

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Таныгин Максим Олегович
Должность: и.о. декана факультета фундаментальной информатики и информатики
Дата подписания: 06.10.2022 12:34:24
Уникальный программный ключ:
65ab2aa0d384efe8480e6a4c688eddbc475e411a

Аннотация к рабочей программе дисциплины «Информационная безопасность ТК систем»

Цель преподавания дисциплины

Целью преподавания дисциплины «Информационная безопасность телеком-муникационных систем» (ИБТКС) сформировать основы знаний по принципам построения телекоммуникационных систем (ТКС), а также ознакомление с методами, средствами и системами обеспечения их информационной безопасности.

1.2 Задачи изучения дисциплины

Основными задачами изучения дисциплины является: определение места и значения ИБТКС в системе принятия хозяйственных решений и её роли как превентивного механизма предупреждения негативных последствий вредоносных воздействий объективного и субъективного характера на функционирование ТКС; ознакомление с принципами передачи сообщений в основных сетях связи, ознакомление с основами информационной безопасности систем и сетей связи, ознакомление с методами несанкционированного извлечения информации из сигналов и сообщений различных систем связи.

Знания и умения, которыми должен обладать студент, успешно освоивший данную дисциплину: знание уязвимостей основных телекоммуникационных технологий, средств и методов обеспечения их информационной безопасности, умение анализировать безопасность функционирования ТКС, а также оценивать уязвимость их протоколов и интерфейсов.

Компетенции, формируемые в результате освоения дисциплины

способностью осуществлять анализ научно-технической информации, нормативных и методических материалов по методам обеспечения информационной безопасности телекоммуникационных систем (ПК-1);

способностью выполнять установку, настройку, обслуживание, диагностику, эксплуатацию и восстановление работоспособности телекоммуникационного оборудования и приборов, технических и программно-аппаратных средств защиты телекоммуникационных сетей и систем (ПК-14);

способностью применять положения теорий электрических цепей, радиотехнических сигналов, распространения радиоволн, цифровой обработки сигналов, информации и кодирования, электрической связи для

решения профессиональных задач (ОПК-3)

Разделы дисциплины

Введение. Информация, основные информационные процессы, классификация информации. Основные понятия информационной безопасности ТКС. Понятие о криптографической защите информации в ТКС. Информационная безопасность глобальной сети Интернет. Информационная безопасность систем телефонной связи. Информационная безопасность систем волоконно-оптической связи. Информационная безопасность автоматизированных систем управления.

МИНОБРНАУКИ РОССИИ

Юго-Западный государственный университет

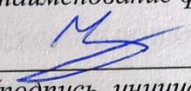
УТВЕРЖДАЮ:

Декан факультета


фундаментальной и прикладной

информатики

(наименование факультета полностью)

 Т.А. Ширабакина

(подпись, инициалы, фамилия)

« 1 »  2017 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Информационная безопасность телекоммуникационных систем

(наименование дисциплины)

направления подготовки (специальность)

10.05.02

(шифр согласно ФГОС)

«Информационная безопасность телекоммуникационных систем»

и наименование направления подготовки (специальности)

«Защита информации в системах связи и управления»

наименование профиля, специализации или магистерской программы

форма обучения

очная

(очная, очно-заочная, заочная)

Рабочая программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования направления подготовки 10.05.02 Информационная безопасность телекоммуникационных систем и на основании учебного плана направления подготовки 10.05.02 Информационная безопасность телекоммуникационных систем, одобренного Учёным советом университета, протокол № 5 «30» 01 2017г.

Рабочая программа обсуждена и рекомендована к применению в учебном процессе для обучения студентов по направлению подготовки 10.05.02 Информационная безопасность телекоммуникационных систем на заседании кафедры информационной безопасности № 9 «01» 02 2017г.

Зав. кафедрой ИБ



Таныгин М.О.

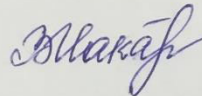
Разработчик программы



Лысенко В.Л.

Согласовано:

Директор научной библиотеки



Макаровская В.Г.

