ЗАЩИТА ИНФОРМАЦИИ В КАНАЛАХ СВЯЗИ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

к самостоятельной работе
для студентов направления 11.04.01 «Радиотехника»
(магистерская программа подготовки «Радиотехнические
средства обработки и защиты информации в каналах связи»)

Воронеж 2023

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Воронежский государственный технический университет»

Кафедра радиотехники

ЗАЩИТА ИНФОРМАЦИИ В КАНАЛАХ СВЯЗИ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

к самостоятельной работе
для студентов направления 11.04.01 «Радиотехника»
(магистерская программа подготовки «Радиотехнические
средства обработки и защиты информации в каналах связи»)

Воронеж 2023

УДК 621.396
ББК 32.85

Составитель *канд. техн. наук Р. П. Краснов*

Защита информации в каналах связи: методические указания к самостоятельной работе для студентов направления 11.04.01 «Радиотехника» (магистерская программа подготовки «Радиотехнические средства обработки и защиты информации в каналах связи») / ФГБОУ ВО «Воронежский государственный технический университет»; сост.: Р. П. Краснов. Воронеж: Изд-во ВГТУ, 2023. 20 с.

В методических указаниях приведены материалы для выполнения самостоятельной работы по дисциплине «Защита информации в каналах вязи» для студентов 1 курса направления 11.04.01 «Радиотехника». Представлено содержание дисциплины, список тем и вопросов для самоподготовки.

Предназначены для студентов 1 курса направления 11.04.01 «Радиотехника».

Методические указания подготовлены в электронном виде и содержатся в файле СР ЗИ в КС 2023.pdf.

УДК 621.396
ББК 32.85

Табл.1. Библиогр. 4 назв.

Рецензент – А. В. Володько, канд. техн. наук, доц. кафедры радиоэлектронных устройств и систем ВГТУ

Издается по решению редакционно-издательского совета Воронежского государственного технического университета

1. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Цель преподавания дисциплины – обеспечение студентов базовыми знаниями, навыками и представлениями в области защиты информации, теории информации и криптографии.

Для достижения цели ставятся *задачи*:

1. Освоение методов защиты аналоговых и цифровых сигналов при передаче в канале связи.
2. Изучение общих принципов и понятий теории информации.
3. Освоение методов расчета помехоустойчивости при применении корректирующих кодов.
4. Изучение базовых принципов построения и использования криптографических систем.
5. Освоение принципов построения и применения разнесенных систем передачи данных.

В результате освоения дисциплины обучающийся должен:

Знать: методы защиты информации в канале при передаче аналоговых и цифровых сигналов, основные понятия теории информации, базовые принципы криптографических методов защиты, методы построения систем передачи данных с разнесением.

Уметь: выбирать методы защиты передаваемых данных в зависимости от типа канала связи, формы представления информации в виде сигналов, требований к качеству связи в системе передачи данных.

Владеть: базовыми понятиями и методами теории информации, помехоустойчивого кодирования, криптографии, разнесенного приема.

Изучаемая дисциплина преподается в течение двух семестров, включает лекционные и лабораторные занятия и курсовую работу.

Методические указания для обучающихся по освоению дисциплины

Основными формами *текущего контроля* при изучении дисциплины являются индивидуальный устный опрос (УО), тестирование (Т), защита результатов лабораторных исследований (ЗЛ).

При устном опросе и защите результатов лабораторных исследований оценка «отлично» выставляется студенту, корректно ответившему на не менее чем 80% задававшихся ему вопросов; оценка «хорошо» выставляется за успешный ответ не менее чем на 60% вопросов; при ответе по меньшей мере на 40% вопросов студент получает оценку «удовлетворительно»; худшие результаты фиксируются как «неудовлетворительные».

