МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

УТВЕРЖДАЮ
Проректор по учебной работе
_____ О.Г. Локтионова
«__» _____ 2022 г.

ЗАЩИТА ИНФОРМАЦИИ В СИСТЕМАХ БЕСПРОВОДНОЙ СВЯЗИ

Методические рекомендации для самостоятельной подготовки к занятиям студентов направлений подготовки, учебные планы которых предусматривают изучение дисциплины «Защита информации в системах беспроводной связи» очной формы обучения

Курск 2022

УДК 004.056.53

Составитель М.А. Ефремов

Рецензент
Кандидат технических наук, доцент *А.Л. Марухленко*

Защита информации в системах беспроводной связи: методические рекомендации для самостоятельной подготовки к занятиям студентов направлений подготовки, учебные планы которых предусматривают изучение дисциплины «Защита информации в системах беспроводной связи» / Юго-Зап. гос. ун-т; сост.: М.А. Ефремов. Курск, 2022. - 18 с.

Содержат информацию, необходимую студентам в процессе самостоятельной подготовки к занятиям по дисциплине.

Методические рекомендации соответствуют требованиям программы, утвержденной учебно-методическими объединениями по специальностям.

Предназначены для студентов направлений подготовки, учебные планы которых предусматривают изучение дисциплины «Защита информации в системах беспроводной связи», очной формы обучения.

Текст печатается в авторской редакции

Подписано в печать Формат 60х84 1/16
Усл.печ.л. 1,10 Уч.-изд.л. 1,00 Заказ 902 Тираж 100 экз. Бесплатно
Юго-Западный государственный университет
305040, г. Курск, ул. 50 лет Октября, 94

ПРЕДИСЛОВИЕ

Методические рекомендации разработаны с целью оказания помощи студентам направлений подготовки, учебные планы которых предусматривают изучение дисциплины «Защита информации в системах беспроводной связи», очной формы обучения, при самостоятельной подготовке к занятиям по дисциплине.

Методические рекомендации разработаны в соответствии с Федеральными государственными образовательными стандартами высшего образования соответствующих направлений подготовки.

Предлагаемые методические рекомендации содержат краткое содержание рассматриваемых тем дисциплины и задания для самоконтроля в форме вопросов.

Студентам предлагается список учебной литературы по дисциплине и перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для самостоятельной подготовки к занятиям.

Методические указания для обучающихся по освоению дисциплины

Основными видами аудиторной работы обучающихся являются лекции и практические занятия.

В ходе лекций преподаватель излагает и разъясняет основные, наиболее сложные понятия темы, а также связанные с ней теоретические и практические проблемы, дает рекомендации на практическое занятие и указания на самостоятельную работу.

Практические занятия завершают изучение наиболее важных тем учебной дисциплины. Они служат для закрепления изученного материала, развития умений и навыков подготовки докладов, сообщений, приобретения опыта устных публичных выступлений, ведения дискуссии, аргументации и защиты выдвигаемых положений, а также для контроля преподавателем степени подготовленности студентов по изучаемой дисциплине.

Практические занятия предполагают свободный обмен мнениями по избранной тематике. Занятие начинается со вступительного слова преподавателя, формулирующего цель занятия и характеризующего его основную проблематику. Затем, как правило, заслушиваются сообщения студентов. Обсуждение сообщения совмещается с рассмотрением намеченных вопросов. Сообщения, предполагающие анализ публикаций по отдельным вопросам семинара, заслушиваются обычно в середине занятия. Поощряется выдвижение и обсуждение альтернативных мнений. В заключительном слове преподаватель подводит итоги обсуждения и объявляет баллы выступавшим студентам. В целях контроля подготовленности студентов и привития им навыков краткого письменного изложения своих мыслей преподаватель в ходе практических занятий может осуществлять текущий контроль знаний в виде тестовых заданий.

При подготовке к занятию студенты имеют возможность воспользоваться консультациями преподавателя. Кроме указанных тем, студенты вправе, по согласованию с преподавателем, избирать и другие интересующие их темы.

