

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Шебзухова Татьяна Анимовна

Должность: Директор Пятигорского государственного казачьего
федерального университета

Дата подписания: 12.09.2023 15:27:13

Уникальный программный ключ:

d74ce93cd40e39275c3ba2f58486412a1c8ef96f

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ КАЗАЧЬЕ

ОБРАЗОВАНИЯ

«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Пятигорский институт (филиал) СКФУ

Методические указания

по организации самостоятельной работы обучающихся
по дисциплине «Защита информации от утечки по техническим каналам»
для студентов направления подготовки /специальности
10.03.01 Информационная безопасность
шифр и наименование направления подготовки/ специальности

(ЭЛЕКТРОННЫЙ ДОКУМЕНТ)

ВВЕДЕНИЕ

Методические рекомендации содержат перечень тем с вопросами для самостоятельной проработки, перечень лабораторных работ с вопросами для самостоятельной проработки, материал для подготовки рефератов.

Методические указания посвящены курсу «Защита информации от утечки по техническим каналам».

СОДЕРЖАНИЕ

Введение	Error! Bookmark not defined.
1. Цель и задачи изучения дисциплины	4
2. Темы самостоятельной работы	4
3. Технологическая карта самостоятельной работы обучающегося	4
4. Рекомендации для самоподготовки.....	5
4.1 Подготовка к лекциям. Самостоятельное изучение литературы	5
4.2 Подготовка к лабораторным работам	7
6. Учебно-методическое и информационное обеспечение дисциплины	9

1. ЦЕЛЬ И ЗАДАЧИ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

Целью дисциплины является обучение студентов основам многоканальных цифровых систем передачи и средствам их защиты.

Задачами дисциплины являются получение представления о:

- принципах организации цифровых линейных трактов (ЦЛТ);
- принципах временного группообразования (ВГ);
- методах синхронизации в ЦСП плезиохронной цифровой иерархии (ПЦИ);
- методах мультиплексирования;
- системах синхронизации и управления в ЦСП;
- синхронной цифровой иерархии (СЦИ);
- принципах защиты информации от несанкционированного доступа;
- принципах криптозащиты;
- скремблировании цифровых сигналов;
- принципах реализации устройств защиты на микропроцессорах.

2. ТЕМЫ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

№ темы	Наименование тем дисциплины, их краткое содержание	Объем часов*
	6 семестр	
2	Тема 2. Структурная схема оконечной станции ЦСП и основные узлы оборудования.	4,5
3	Тема 3. Построение линейного тракта (ЛТ) ЦСП.	9
4	Тема 4. Принципы временного группообразования (ВГ) в ЦСП плезиохронной цифровой иерархии (ПЦИ).	4,5
6	Тема 6. Канальное кодирование	4,5
7	Тема 7. Многостанционный доступ (МД)	4,5
8	Тема 8. Расширение спектра	9
9	Тема 9. Системы защиты информации с несимметричными ключами (двухключевые системы).	4,5
	Итого за 6 семестр	40,5

3. ТЕХНОЛОГИЧЕСКАЯ КАРТА САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩЕГОСЯ

Коды реализуемых компетенций	Вид деятельности студентов	Итоговый продукт самостоятельной работы	Средства и технологии и оценки	Объем часов, в том числе		
				СРС	Контактная работа с преподавателем	Всего
ПК-1, ПК-3	Изучение литературы по темам 1-9	Конспект	■ собеседование	27,95	3,25	31,2
ПК-1, ПК-3	проработка лекционного материала	Конспект	■ собеседование	1,21	0,14	1,35
ПК-1, ПК-3	подготовка к лабораторным	Отчет	■ отчет письменный	7,29	0,81	8,1

	м работам		ый			
Итого				36,45	4,05	40,5

4. РЕКОМЕНДАЦИИ ДЛЯ САМОПОДГОТОВКИ

4.1 Подготовка к лекциям. Самостоятельное изучение литературы

Базовый уровень

Тема 1

1. Понятия: телекоммуникационная система, система связи, система электросвязи, система радиосвязи, защищенная система связи
2. Классификация телекоммуникационных систем по типам передаваемых сообщений, от вида распространения радиоволн и по диапазонам несущих частот.
3. Понятия: информация, сообщение, сигнал. Виды сигналов, используемых в многоканальных телекоммуникационных системах.

Тема 2

1. Понятие канала связи. Виды каналов связи. Условие неискажённой передачи сигнала по каналу связи.
2. Основные элементы современной многоканальной телекоммуникационной системы.
3. Основные типы и структуры многоканальных телекоммуникационных систем и сетей.

Тема 3

1. Программное обеспечение телекоммуникационных систем.
2. Классификация защищенных многоканальных систем по виду канала связи.
3. Особенности построения многоканальных систем по видам каналов. Методы селекции каналов в многоканальных системах.

