення теорії чисел
2.1.3. Методи булевої алгебри, елементи кореляційного та спектрального аналізу

2.2. Компоненти криптосистеми та їх функціональні характеристики
2.3. Прості шифри
2.4. Криптографічні примітиви й типи структур симетричної криптосистеми
2.4.1. Основні криптографічні примітиви
2.4.2. Структура Файстеля алгоритму блокового симетричного шифрування
2.4.3. SPN-структура алгоритму блокового симетричного шифрування
2.4.4. Типи структур потокових алгоритмів шифрування
2.4.5. Математичні моделі нелінійних вузлів замін у термінах булевої алгебри
2.5. Алгоритми блокового симетричного шифрування DES, ГОСТ-28147
2.5.1. Алгоритм блокового симетричного шифрування DES
2.5.2. Алгоритм блокового симетричного шифрування ГОСТ-28147
2.6. Типові режими роботи криптосистеми
2.6.1. Шифрування в режимі Electronic Code Book, ECB
2.6.2. Шифрування в режимі Cipher Block Changing, CBC
2.6.3. Шифрування в режимі Electronic Feedback, CFB
3.6.4. Шифрування в режимі Output Feedback, OFB
2.6.5. Шифрування в режимах удосконаленого OFB і PCBC
2.6.6. Інші режими шифрування
2.7. Атаки на блокові шифри
2.7.1. Диференціальний криптоаналіз
2.7.2. Лінійний криптоаналіз
2.7.3. Силова атака на основі розподілених розв’язань
2.8. Інші відомі блокові шифри
2.8.1. RC2
2.8.2. RC5
2.8.3. IDEA
2.8.4. Алгоритм SAFER
2.8.5. FEAL
2.8.6. Skipjack
2.8.7. Blowfish
2.8.8. REDOC
2.8.9. LOKI
2.8.10. Khufu
2.8.11. Khafre
2.8.12. Алгоритм Rijndael
2.9. Потокові шифри
2.9.1. Регістри зсуву зі зворотнім зв’язком
2.9.2. Алгоритм A5
2.9.3. RC4
2.9.4. SEAL
2.10. Принципи побудови криптосистем з відкритим ключем
2.10.1. Криптосистема шифрування даних RSA
2.10.2. Криптосистема Ель Гамаля
2.10.3. Комбінований метод шифрування
2.10.4. Керування криптографічними ключами
2.10.5. Механізми керування ключами на основі використання несиметричних методів (ISO/IEC 11770-3)
2.10.6. Безпека розподілу ключів
2.10.7. Криптографія на еліптичних кривих
2.11. Методи та алгоритми забезпечення автентичності та цілісності даних
2.11.1. Електроний підпис
2.11.2. MDC-коди
2.11.3. MAC-коди
Контрольні запитання до теми 2
Використана література до теми 2
Тема 3. Основи квантової криптографії
3.1. Небезпека криптографічних технологій
3.2. Фізичні основи квантових обчислень
3.3. Квантові біти

3.4. Квантові операції
3.5. Парадокс Ейнштейна-Подольські-Розена
3.6. Квантові алгоритми
3.6.1. Протокол квантового щільного кодування
3.6.2. Алгоритм Дойча
3.7. Квантова криптографія
3.7.1. Алгоритм факторизації цілих чисел (алгоритм Шора)
3.7.2. Алгоритм пошуку у невпорядкованому масиві (алгоритм Гровера)
3.7.3. Квантові протоколи узгодження ключів
3.7.4. Квантовий протокол узгодження криптографічного ключа BB84
3.7.5. Протокол узгодження ключа B92
3.7.6. Атаки на протоколи квантового узгодження ключа
3.7.7. Реалізації протоколу квантового узгодження ключа
3.7.8. Протокол узгодження ключа E91
3.7.9. Квантові гроші Стівена Візнера
3.8. Архітектура та основні вимоги до квантових комп’ютерів
3.9. Огляд фізичних реалізацій квантових комп’ютерів
3.9.1. Гармонічний осцилятор як модель квантового комп’ютера
3.9.2. Квантовий комп’ютер на фотонах
3.9.3. Квантовий комп’ютер на оптичних резонаторах
3.9.4. Йони у пастках
3.9.5. Ядерний магнітний резонанс
Контрольні запитання до теми 2
Використана література до теми 3