Качество учебной работы студентов преподаватель оценивает в конце занятия.

При освоении данного курса студент может пользоваться библиотекой вуза, которая в полной мере обеспечена соответствующей литературой.

В процессе *подготовки к зачету* студенту следует руководствоваться следующими рекомендациями:

- необходимо стремиться к пониманию всего материала, чтобы еще до экзамена не оставалось непонятных вопросов;
- необходимо строго следить за точностью своих выражений и правильностью употребляемых терминов;
- не следует опасаться дополнительных вопросов – чаще всего преподаватель использует их как один из способов помочь студенту или сэкономить время;
- прежде чем отвечать на вопрос, необходимо сначала правильно его понять.

Содержание дисциплины, структурированное по темам (разделам)

Таблица 1 – Содержание дисциплины, структурированное по темам (разделам)

№ п/п	Раздел (тема) дисциплины	Содержание
1.	Краткий обзор систем беспроводной связи	Общая характеристика систем электросвязи: системы проводной и беспроводной связи. Принципиальное отличие радиосистем передачи информации от проводных систем. Диапазоны частот радиосистем. Симплексная, полудуплексная и дуплексная радиосвязь. Классификация систем беспроводной связи. Системы узкополосной радиосвязи: радионаправление и радиосеть, системы прямой радиосвязи и системы с переотражением. Системы широкополосной радиосвязи: системы прямой радиосвязи и радиорелейные системы. Основные аспекты инфокоммуникационной безопасности СБС: доступность, целостность и конфиденциальность. Основные угрозы аспектам инфокоммуникационной безопасности СБС.
2.	Основы радиоэлектронной бизнесс-разведки	Основы радиоэлектронной бизнес-разведки. Демаскирующие признаки объектов и действий. Назначение, задачи и особенности радиоэлектронной бизнес-разведки. Характеристика

		видов радиоэлектронной бизнес-разведки. Радиоразведка и радиотехническая разведка. Помехи, классификация помех и их влияние на функционирование радиоэлектронных средств.
3.	Основы радиоэлектронной борьбы и радиоэлектронного подавления	Радиоэлектронная борьба и радиоэлектронное подавление. Пассивные и активные целенаправленные радиопомехи, выбор структуры радиопомех, маскирующие и имитирующие радиопомехи.
4.	Радиоэлектронное подавление	Радиоподавление, эффективность радиоэлектронного подавления, условия эффективного радиоподавления, показатели и критерии его эффективности.
5.	Последовательность расчета *Rn*	Радиоподавление, эффективность радиоэлектронного подавления, условия эффективного радиоподавления, показатели и критерии его эффективности.
6.	Нарушения нормального функционирования средств беспроводной связи	Общие методы и средства защиты беспроводных систем связи от радиоэлектронного подавления, четыре основных требования к защищенности беспроводной системы связи. Методы защиты радиосистем от средств бизнес-разведки: крипто- и имитозащита сообщений.
7.	Помехозащита радиолиний	Методы сигнальной помехозащиты: уравнение помехозащиты, применение методов фильтрации и программной перестройки частоты, функциональная схема помехозащищенной радиолинии.
8.	Безопасность спутниковой связи	Безопасность спутниковой связи: общая характеристика систем спутниковой связи, основные угрозы безопасности, методы и средства защиты.
9.	Спутниковые технологии VSAT и информационная безопасность сети	Информационная безопасность радиорелейной связи: общая характеристика систем радиорелейной связи, основные угрозы безопасности, методы и средства защиты.
10.	Информационная безопасность сотовой связи GSM	Информационная безопасность узкополосных систем сотовой связи: общая характеристика систем сотовой связи, основные угрозы безопасности, методы и средства защиты.
11.	Обеспечение секретности абонента	Обеспечение секретности абонента. Угрозы информационной безопасности при использовании сотовых систем связи. Нарушение связи в сотовых сетях. Нарушение конфиденциальности информации, передаваемой в сотовых сетях связи. Клонирование SIM-карты.