Тема 4

1. Методы разделения каналов и их особенности. Методы синхронизации многоканальных систем.
2. Особенности защиты информации в многоканальных системах.
3. Особенности временного разделения каналов.

Тема 5

1. Принципы организации многоканальных систем с ВРК.
2. Синхронизация в системах с ВРК.
3. Понятие кодирования. Назначение кодирования.

Тема 6

1. Особенности радиорелейной связи. Частотные диапазоны РРС.
2. Оборудование РРС.
3. Общие черты и различия систем сотовой и радиорелейной связи.

Тема 7

1. Синхронизация систем РРС.
2. Взаимодействие систем РРС с другими системами связи
3. Обслуживание РРС.

Тема 8

1. Особенности тропосферной связи.
2. Физические эффекты и явления, возникающие при тропосферной связи.
3. Особенности разделения каналов при тропосферной связи.

Тема 9

1. Аппаратные средства защиты.
2. Программные средства защиты.

3. Авторизация участников защищенной связи. Идентификация и аутентификация.

Повышенный уровень

Тема 1

1. Частотный диапазон для тропосферной связи. Затухания (замирания), задержки и помехи при тропосферной связи. Синхронизация при тропосферной связи.
2. Оборудование для тропосферной связи.

Тема 2

1. Основные технические характеристики и разновидности спутников связи.
2. Организация радиообмена спутников и наземных приёмо – передатчиков.

Тема 3

1. Организация скрытности радиовзаимодействия со спутниками.
2. Оборудование спутниковой связи. Стационарные компоненты.

Тема 4

1. Оборудование спутниковой связи. Мобильные компоненты.
2. Использование спутниковой связи в условиях чрезвычайных ситуаций.

Тема 5

1. Классификация методов и средств защиты информации в многоканальных цифровых системах передачи.
2. Организационные меры защиты информации.

Тема 6

1. Шифрование информации. Классификация методов шифрования.
2. Поточные шифры на примере шифра по ГОСТ 28147 – 89.

Тема 7

1. Алгебраические шифры. Способы построения.
2. Электронная цифровая подпись и границы ее использования.

Тема 8

1. Дополнительное оборудование для защиты информации. Оборудование для контроля перехватов информации.
2. Мероприятия по противодействию нарушениям информационной безопасности.

Тема 9

1. Метод прямой последовательности.
2. Методы скачкообразной перестройки частоты.

4.2 Подготовка к лабораторным работам

Лабораторная работа №1 «Принципы построения многоканальной системы передачи с частотным разделением каналов»

Базовый уровень

1. Дайте определение понятия «Канал связи».
2. Укажите назначение узлов многоканальной системы с разделением каналов по частоте (по структурной схеме системы).

Повышенный уровень

1. Для чего в МСП с ЧРК необходимо преобразование частоты?
2. Какова классификация способов передачи амплитудно-модулированных сигналов?

Лабораторная работа №2 «Изучение принципов построения аппаратуры многоканальной связи с разделением каналов по времени»

Базовый уровень

1. В чем заключается принцип временного уплотнения линий связи?
2. Исходя из каких соображений выбирается частота дискретизации (частота стробирования) канального сигнала во времени?

Повышенный уровень

1. Какое назначение узлов системы АИМ - ВР?
2. Для чего нужна синхронизация в системе АИМ - ВР?

Лабораторная работа №3 «Исследование электрических характеристик канала тональной частоты»

Базовый уровень

1. Дайте определение канала связи. Перечислите основные параметры и характеристики канала ТЧ. С какой целью их нормируют?
2. Какие точки на схеме разделяют: канал ТЧ и двухпроводное окончание; низкочастотную (тональную) и высокочастотную части аппаратуры?

Повышенный уровень

1. Что называется остаточным затуханием?
2. Что называется амплитудно-частотной характеристикой и как она измеряется?

Лабораторная работа №4. «Исследование дифференциальных систем»

Базовый уровень

1. Назначение дифференциальных систем.
2. Чем объяснить различие между расчетными и экспериментальными значениями затухания?

Повышенный уровень

1. Почему измеренные затухания α_{1-3} и α_{1-4} получились отличными от расчетных?
2. Каковы физические и аналитические условия развязки трансформаторной дифсистемы в направлениях от зажимов 1 - 1' к зажимам 2 - 2' и от зажимом 3 - 3' к зажимам 4 - 4'?

Лабораторная работа №5. «Изучение оконечной аппаратуры системы передачи к - 60п»

Базовый уровень

1. Построение первичной стандартной группы.
2. Назначение заграждающих фильтров ФЗ - 16, 112 и 248 кГц.

Повышенный уровень

1. Назначение контура предварительного наклона (КПН) в тракте приема.
2. Назначение линейного выравнивателя (ЛВ) и место его включения.

Лабораторная работа №6. «Изучение кодирующего устройства»

Базовый уровень

1. Назначение кодера.
2. Принцип работы компаратора.