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.05.02 Информационная безопасность телекоммуникационных систем, одобренного Ученым советом университета протокол № 5 «30» 01 2017г. на заседании кафедры информационной безопасности 28.08.2017г. прот. № 1
(наименование кафедры, дата, номер протокола)

Зав. кафедрой

к.т.н., доцент Таныгин М.О.

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.05.02 Информационная безопасность телекоммуникационных систем, одобренного Ученым советом университета протокол № 5 «30» 01 2017г. на заседании кафедры информационной безопасности 29.06.2018г. прот. № 2
(наименование кафедры, дата, номер протокола)

Зав. кафедрой

к.т.н., доцент Таныгин М.О.

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.05.02 Информационная безопасность телекоммуникационных систем, одобренного Ученым советом университета протокол № « » 20 г. на заседании кафедры информационной безопасности 27.06.2019г. прот. № 11
(наименование кафедры, дата, номер протокола)

Зав. кафедрой

к.т.н., доцент Таныгин М.О.

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.05.02 – «Информационная безопасность телекоммуникационных систем», одобренного Ученым советом университета протокол № 7 «25» 02 2020 г. на заседании кафедры информационной безопасности. Протокол № 1 от «31» 08 2020 г.

Зав. кафедрой _____

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.05.02 – «Информационная безопасность телекоммуникационных систем», одобренного Ученым советом университета протокол № 7 «25» 02 2020 г. на заседании кафедры информационной безопасности. Протокол № 11 от «28» 06 2021 г.

Зав. кафедрой _____

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.05.02 – «Информационная безопасность телекоммуникационных систем», одобренного Ученым советом университета протокол № 7 «25» 02 2020 г. на заседании кафедры информационной безопасности. Протокол № 11 от «30» 06 2022 г.

Зав. кафедрой _____

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.05.02 – «Информационная безопасность телекоммуникационных систем», одобренного Ученым советом университета протокол №__ «__» ____ 20__ г. на заседании кафедры информационной безопасности. Протокол №__ от «__» ____ 20__ г.

Зав. кафедрой _____

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.05.02 – «Информационная безопасность телекоммуникационных систем», одобренного Ученым советом университета протокол №__ «__» ____ 20__ г. на заседании кафедры информационной безопасности. Протокол №__ от «__» ____ 20__ г.

Зав. кафедрой _____

1. Цель и задачи дисциплины. Перечень планируемых результатов обучения, соотнесённых с планируемыми результатами освоения образовательной программы

1.1. Цель преподавания дисциплины

Дисциплина «Информационная безопасность телекоммуникационных систем» является получение студентами знаний о принципах обеспечения

информационной безопасности в телекоммуникационных системах, методах оценки и защиты безопасности систем связи.

1.2. Задачи изучения дисциплины

В результате изучения дисциплины студенты должны:

- получить знания об основных понятиях информационной безопасности телекоммуникационных систем;
- получить знания об угрозах информационной безопасности и их классификации;
- получить знания о методах оценки телекоммуникационных систем;
- получить знания о системах электросвязи, угрозах их безопасности и методах защиты;
- получить знания о защите речевой информации в канале связи путем преобразования сигнала;
- получить знания об информационной безопасности телефонной связи;
- получить знания о современных криптографических алгоритмах;
- получить знания о защите информации в системах волоконно-оптической связи;
- получить знания о виртуальных частных сетях.

1.3. Перечень планируемых результатов обучения, соотнесённых с планируемыми результатами освоения образовательной программы

Обучающиеся должны **знать:**

- общие характеристики телекоммуникационных систем;
- основные аспекты инфокоммуникационной безопасности телекоммуникационных систем;
- основные угрозы аспектам инфокоммуникационной безопасности телекоммуникационных систем связи;

уметь:

- оценивать уровень безопасности телекоммуникационных систем;
- классифицировать угрозы безопасности и их влияние на работу телекоммуникационных систем;

владеть:

- методами защиты информации систем связи;
- методами защиты речевой информации в канале связи путем преобразования сигнала.