12.	Инфобезопасность транкинговых систем связи	Информационная безопасность узкополосных систем транкинговой связи: общая характеристика систем транкинговой связи, основные угрозы безопасности, методы и средства защиты.
13.	Стандарт TETRA	Распределение сеансовых ключей аутентификации по базовым станциям. Алгоритм аутентификации пользователей с применением сеансовых ключей. Возможности по разграничению доступа к передаваемой информации. Четыре алгоритма шифрования (TEA1 – TEA4). Поточный метод шифрования.
14.	Безопасность широкополосных систем радиосвязи	Информационная безопасность широкополосных систем радиосвязи: общая характеристика систем широкополосной радиосвязи, основные угрозы безопасности, методы и средства защиты.
15.	Виды удаленных атак на устройства с поддержкой Bluetooth	Классификация видов удаленных атак. Атака типа bluesnarfing. Защита от атак на широкополосную систему беспроводной передачи данных.
16.	Защита сетей Wi-Fi	Особенности беспроводной связи с точки зрения безопасности. Риски безопасности. Легкость в развертывании и мобильность. Особенности атаки.
17.	Обеспечение безопасного функционирования беспроводных сетей. Риски.	Четыре риска безопасности. Разведка. Имперсонация и Identity Theft.
18.	Отказы в обслуживании.	Специализированные инструменты атакующего. Denial of Service, DoS. Активность в нерабочее время. Скорости. Интерференция. Связь.

Задания для самоконтроля по темам курса

Тема 1. Краткий обзор систем беспроводной связи.

1. Что такое системы электросвязи, и на какие виды они делятся в зависимости от среды распространения?

2. Какую полосу частот занимают диапазоны частот радиосистем?

3. Какие бывают виды радиосвязи?

4. Перечислите основные факторы, оказывающие влияние на величину напряженности поля в точке приема.

5. На какие системы делятся СБС по типу используемой технологии?

6. Что такое радиосеть?

Тема 2. Основы радиоэлектронной бизнес-разведки.

1. Перечислите демаскирующие признаки объекта бизнес-разведки.

2. Что такое тепловое излучение?

3. Для чего применяется радиоэлектронная разведка?

4. Какие задачи решает радиоэлектронная разведка?

5. Что дает анализ результатов радиоэлектронной разведки?

6. Как радиотехническая разведка получает информацию о технических средствах бизнес-конкурента?

Тема 3. Основы радиоэлектронной борьбы и радиоэлектронного подавления.

1. Дайте определение помехе.

2. При каких условиях возникают неорганизованные радиопомехи?

3. Что такое взаимные помехи?

4. Как создаются организованные радиопомехи?

5. Что такое целостность информации?

6. Что такое защита конфиденциальности?

Тема 4. Радиоэлектронное подавление.

1. Что такое радиоэлектронное подавление?

2. Что такое эффективность радиоподавления?

3. Перечислите условия эффективного радиоподавления.

4. Что такое коэффициент радиоподавления?

5. Перечислите факторы, от которых зависит коэффициент радиоподавления.

6. Что такое электромагнитная доступность?

Тема 5. Последовательность расчета R_n.

1. Порядок последовательности расчета R_n.

2. Пространственное условие возможности РП радиосвязи.

3. Коэффициент рельефа.

4. Магнитная и диэлектрическая проницаемость среды.

Тема 6. Нарушения нормального функционирования средств беспроводной связи.

1. Что такое радиоэлектронная борьба?

2. Что такое радиоэлектронное подавление?

3. Назовите условия возникновения пассивных организованных радиопомех.

4. Чем определяется структура пассивного помехового сигнала?

5. От чего зависит эффективность маскирующих радиопомех?

6. В чем суть имитозащиты?

Тема 7. Помехозащита радиолиний.

1. Что такое помехоустойчивость?