Повышенный уровень

1. Поясните назначение импульсов "строб - 1", "строб - 2".

2. Что такое перегрузка кодера?

Лабораторная работа №7. «Исследование регенератора ЦСП»

Базовый уровень

1. Назначение регенератора ЦСП.

2. Как изменяются параметры импульсов при прохождении по линии канала связи?

Повышенный уровень

1. Назначение ВТЧ.

2. Принцип работы КУВ.

Лабораторная работа №8. «Необслуживаемый регенерационный пункт НРП-K12 системы передачи ИКМ-30»

Базовый уровень

1. Как конструктивно выполнен НРП-K12?

2. Сколько блоков РЛ размещается в НРП-K12?

Повышенный уровень

1. Как осуществляется соединение НРП-K12 с магистральным кабелем?

2. Где устанавливается НРП-K12?

Лабораторная работа №9 «Технические средства защиты информации в телефонных линиях»

Базовый уровень

1. Назовите методы подавления телефонных закладных устройств.

2. Какие степени защиты передаваемых сообщений обеспечивает «ГРОТ» в режиме защиты передаваемых сообщений по всей линии связи ТС.

Повышенный уровень

1. Назначение прибора «ПРОКРУСТ-2000».

2. Опишите порядок выполнения работы с телефонным скремблером «ГРОТ».

5. ТЕОРЕТИЧЕСКИЙ МАТЕРИАЛ

1. Тема. Общие принципы построения многоканальных цифровых систем передачи (ЦСП).

Методы цифровой обработки сигналов и виды цифровой модуляции. Иерархический принцип построения ЦСП.

2. Тема. Структурная схема оконечной станции ЦСП и основные узлы оборудования. Формирование структуры цикла передачи и системы синхронизации ЦСП.

3. Тема. Построение линейного тракта (ЛТ) ЦСП.
Коды в различных типах ЛТ ЦСП. Регенерация сигналов в ЦЛТ.

4. Тема. Принципы временного группообразования (ВГ) в ЦСП плезиохронной цифровой иерархии (ПЦИ).
Синхронная цифровая иерархия (СЦИ), схема мультиплексирования.

5. Тема. Общие принципы защиты информации от несанкционированного доступа. Системы защиты информации с симметричными ключами (одноключевые системы).

6. Тема. Канальное кодирование.
Назначение и способы. Оптимальные системы сигналов для передачи в постоянном канале с белым шумом. Сигнально-кодовые конструкции. Симплексные коды, коды Адамара, биортогональные коды.

Линейные блочные коды. Циклические коды, техника кодирования и декодирования. Коды Хэмминга, БЧХ, Рида-Соломона. Объединение кодов: композиционные и каскадные коды, турбо-коды. Перемежение символов во времени и по частоте при наличии пакетов ошибок. Кодирование при записи на CD.

Сверточные коды. Техника кодирования. Методы декодирования: максимума правдоподобия, пороговый, последовательный, алгоритм декодирования Витерби.

7. Тема. Многостанционный доступ (МД)

Способы разделения каналов при МД: частотный, временной, кодовый. Методы МД в сотовых системах стандартов NMT-450, GSM и CDMA, а также в спутниковых системах Intelsat, Iridium, Globalstar.

8. Тема. Расширение спектра

Цели и методы, типичные заблуждения. Метод прямой последовательности. Методы скачкообразной перестройки частоты. Роль синхронизации приемника сигнала с расширенным спектром.

9. Тема. Системы защиты информации с несимметричными ключами (двухключевые системы).

Генерация и распространение ключей. Реализация принципов криптозащиты на основе средств микропроцессорной техники.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1. Перечень основной и дополнительной литературы, необходимой для освоения дисциплины

6.1.1. Перечень основной литературы

1. Гафнер В. В. Информационная безопасность : учеб.пособие /В.В. Гафнер. — Ростов н/Д : Феникс, 2010. — 324 с.

2. Программно-аппаратная защита информации: учеб.пособие/ П. Б. Хорев.- М.: Форум, 2012.- 352 с.

6.1.2. Перечень дополнительной литературы

1. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др.; Технические средства и методы защиты информации: Учебник для вузов / под ред. А.П. Зайцева и А.А. Шелупанова. - М.: ООО "Издательство Машиностроение", 2009. - 508 с.

2. Защита информации в операционных системах: учеб.пособие.- Ставрополь: Изд-во СГУ, 2008.- 318 с

6.2. Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

1. Методические указания по организации и проведению самостоятельной работы по дисциплине Многоканальные цифровые системы передачи и средства их защиты.

2. Методические указания по выполнению лабораторных работ по дисциплине Многоканальные цифровые системы передачи и средства их защиты

6.3. Перечень ресурсов информационно-телекоммуникационной сети Интернет, необходимых для освоения дисциплины

1. <http://biblioclub.ru>

2. <http://elibrary.ru/>