При *промежуточном (итоговом) контроле* в форме зачета с оценкой или экзамена на оценку «отлично» могут претендовать студенты, демонстрирующие знание теоретического материала, способные ответить по меньшей мере на 80% вопросов преподавателя (в рамках утвержденного комплекта оценочных средств (КОС)) и самостоятельно решать задачи, как минимум, среднего уровня сложности. Оценку «хорошо» заслуживают студенты, демонстрирующие знание наиболее важных положений теоретического материала, способные ответить по меньшей мере 60% вопросов преподавателя (в рамках утвержденного КОС) и самостоятельно решать задачи невысокой сложности, а также решать задачи среднего уровня сложности под руководством преподавателя. Оценку «удовлетворительно» получают студенты, демонстрирующие знание наиболее важных положений теоретического материала, способные ответить, как минимум, на 40% вопросов преподавателя (в рамках КОС), а также решать задачи невысокой сложности под руководством преподавателя. При более низкой результативности студент получает оценку «неудовлетворительно».

Контроль в форме тестирования_проводится по тест-билетам, каждый из которых содержит 10 вопросов. Каждый правильный ответ на вопрос в тесте оценивается 1 баллом. Максимальное количество набранных баллов – 30.

1. Оценка «Неудовлетворительно» ставится в случае, если студент набрал менее 16 баллов.
2. Оценка «Удовлетворительно» ставится в случае, если студент набрал от 16 до 20 баллов.
3. Оценка «Хорошо» ставится в случае, если студент набрал от 21 до 25 баллов.
4. Оценка «Отлично» ставится, если студент набрал от 26 до 30 баллов

Основой изучения дисциплины являются лекции, на которых излагаются наиболее существенные и трудные вопросы, а также вопросы, не нашедшие отражения в учебной литературе.

Лабораторные занятия проводятся в режиме моделирования на ПЭВМ типовых методов защиты информации в каналах связи. Они направлены на наглядное изучение взаимосвязи между параметрами радиотехнических устройств, статистическими характеристиками помех, возникающих в каналах связи.

Большое значение по закреплению и совершенствованию знаний имеет самостоятельная работа студентов. Информацию о всех видах самостоятельной работы студенты получают на занятиях.

Контроль усвоения материала дисциплины производится устным опросом при защите результатов лабораторных работ. Освоение дисциплины оценивается на экзамене.

Таблица

Виды деятельности студента

Вид учебных занятий	Деятельность студента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Обозначение вопросов, терминов, материала, которые вызывают трудности, поиск ответов в рекомендуемой литературе.
Лабораторные занятия	Работа с конспектом лекций, просмотр рекомендуемой литературы. Изучение теоретических материалов и подготовка домашних заданий к лабораторным работам. Выполнение исследований; при этом особое внимание следует уделить выявлению взаимосвязей между изменением параметров помех и возможностью кода.
Самостоятельная работа	Самостоятельная работа предполагает следующие составляющие: - работа с текстами: учебниками, справочниками, дополнительной литературой, а также проработка конспектов лекций; - выполнение домашних заданий и расчетов; - работа над темами для самостоятельного изучения; - подготовка к промежуточной аттестации.
Подготовка к замену	При подготовке к экзамену необходимо ориентироваться на конспекты лекций, рекомендуемую литературу, и результаты лабораторных занятий.

2. ТЕМЫ ЛЕКЦИЙ И ВОПРОСЫ ДЛЯ САМОПРОВЕРКИ

1. Методы защиты информации в каналах связи. Виды помех. Типы защиты от ошибок. Связность оконечных устройств.

Вопросы для самопроверки:

1) Перечислите виды защиты информации в каналах связи.
2) Приведите виды помех, воздействующих на сигналы систем передачи данных.
3) Приведите методы защиты информации в цифровых каналах связи.
4) Приведите методы защиты информации в аналоговых каналах связи.
5) Перечислите виды связности оконечных устройств.
6) Перечислите методы реакции приемного оборудования на нарушения при приеме данных.