Процесс изучения дисциплины направлен на формирование следующих компетенций:

- способность применять положения теорий электрических цепей, радиотехнических сигналов, распространения радиоволн, цифровой обработки

сигналов, информации и кодирования, электрической связи для решения профессиональных задач (ОПК-3);

– способность осуществлять анализ научно-технической информации, нормативных и методических материалов по методам обеспечения информационной безопасности телекоммуникационных систем (ПК-1);

– способность выполнять установку, настройку, обслуживание, диагностику, эксплуатацию и восстановление работоспособности телекоммуникационного оборудования и приборов, технических и программно-аппаратных средств защиты телекоммуникационных сетей и систем (ПК-14)

2. Указание места дисциплины в структуре образовательной программы

Дисциплина относится к базовой части теоретического курса (Б1.Б.26). Изучается на 4 курсе в 8 семестре.

3. Объем дисциплины в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоёмкость (объём) дисциплины составляет 3 зачётные единицы, 108 академических часов.

Таблица 3.1 – Объём дисциплины по видам учебных занятий

| | |
|---|-----------------|
| Общая трудоёмкость дисциплины | 108 |
| Контактная работа обучающихся с преподавателем (по видам учебных занятий) (всего) | 36,1 |
| лекции | 18 |
| лабораторные занятия | 0 |
| практические занятия | 18 |
| экзамен | Не предусмотрен |
| зачет | 0,1 |
| курсовая работа (проект) | Не предусмотрен |
| расчетно-графическая (контрольная) работа | Не предусмотрен |
| Аудиторная работа (всего): | 36,1 |
| в том числе: | |
| лекции | 18 |
| лабораторные занятия | 0 |
| практические занятия | 18 |

| | |
|--|------|
| Самостоятельная работа обучающихся (всего) | 35,9 |
| Контроль/экза (подготовка к экзамену) | 0 |

4. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1. Содержание дисциплины

Таблица 4.1 – Содержание дисциплины, структурированное по темам (разделам)

| № п/п | Раздел (тема) дисциплины | Содержание |
|-------|--|--|
| 1. | Основные положения, предмет дисциплины «Информационная безопасность телекоммуникационных систем» | Понятие информации, конфиденциальная и открытая информация, информационная безопасность, защита информации, утечка информации, защита информации от несанкционированного доступа, телекоммуникационные системы, отличие дисциплин «Информационная безопасность» и «Информационная безопасность телекоммуникационных систем». |
| 2. | Доктрина информационной безопасности РФ | Доктрина информационной безопасности Российской Федерации, типы угроз информационной безопасности Российской Федерации, правовые, организационно-технические и экономические методы обеспечения ИБ РФ. |
| 3. | Угрозы информационной безопасности ТКС | Угроза, атака, злоумышленник, уязвимость ТКС, окно опасности, классификация угроз по аспекту информационной безопасности, основные угрозы доступности, основные угрозы целостности, основные угрозы конфиденциальности |
| 4. | Классификация угроз по компонентам ТКС | Три класса угроз передачи информации в ТКС, классификации угроз по компонентам ТКС, информационные угрозы. |
| 5. | Методы оценки уязвимостей ТКС | Тестирование ТКС, тестирование и оценивание безопасности, тестирование на проникновение, идентификация потенциальных сбоев, уязвимости системы. |
| 6. | Системы электросвязи, угрозы безопасности и методы их защиты | Системы телефонной связи, организационные проблемы. |
| 7. | Общие методы организации защищенной речевой связи в телефонной сети | Стационарные абоненты, пеший режим, блуждающий режим, подвижный режим. |
| 8. | Методы защиты информации в телефонном канале связи | Методы, основанные на ограничении физического доступа к линии и аппаратуре связи, и методы, основанные на преобразовании сигналов в линии к форме, включающей (затрудняющей) для злоумышленника восприятие или искажение содержания передачи. |