2. На какие классы разделяется помехозащита?

3. Принцип работы сигнальной помехозащиты?

4. Чем определяется вероятность ошибки на бит?

5. Как можно повысить помехозащищенность радиолинии?

6. Как подавить ретранслированные помехи?

Тема 8. Безопасность спутниковой связи.

1. Перечислите основные службы (в соответствии с Регламентом радиосвязи)?

2. Перечислите основные достоинства при размещении спутников на геостационарной орбите.

3. Что такое фиксированные системы спутниковой связи?

4. Перечислите основные отличительные особенности подвижных систем связи второго поколения.

5. Перечислите этапы получения информационного доступа.

6. Назовите частоты диапазона Ka.

Тема 9. Спутниковые технологии VSAT и информационная безопасность сети.

1. Что такое VSAT?

2. Назовите недостатки спутниковых систем связи.

3. Дайте определение обратному спутниковому каналу.

4. Назовите основной способ обеспечения безопасности передачи данных в беспроводном спутниковом канале.

5. Где располагается специальная база данных ключей шифрования?

6. Дайте определение прямому спутниковому каналу.

Тема 10. Информационная безопасность сотовой связи GSM.

1. Что из себя представляет стандарт GSM?

2. К сетям какого поколения относится стандарт GSM?

3. Перечислите подсистемы сети GSM.

4. Какую функцию выполняет центр коммутации?

5. Для чего нужен регистр идентификации оборудования?

6. Перечислите механизмы безопасности стандарта GSM.

Тема 11. Обеспечение секретности абонента.

1. Перечислите основные угрозы информационной безопасности при использовании систем сотовой связи.

2. Перечислите возможные последствия от воздействия вредоносных программ (вирусов)

3. Как можно противодействовать использованию сотовых аппаратов как средств ведения технической разведки и как устройства дистанционного управления?

4. Какова максимальная дальность перехвата информации, передаваемой в сетях сотовой связи?

5. Перечислите алгоритмы защиты информации, применяемых в сетях GSM

6. Перечислите варианты получения злоумышленником KI.

Тема 12. Инфобезопасность транкинговых систем связи.

1. Время установления связи в стандарте TETRA?

2. Назовите 3 вида услуг передачи данных, предлагаемых пользователю при использовании стандарта TETRA.

3. Перечислите основные требования, предъявляемые к стандарту TETRA R2.

4. Дайте определение защиты информации, применительно к стандарту TETRA.

5. Как реализуется механизм аутентификации в стандарте TETRA?

6. В каком году и где прошел TETRA World Congress 2000?

Тема 13. Стандарт TETRA.

1. Какие функции у центра аутентификации?

2. По какому алгоритму в мобильном терминале вычисляется значение сеансового ключа KS?

3. Когда активизируется процесс шифрования в стандарте TETRA?

4. Как реализуется шифрование речи в стандарте TETRA?

5. Какой метод шифрования используется в стандарте TETRA?

6. Что такое статические ключи?

Тема 14. Безопасность широкополосных систем радиосвязи.

1. Что такое Bluetooth?

2. Какое максимальное число устройств, объединенных в одну пикосеть?

3. Перечислите и поясните угрозы безопасности, реализуемых через Bluetooth-интерфейс?

4. Что может сделать злоумышленник с устройством, над которым он получил дистанционный контроль?

5. Какое максимальное число устройств может быть объединено технологией Bluetooth?

6. В каком частотном диапазоне работает система Bluetooth?

Тема 15. Виды удаленных атак на устройства с поддержкой Bluetooth.

1. Что такое Bluejacking?
2. Что такое Bluesnarfing?
3. Что такое Bluebugging?
4. Что такое Bluetracking?
5. Перечислите основные рекомендации, позволяющие обезопасить себя при использовании технологии Bluetooth.
6. Какова дальность действия технологии Bluetooth?

Тема 16. Защита сетей Wi-Fi.