2. Помехозащита радиоприемных устройств. Модели каналов связи: дискретный канал с памятью и без, двоичный симметричный, гауссовский.

Вопросы для самопроверки:

1) Приведите основные типы устройств АРУ и дайте краткую характеристику их принципов их работы.
2) Перечислите основные виды ограничителей сигналов, дайте краткую характеристику их принципов их работы.
3) Приведите модель дискретного канала без памяти.
4) Приведите модель двоичного симметричного канала
5) Приведите модель гауссовского канала.

3. Защита информация при передаче аналоговых сигналов. Методы защиты информации с инверсией спектра, временными и частотными перестановками.

Вопросы для самопроверки:

1) Поясните сущность процесса частотной инверсии.
2) Поясните сущность процесса частотной перестановки.

3) Поясните сущность процесса временной перестановки.

4) Каков принцип работы инвертора спектра?

5) Каков принцип работы устройства частотной перестановки?

6) Поясните принцип работы скремблера.

7) Поясните принцип работы скремблера под управлением криптоблока.

4. Основы теории информации. Количество информации и энтропия. Дискретный источник. Информационная модель канала связи. Принципы оптимального кодирования.

Вопросы для самопроверки:

1) Что представляет собой дискретный источник информации, какими параметрами характеризуется?

2) Дайте определение количества информации и энтропии.

3) Приведите выражения для совместной, частной и средней условной энтропии.

4) Приведите выражение для полного количества информации в ДСК.

5) Приведите информационную модель канала связи.

6) Сформулируйте теорему кодирования в канале без помех.

7) Сформулируйте теорему кодирования в канале с помехами.

5. Эффективность систем передачи. Помехоустойчивость основных видов корректирующих кодов. Энергетический выигрыш кодирования.

Вопросы для самопроверки:

1) Проведите сравнение помехоустойчивости сигналов различных видов цифровой модуляции.

2) Приведите выражения для информационной, энергетической и частотной эффективности систем передачи данных.

3) Приведите выражение для вероятности ошибок при использовании в канале блочных линейных кодов.

4) Приведите выражение для вероятности ошибок при использовании в канале циклических кодов.

5) Приведите выражение для вероятности ошибок при использовании в канале сверточных кодов.

6) Приведите выражение для вероятности ошибок при использовании в канале каскадных кодов.

6. Оптические системы передачи данных. Атмосферные оптические линии связи. Линии оптической связи в помещении. Особенности передачи оптических сигналов в атмосферном канале.

Вопросы для самопроверки:

1) Приведите выражение закона Бира-Ламберта.

2) Что такое атмосферная турбулентность, как и какими параметрами она описывается?

3) Что представляет собой сцинтилляция и каковы методы борьбы с ней?

4) Перечислите методы компенсации влияния атмосферного канала передачи на качество связи в оптических каналах.

5) Каковы особенности реализации оптической связи в помещениях?

7. Классификация криптографических алгоритмов и шифров. Методы криптоанализа и типы атак.

Вопросы для самопроверки:

1) Сравните модели защищенного канала с криптозащитой и шифрованием.

2) Дайте определение симметричной и асимметричной криптосистемы.

3) В чем отличие шифров замены и перестановки?

4) Перечислите известные Вам методы криптоатак.

5) Поясните принцип построения шифра Цезаря, аддитивного шифра, аффинного шифра, шифра Плейфера.

8. Криптографические методы с открытым ключом. Система Диффи-Хеллмана. Шифры Шамиля и Эль-Гамаля. Шифр RSA.

Вопросы для самопроверки:

1) Сформулируйте принцип односторонности функции.
2) Объясните правила хранения, передачи и чтения ключей в системе Диффи – Хеллмана.
3) Объясните правила хранения, передачи и чтения ключей в шифре Шамира.
4) Объясните правила хранения, передачи и чтения ключей в шифре Эль-Гамаля.
5) Объясните правила хранения, передачи и чтения ключей в шифре RSA.