| | | |
|-----|---|--|
| 9. | Рекомендации по ограничению физического доступа к оборудованию связи | Правила организации рабочего места абонента защищенной связи. |
| 10. | Защита речевой информации в канале связи путем преобразования сигнала | Аппаратура защиты с кодированием голоса, аппаратура защиты с кодированием звуковых сигналов на скорости 30-64 кбит/сек с последующим шифрованием полученного цифрового потока, преобразования с временными или частотными перестановками (скремблированием) с переменными перестановками под управлением криптоблока и комбинированные мозаичные преобразования, преобразования с временными перестановками (скремблированием) и временной инверсией элементов речевого сигнала со статическим законом перестановки, преобразования с инверсией спектра и статическими перестановками спектральных компонент речевого сигнала. |
| 11. | Информационная безопасность телефонной связи | Краткая характеристика систем телефонной связи, пути и места утечки информации в телефонных системах, каналы побочной утечки телефонной информации, основные методы защиты информации, скремблирование сигнала и шифрование цифровой информации, варианты подключения шифрующих устройств. |
| 12. | Современные криптографические алгоритмы | Общая характеристика криптографических систем, Классические алгоритмы шифрования, шифрование по стандарту DES, асимметричные криптосистемы, использование генератора псевдослучайных чисел. |
| 13. | Защита информации в системах волоконно-оптической связи | Особенности оптических систем связи, физические особенности, технические особенности, недостатки волоконной технологии. |
| 14. | Факторы, влияющие на надежность и конфиденциальность передачи информации в ВОЛС | Поляризационная модовая дисперсия, внешние факторы воздействия на величину ПМД, быстрые и медленные состояниями поляризации PSP |
| 15. | Пути утечки информации из ВОЛС | Пути утечки информации, основные физические принципы формирования каналов утечки в ВОЛС, способы формирования каналов утечки излучений из ВОЛС, способы осуществления несанкционированного доступа к ВОЛС. |
| 16. | Методы защиты информации, передаваемой по ВОЛС | Физические методы защиты, разработка технических средств контроля НД к информационному сигналу, передаваемому по ОВ, СДС с анализом прошедшего сигнала, СДС с анализом отраженного сигнала, краткий обзор криптографических методов защиты, пример использования криптографического метода защиты. |
| 17. | Защита ВОЛС | Три основных направления защиты, кодовое зашумления передаваемых сигналов, метод создания и контроля картины интерференции, метод анализа модо- |

| | | |
|-----|--------------------------|--|
| | | вого состава, метод режима динамического хаоса, механические и электрические средства защиты, датчики контроля подключения к оптическому кабелю, метод частотно-модулированного зондирования, метод защиты с использованием многослойного оптического волокна со специальной структурой, квантовая криптография. |
| 18. | Виртуальные частные сети | VPN-соединение, туннель, канал доступа, виды VPN, безопасность VPN, атаки на VPN, преимущества VPN, возможности VPN. |

Таблица 4.2 –Содержание дисциплины и её методическое обеспечение

| № п/п | Раздел (тема) дисциплины | Виды деятельности | | | Учебно-методические материалы | Формы текущего контроля успеваемости (по неделям семестра) | Компетенции |
|-------|--|-------------------|-------|-------|-------------------------------|--|-------------|
| | | лек., час | № лб. | № пр. | | | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 1. | Основные положения, предмет дисциплины «Информационная безопасность телекоммуникационных систем» | 1 | - | - | О – 1 Д – 3, 4 | С2 | ПК-1 |
| 2. | Доктрина информационной безопасности РФ | 1 | - | - | О – 1 Д – 3, 4 | С2 | ПК-1 |
| 3. | Угрозы информационной безопасности ТКС | 1 | - | - | О – 1 Д – 1, 2 | С3 | ПК-1 |
| 4. | Классификация угроз по компонентам ТКС | 1 | - | - | О – 1 Д – 2, 3 | С4 | ПК-1 |
| 5. | Методы оценки уязвимостей ТКС | 1 | - | - | О – 2 Д – 5, 6 | С5 | ПК-14 |
| 6. | Системы электросвязи, угрозы безопасности и методы их защиты | 1 | - | 1 | О – 2 Д – 5 МУ – 1 | С6, КО6 | ПК-14 |
| 7. | Общие методы организации защищенной речевой связи в телефонной сети | 1 | - | 2 | О – 2 Д – 7 МУ – 2 | С7, КО7 | ПК-14 |
| 8. | Методы защиты информации в телефонном канале связи | 1 | - | 3 | О – 2 Д – 6 МУ – 3 | С8, КО8 | ПК-14 |
| 9. | Рекомендации по ограничению физического доступа к оборудованию связи | 1 | - | 4 | О – 2 Д – 7 МУ – 4 | С9, КО9 | ПК-14 |
| 10. | Защита речевой информации в канале связи путем преобразования сигнала | 1 | - | 5 | О – 2 Д – 3 МУ – 5 | С10, КО10 | ПК-14 |