1. Какая среда распространения информации считается «контролируемой»?
2. Какая среда распространения информации считается «неконтролируемой»?

Тема 17. Обеспечение безопасного функционирования беспроводных сетей. Риски.

1. Чем опасны устройства-чужаки?
2. Поясните суть нефиксированной природы связи.
3. Какой промежуток времени требуется злоумышленнику для сбора данных и дальнейшего восстановления ключа шифрования стандарта WEP?
4. Как производится разведка?
5. Что такое имперсонация?
6. В чем опасность некорректно сконфигурированных точек доступа?

Тема 18. Отказы в обслуживании.

1. Какова задача атаки «Отказ в обслуживании»?

2. Перечислите варианты утечки информации из проводной сети.

3. В чем выражается влияние интерференции?

Учебная литература, необходимая для самостоятельной подготовки к занятиям

1) Сети и системы передачи информации: телекоммуникационные сети [Текст]: учебник и практикум для вузов : [для студентов, обуч. по инженерно-техническим направлениям и специальностям] / К. Е. Самуйлов, И. А. Шалимов, Д. С. Кулябов ; Российский университет дружбы народов. - Москва : Юрайт, 2017. - 363 с. Операционные системы :[Текст] : учебник / С. В. Синицын, А. В. Батаев, Н. Ю. Налютин. – 2-е изд., испр. – М.: Академия, 2012. – 304 с.

2) Технологии коммутации и маршрутизации в локальных компьютерных сетях [Текст] : учебное пособие / под общ. ред. А. В. Пролетарского. - Москва : Изд - во МГТУ им. Н. Э. Баумана, 2013. - 389, [3] с. : ил.

3) Технологии защиты информации в компьютерных сетях. Межсетевые экраны и интернет-маршрутизаторы [Текст] : учебное пособие / Е. А. Богданова [и др.]. - Москва : Национальный Открытый Университет "ИНТУИТ", 2013. - 743 с.

4) Олифер, Виктор Григорьевич. Компьютерные сети. Принципы, технологии, протоколы [Текст] : учебник для вузов / В. Г. Олифер, Н. А. Олифер. - 4-е изд. - Санкт-Петербург : Питер, 2015. - 943 с.

5) Крук, Борис Иванович. Телекоммуникационные системы и сети [Текст] : учебное пособие / Б. И. Крук, В. Н. Попантонопуло, В. П. Шувалов ; под ред. В. П. Шувалова. - 4-е изд., испр. и доп. - Москва : Горячая линия - Телеком. Т. 1 : Современные технологии. - 2013. - 620 с. : ил.

6) Богомолов, С. И. Введение в системы радиосвязи и радиодоступа [Электронный ресурс] : учебное пособие / С. И. Богомолов. - Томск : Эль Контент, 2012. - 152 с.

7) Винокуров, В. М. Цифровые системы передачи [Электронный ресурс] : учебное пособие / В. М. Винокуров. - Томск : Томский государственный университет систем управления и радиоэлектроники, 2012. - 160 с.

8) Технические средства и методы защиты информации [Текст] : учебное пособие / под ред. А. П. Зайцева и А. А. Шелупанова. - Москва : Горячая линия - Телеком, 2012. - 616 с. : ил.

9) Информационная безопасность и защита информации [Текст] : учебное пособие / Ю. Ю. Громов [и др.]. - Старый Оскол : ТНТ, 2013. - 384 с.

10) Подавление радиосигнала радиопомехой: методические указания по выполнению лабораторной работы по дисциплине «Защита информации в системах беспроводной связи» / Юго-Зап. гос. ун-т; сост.: В.Л. Лысенко, М.А. Ефремов. Курск, 2017. 6 с.: ил., Библиогр.: с. 6..

11) Исследование метода защиты речевых сигналов от воздействия широкополосных аддитивных помех: методические указания по выполнению лабораторной работы по дисциплине

«Защита информации в системах беспроводной связи» / Юго-Зап. гос. ун-т; сост.: В.Л. Лысенко, М.А. Ефремов. Курск, 2017. 13 с.. Библиогр.: с. 13..