9. Криптографические хэш-функции. Стандарты хэш-функций. Имитовставка.

Вопросы для самопроверки:

1) Приведите определение и перечислите основные свойства хэш-функции.
2) Опишите способ построения хеш-функций на базе блоковых шифров.
3) Опишите способ построения хеш-функций методом Меркла — Дамгарда.
4) Приведите основные этапы формирования хэш-функции по алгоритму ГОСТ Р 34.11-94.
5) Опишите основные принципы формирования имитовставок.

10. Электронная цифровая подпись. Подпись на базе шифра Эль-Гамаля, RSA.

Вопросы для самопроверки:

1) Поясните назначение и приведите области использования электронных цифровых подписей.
2) Приведите алгоритм формирования электронных цифровых подписей на базе шифра RSA.
3) Приведите алгоритм формирования электронных цифровых подписей на базе шифра Эль-Гамаля.
4) Приведите алгоритм формирования электронных цифровых подписей на базе ГОСТ Р34.10-94.
5) Приведите сравнительную характеристику стандартов ГОСТ Р34.10-94 и FIPS 186.

11. Стойкость криптосистем. Теоретические пределы скрытности. Системы с совершенной секретностью.

Вопросы для самопроверки:

1) При каком условии криптосистема называется совершенно секретной?
2) Поясните принципы формирования шифра Вернама. Почему такой шифр является совершенно секретной криптосистемой?
3) Поясните понятие расстояние единственности шифра.
4) При каком условии шифр можно называть строго идеальным?
5) Приведите пример построения строго идеальной криптосистемы.

12. Блочные алгоритмы шифрования данных. Стандарт шифрования DES, ГОСТ 28147-89, RC6, AES. Режимы функционирования блочных шифров.

Вопросы для самопроверки:

1) Дайте определение блочным шифрам.
2) В чем заключается алгоритм работы ячейки Фейстела?

3) Приведите структуру алгоритма шифрования стандарта DES.

4) Перечислите основные элементы базового цикла шифра ГОСТ 28147-89.

5) Перечислите элементы алгоритма шифрования стандарта RC6.

6) Перечислите элементы алгоритма дешифрования стандарта RC6.

7) Перечислите операции раунда шифрования стандарта AES.

8) Дайте краткое описание операциям раунда шифрования стандарта AES.

9) Перечислите основные режиму функционирования блочных шифров, дайте пояснения особенностей работы в каждом из них.

13. Потоковые шифры. Алгоритм RC4. Генераторы псевдослучайных последовательностей.

Вопросы для самопроверки:

1) Перечислите виды поточных шифров и укажите принципы их функционирования.

2) Дайте краткое описание работы алгоритма RC4.

3) Приведите алгоритм работы линейного конгруэнтного генератора.

4) Приведите принцип работы генератора на основе регистра сдвига с обратными связями.

5) Поясните принцип действия генератора BBS.

14. Криптосистемы на эллиптических кривых. Инфраструктура открытых ключей.

Вопросы для самопроверки:

1) Дайте определение эллиптической кривой. Поясните, в каком виде эти кривые используются при шифровании данных.

2) Какие свойства имеет множество точек эллиптической кривой? Как его применять в прочих стандартах шифрования?

3) Поясните принцип работы шифра Эль-Гамаля на эллиптической кривой.

4) Перечислите этапы формирования электронной подписи в ГОСТ Р34.10-2001.

5) Перечислите этапы проверки электронной подписи в ГОСТ Р34.10-2001.

6) Перечислите иерархические элементы структуры распределения открытых ключей.

15. Принципы разнесенного приема. Системы SISO, SIMO, MISO, MIMO. Математическая модель системы. Пропускная способность.

Вопросы для самопроверки:

1) Приведите конфигурации систем связи типа SISO, SIMO, MISO, MIMO.

2) Приведите модель сигналов в системе типа MIMO.