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|-----|---|---|---|---|--------------------------|--------------|-------|
| 11. | Информационная безопасность телефонной связи | 1 | - | 6 | О – 1 Д – 1 МУ – 6 | С11, КО11 | ПК-1 |
| 12. | Современные криптографические алгоритмы | 1 | - | - | О – 1 Д – 2, 4 | С12 | ПК-1 |
| 13. | Защита информации в системах волоконно-оптической связи | 1 | - | - | О – 2 Д – 4, 6 | С13 | ПК-14 |
| 14. | Факторы, влияющие на надежность и конфиденциальность передачи информации в ВОЛС | 1 | - | - | О – 1 Д – 6 | С14 | ПК-1 |
| 15. | Пути утечки информации из ВОЛС | 1 | - | - | О – 1 Д – 5 | С15 | ПК-1 |
| 16. | Методы защиты информации, передаваемой по ВОЛС | 1 | - | - | О – 2 Д – 7 | С16 | ПК-14 |
| 17. | Защита ВОЛС | 1 | - | - | О – 2 Д – 7 | С17 | ПК-14 |
| 18. | Виртуальные частные сети | 1 | - | - | О – 1 Д – 6, 7 | С18 | ПК-1 |

С – собеседование, КО – контрольный опрос.

4.2. Лабораторные работы и практические занятия

4.2.1. Практические занятия

Таблица 4.4 – Практические занятия

| № | Наименование практического занятия | Объем, час. |
|-------|--|-------------|
| 1. | Практическая работа №1 «Общие вопросы обработки сигналов в программе Adobe Audition» | 3 |
| 2. | Практическая работа №2 «Маскировка тонального телефонного сигнала путем его зашумления» | 3 |
| 3. | Практическая работа №3 «Определение неизвестного номера абонента аналоговой телефонной сети путем спектральной оценки частотных параметров его сигналов» | 3 |
| 4. | Практическая работа №4 «Обработка тональных сигналов набора номера» | 3 |
| 5. | Практическая работа №5 «Модификация тонального сигнала набора номера» | 3 |
| 6. | Практическая работа №6 «Маскировка телефонного сигнала методом статической перестановки его временных сегментов» | 3 |
| Итого | | 18 |

4.3. Самостоятельная работа студентов (СРС)

Таблица 4.5 – Самостоятельная работа студентов

| № | Наименование раздела учебной дисциплины | Срок выполнения | Время, затрачиваемое на выполнение СРС, час. |
|-------|--|-----------------|--|
| 1. | Основные положения, предмет дисциплины «Информационная безопасность телекоммуникационных систем» | 1 неделя | 1,5 |
| 2. | Доктрина информационной безопасности РФ | 2 неделя | 2 |
| 3. | Угрозы информационной безопасности ТКС | 3 неделя | 2 |
| 4. | Классификация угроз по компонентам ТКС | 4 неделя | 2 |
| 5. | Методы оценки уязвимостей ТКС | 5 неделя | 2 |
| 6. | Системы электросвязи, угрозы безопасности и методы их защиты | 6 неделя | 2 |
| 7. | Общие методы организации защищенной речевой связи в телефонной сети | 7 неделя | 2 |
| 8. | Методы защиты информации в телефонном канале связи | 8 неделя | 2 |
| 9. | Рекомендации по ограничению физического доступа к оборудованию связи | 9 неделя | 2 |
| 10. | Защита речевой информации в канале связи путем преобразования сигнала | 10 неделя | 2 |
| 11. | Информационная безопасность телефонной связи | 11 неделя | 2 |
| 12. | Современные криптографические алгоритмы | 12 неделя | 2 |
| 13. | Защита информации в системах волоконно-оптической связи | 13 неделя | 2 |
| 14. | Факторы, влияющие на надежность и конфиденциальность передачи информации в ВОЛС | 14 неделя | 2 |
| 15. | Пути утечки информации из ВОЛС | 15 неделя | 2 |
| 16. | Методы защиты информации, передаваемой по ВОЛС | 16 неделя | 2 |
| 17. | Защита ВОЛС | 17 неделя | 2 |
| 18. | Виртуальные частные сети | 18 неделя | 2 |
| Итого | | | 35,9 |