12) Исследование методов защиты абонентского терминала в системе сотовой связи GSM: методические указания по выполнению лабораторной работы по дисциплине «Защита информации в системах беспроводной связи» / Юго-Зап. гос. ун-т; сост.: В.Л. Лысенко, М.А. Ефремов. Курск, 2017. 10 с.: Библиогр.: с. 10.

13) Исследование методов защиты абонентского терминала сотовой связи GSM в системе Android: методические указания по выполнению лабораторной работы по дисциплине «Защита информации в системах беспроводной связи» / Юго-Зап. гос. ун-т; сост.: В.Л. Лысенко, М.А. Ефремов. Курск, 2017. 10 с.: Библиогр.: с. 10.

14) Исследование методов защиты терминала беспроводной связи Bluetooth: методические указания по выполнению лабораторной работы по дисциплине «Защита информации в системах беспроводной связи» / Юго-Зап. гос. ун-т; сост.: В.Л. Лысенко, М.А. Ефремов. Курск, 2017. 9 с.: Библиогр.: с. 8.

15) Оценка возможности эффективного функционирования средств радиосвязи условиях их радиоподавления: методические указания по выполнению практической работы по дисциплине «Защита информации в системах беспроводной связи» / Юго-Зап. гос. ун-т; сост.: В.Л. Лысенко, М.А. Ефремов. Курск, 2017. 12 с.: ил., Библиогр.: с. 12.

16) Методы защиты информации в средствах беспроводной радиосвязи от нарушения конфиденциальности: методические указания по выполнению практической работы по дисциплине «Защита информации в системах беспроводной связи» / Юго-Зап. гос. ун-т; сост.: В.Л. Лысенко, М.А. Ефремов. Курск, 2017. 12 с.: ил., Библиогр.: с. 12.

17) Защита информации в системах беспроводной связи путем имитозащиты передаваемых сообщений: методические указания по выполнению практической работы по дисциплине «Защита информации в системах беспроводной связи» / Юго-Зап. гос. ун-т; сост.: В.Л. Лысенко, М.А. Ефремов. Курск, 2017. 8 с.: ил., Библиогр.: с. 8.

18) Методы сигнальной помехозащиты радиолиний: методические указания по выполнению практической работы по дисциплине «Защита информации в системах беспроводной связи» / Юго-Зап. гос. ун-т; сост.: В.Л. Лысенко, М.А. Ефремов. Курск, 2017. 10 с.: ил., Библиогр.: с. 10.

19) Оценка помехозащиты спутниковой линии связи: методические указания по выполнению практической работы по дисциплине «Защита информации в системах беспроводной связи» / Юго-Зап. гос. ун-т; сост.: В.Л. Лысенко, М.А. Ефремов. Курск, 2017. 6 с. Библиогр.: с. 6.

20) Оценка эффективности применения методов повышения скрытности РЭС: методические указания по выполнению практической работы по дисциплине «Защита информации в

системах беспроводной связи» / Юго-Зап. гос. ун-т; сост.: В.Л. Лысенко, М.А. Ефремов. Курск, 2017. 14 с. Библиогр.: с. 14.

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для самостоятельной подготовки к занятиям по дисциплине

1. Электронная библиотека ЮЗГУ (http://www.lib.swsu.ru)
2. Электронно-библиотечная система «Университетская библиотека online»
3. (http://www.biblioclub.ru)
4. Федеральное хранилище Единая коллекция цифровых образовательных ресурсов (http://school-collection.edu.ru)
5. Федеральный портал Российское образование (http://www.edu.ru)
6. Электронная библиотека образовательных и просветительных изданий (http://www.iqlib.ru)
7. Научная электронная библиотека «Elibrary» (http://elibrary.ru/defaultx.asp)
8. Официальный сайт компании «Консультант Плюс» (http://www.consultant.ru)