3) Как определяется пропускная способность системы MIMO?

4) Как определяется пропускная способность системы SIMO?

5) Как определяется пропускная способность системы MISO?

16. Пространственно-временное блочное кодирование. Схема Аламути. Ортогональные, квазиортогональные, неортогональные коды.

Вопросы для самопроверки:

1) Приведите схему пространственно-временного кодера по схеме Аламути.

2) Приведите выражение для пространственно-временной матрицы Аламути.

3) Как происходит детектирование сигналов по схеме Аламути?

4) Приведите пример пространственно-временной матрицы ортогонального кода.

5) Приведите пример пространственно-временной матрицы квазиортогонального кода.

6) Приведите пример пространственно-временной матрицы неортогонального кода.

17. Системы MIMO, использующие информацию о состоянии канала связи. Методы получения информации о канале передатчиком. Модель информации о канале связи. Методы прекодирования.

Вопросы для самопроверки:

1) Приведите модель системы с информацией о текущем состоянии канала связи, получаемой с помощью принципа взаимности.

2) Приведите модель системы с информацией о текущем состоянии канала связи, получаемой с помощью обратной связи.

3) Дайте определения параметрам модели информации о состоянии канала связи.

4) Приведите схему системы связи с линейным прекодированием.

5) Поясните работу системы передачи данных с алгоритмом прекодирования Косты.

3. КОНТРОЛЬНЫЕ ВОПРОСЫ

1 семестр

1. Виды защиты информации.
2. Виды нарушения передачи информации.
3. Виды помех в системах передачи данных.
4. Методы защиты аналоговых и цифровых сигналов в канале связи.
5. Типы связности оконечных устройств.
6. Принцип действия АРУ: АРУ «вперед», АРУ по ближним шумам.
7. Принцип действия АРУ: медленная АРУ, АРУ с многократными стробами.
8. Виды и принцип действия ограничителей сигнала.
9. Схемы амплитудно-частотной селекции.
10. Модель дискретного канала без памяти, двоичного симметричного канала.
11. Модель гауссовского канала.
12. Принцип частотной и временной инверсии и перестановки.
13. Аппаратура частотной инверсии.
14. Аппаратура частотных перестановок.
15. Аппаратура скремблирования.
16. Принцип работы аппаратуры перестановок под управлением криптоблока.
17. Дискретный источник информации. Энтропия источника.
18. Энтропия: частная, совместная, частная условная. Связь между ними.
19. Полное количество информации в двоичном симметричном канале.
20. Информационная модель канала связи.
21. Теорема кодирования в канале без помех.
22. Теорема кодирования в канале с помехами.
23. Помехоустойчивость сигналов цифровой модуляции.
24. Эффективность систем передачи данных.
25. Помехоустойчивость блочных кодов.
26. Энергетический выигрыш кодирования.

27. Помехоустойчивость кодов БЧХ.
28. Помехоустойчивость сверточных кодов.
29. Помехоустойчивость каскадных кодов.

2 семестр

1. Характеристики оптических сигналов. Методы передачи и приема.
2. Поглощение и рассеяние оптического излучения в атмосфере. Закон Бира-Ламберта.
3. Виды атмосферной турбулентности, параметры.
4. Сцинтилляция и апертурное усреднение.
5. Оптические приемники. Методы приема.
6. Стандарты оптической связи в помещениях.
7. Модель системы передачи информации с криптографической защитой по открытому и защищенному каналу.
8. Модель системы передачи информации с аутентификацией и шифрованием.
9. Виды криптоалгоритмов: симметричные и несимметричные, замены, перестановки, композиционные.
10. Методы криптоанализа и криптоатак.
11. Шифр Цезаря, аддитивный перестановочный шифр.
12. Афинный шифр, шифр Плейфера.
13. Понятие криптосистемы с открытым ключом, дискретного логарифма.
14. Система Диффи–Хеллмана с открытым ключом.
15. Шифр Шамира.
16. Шифр Эль-Гамаля.
17. Шифр RSA.
18. Понятие хэш-функции. Требования к хэш-функции.
19. Алгоритм построения хэш-функции.
20. Метод построения хэш-функции Меркла — Дамгарда.
21. Стандарт хэш-функций ГОСТ Р 34.11-94.
22. Имитовставки. Типы имитовставок.
23. Электронная подпись RSA.