5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Студенты могут при самостоятельном изучении отдельных тем и вопросов дисциплин пользоваться учебно-наглядными пособиями, учебным оборудованием и методическими разработками кафедры в рабочее время, установленное Правилами внутреннего распорядка работников.

Учебно-методическое обеспечение для самостоятельной работы обучающихся по данной дисциплине организуется:

библиотекой университета:

– библиотечный фонд укомплектован учебной, методической, научной, периодической, справочной и художественной литературой в соответствии с данной РПД;

– имеется доступ к основным информационным образовательным ресурсам, информационной базе данных, в том числе библиографической, возможность выхода в Интернет.

кафедрой:

– путем обеспечения доступности всего необходимого учебно-методического и справочного материала;

– путем предоставления сведений о наличии учебно-методической литературы, современных программных средств;

– путем составления заданий для самостоятельной работы;

– путем разработки вопросов к зачету, методических указаний к выполнению практических работ.

типографией университета:

– путем помощи авторам в подготовке и издании научной, учебной, учебно-методической литературы;

– путем удовлетворения потребностей в тиражировании научной, учебной, учебно-методической литературы.

6. Образовательные технологии

В соответствии с требованиями ФГОС и Приказа Министерства образования и науки РФ от 15 апреля 2017 г. №301 реализация компетентностного подхода предусматривает широкое использование в образовательном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков студентов. Удельный вес занятий, проводимых в интерактивных формах, составляет 22.2% от аудиторных занятий согласно УП. Средствами промежуточного контроля успеваемости студентов являются защита практических работ, опросы на практических занятиях по темам лекций.

Таблица 6.1 – Интерактивные образовательные технологии, используемые при проведении аудиторных занятий

| № | Наименование раздела (темы лекции, практического или лабораторного занятия) | Используемые интерактивные образовательные технологии | Объем, час. |
|----|--|--|-------------|
| 1. | Практическая работа №1 «Общие вопросы обработки сигналов в программе Adobe Audition»; | Выполнение студентом интерактивных заданий в программе Adobe Audition. | 2 |
| 2. | Практическая работа №2 «Маскировка тонального телефонного сигнала путем его зашумления»; | Выполнение студентом интерактивных заданий по маскировке тонального телефонного сигнала. | 2 |
| 3. | Практическая работа №3 «Определение неизвестного номера абонента» | Выполнение студентом интерактивных заданий по определению | 2 |

| | | | |
|----|---|---|----|
| | аналоговой телефонной сети путем спектральной оценки частотных параметров его сигналов»; | неизвестного номера абонента. | |
| 4. | Практическая работа №4 «Обработка тональных сигналов набора номера»; | Выполнение студентом интерактивных заданий по обработке тональных сигналов набора номера. | 2 |
| 5. | Практическая работа №5 «Модификация тонального сигнала набора номера»; | Выполнение студентом интерактивных заданий по модификации тонального сигнала | 2 |
| 6. | Практическая работа №6 «Маскировка телефонного сигнала методом статической перестановки его временных сегментов»; | Выполнение студентом интерактивных заданий по маскировке телефонного сигнала. | 2 |
| | Итого | | 12 |