24. Электронная подпись на базе шифра Эль-Гамаля.
25. Электронная подпись на базе стандарта ГОСТ Р34.10-94.
26. Понятие совершенно секретной криптосистемы
27. Шифр Вернама.
28. Расстояние единственности шифра с секретным ключом.
29. Строго идеальный шифр.
30. Принципы блочного шифрования. Ячейка Фейстеля.
31. Алгоритм шифрования стандарта DES.
32. Шифр ГОСТ 28147-89.
33. Шифр RC6: шифрование блока данных.
34. Шифр RC6: дешифрование блока данных.
35. Шифр AES: функции одного раунда шифрования.
36. Режимы функционирования блочных шифров: электронная кодовая книга.
37. Режимы функционирования блочных шифров: сцепление блоков шифра
38. Режимы функционирования блочных шифров: обратная связь по выходу
39. Режимы функционирования блочных шифров: счетчик
40. Принцип работы потоковых шифров.
41. Шифр RC4.
42. Линейный конгруэнтный генератор псевдослучайных последовательностей.
43. Генератор псевдослучайных последовательностей на регистре сдвига с обратными связями.
44. Основные принципы построения шифра на эллиптических кривых.
45. ГОСТ Р34.10-2001на эллиптической кривой.
46. Инфраструктура открытых ключей.
47. Конфигурация разнесенной системы: SISO, SIMO, MISO, MIMO.
48. Модель системы MIMO
49. Пропускная способность системы MIMO
50. Пространственно-временное блочное кодирование: схема Аламути.

51. Ортогональные и квазиортогональные пространственно-временные блочные коды.
52. Неортогональные пространственно-временные блочные коды.
53. Методы получения передатчиком информации о состоянии канала связи.
54. Динамическая модель информации о состоянии канала связи.
55. Линейное прекодирование.
56. Нелинейный алгоритм прекодирования Косты.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Краснов, Р.П. Теория электрической связи: курс лекций / Р.П. Краснов, Р.Н. Андреев, М.Ю. Чепелев. – М.: Горячая линия - Телеком, 2014, 230с.

2. Скляр, Б. Цифровая связь: Теоретические основы и практическое применение / Б. Скляр — М.: ИД «Вильямс», 2004. — 1104 с.

3. Бакулин, М. Г. Технология MIMO: принципы и алгоритмы / М. Г. Бакулин, Л. А. Варукина, В. Б. Крейнделин – М.: Горячая линия – Телеком, 2014. – 244 с.

4. Рябко, Б. С. Криптографические методы защиты информации: учебное пособие для вузов / Б.С. Рябко, А.Н. Фионов – М.: Горячая линия – Телеком, 2012. – 229 с.

ОГЛАВЛЕНИЕ

1. Содержание дисциплины 3
2. Темы лекций и вопросы для самопроверки 7
3. Контрольные вопросы 15
Библиографический список 19

ЗАЩИТА ИНФОРМАЦИИ В КАНАЛАХ СВЯЗИ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

к самостоятельной работе
для студентов направления 11.04.01 «Радиотехника»
(магистерская программа подготовки «Радиотехнические средства обработки и защиты информации в каналах связи»)

Составитель
Краснов Роман Петрович

Компьютерный набор Р. П. Краснова

Издается в авторской редакции

Подписано к изданию 08.06.2023.
Уч.-изд. л 1,0

ФГБОУ ВО «Воронежский государственный технический университет»
394006 Воронеж, ул. 20-летия Октября, 84