7. Фонд оценочных средств для проведения промежуточной аттестации

7.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Таблица 7.1 – Этапы формирования компетенций

| Код и содержание компетенции | Этапы* формирования компетенций и дисциплины (модули), при изучении которых формируется данная компетенция | | |
|--|--|--|---|
| | начальный | основной | завершающий |
| 1 | 2 | 3 | 4 |
| осуществлять анализ научно-технической информации, нормативных и методических материалов по методам обеспечения информационной безопасности телекоммуникационных систем (ПК-1) | Русский язык и культура речи Практика по получению первичных профессиональных умений, в том числе первичных умений и навыков научно-исследовательской деятельности Учебно-лабораторный практикум | Информационная безопасность телекоммуникационных систем Основы информационной безопасности Основы криптографии Основы теории чисел Научно-исследовательская работа | Планирование и управление информационной безопасностью Основы многоканальных систем передачи Системы и сети радиосвязи Системы и сети мобильной связи Ознакомительная практика Практика по получению профессиональных умений и опыта профессиональной деятельности Преддипломная практика Защита выпускной квалификационной работы, включая под- |

| | | | |
|---|--|---|---|
| | | | готовку к процедуре защиты и процедуру защиты |
| <p>применять положения теорий электрических цепей, радиотехнических сигналов, распространения радиоволн, цифровой обработки сигналов, информации и кодирования, электрической связи для решения профессиональных задач (ОПК-3);</p> <p>выполнять установку, настройку, обслуживание, диагностику, эксплуатацию и восстановление работоспособности телекоммуникационного оборудования и приборов, технических и программно-аппаратных средств защиты телекоммуникационных сетей и систем (ПК-14)</p> | | Информационная безопасность телекоммуникационных систем | <p>Антенны и распространение радиоволн</p> <p>Аппаратные средства телекоммуникационных систем</p> <p>Техническая защита информации</p> <p>Программно-аппаратные средства обеспечения информационной безопасности</p> <p>Защита информации в системах беспроводной связи</p> <p>Защита информации в компьютерных сетях</p> <p>Администрирование защищенных телекоммуникационных систем</p> <p>Практика по получению профессиональных умений и опыта профессиональной деятельности</p> <p>Эксплуатационная практика</p> <p>Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты</p> |

**Этапы для РПД всех форм обучения определяются по учебному плану очной формы обучения следующим образом:*

| Этап | Учебный план очной формы обучения/ семестр изучения дисциплины | | |
|--------------------|---|---------------|--------------|
| | Бакалавриат | Специалитет | Магистратура |
| <i>Начальный</i> | 1-3 семестры | 1-3 семестры | 1 семестр |
| <i>Основной</i> | 4-6 семестры | 4-6 семестры | 2 семестр |
| <i>Завершающий</i> | 7-8 семестры | 7-10 семестры | 3-4 семестр |

****** Если при заполнении таблицы обнаруживается, что *один или два этапа* не обеспечены дисциплинами, практиками, НИР, необходимо:

- при наличии дисциплин, изучающихся в разных семестрах, – распределить их по этапам в зависимости от № семестра изучения (начальный этап соответствует более ран-

нему семестру, основной и завершающий – более поздним семестрам);

- при наличии дисциплин, изучающихся в одном семестре, – все дисциплины указать для всех этапов.

7.2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Таблица 7.2 – Критерии и шкала оценивания компетенций

| Наименование компетенции | Показатели оценивания компетенций | Критерии и шкала оценивания компетенций | | |
|---|---|---|--|--|
| | | Пороговый уровень («удовлетворительно») | Продвинутый уровень («хорошо») | Высокий уровень («отлично») |
| применять положения теорий электрических цепей, радиотехнических сигналов, распространения радиоволн, цифровой обработки сигналов, информации и кодирования, электрической связи для решения профессиональных задач (ОПК-3) | <p>1. Доля освоенных обучающимся знаний, умений, навыков от общего объема ЗУН, установленных в п.1.3 РПД</p> <p>2. Качество освоенных обучающимся знаний, умений, навыков</p> <p>3. Умение применять знания, умения, навыки в типовых и нестандартных ситуациях</p> | <p>Знать: основное понятие ИБ ТКС, основные её функции</p> <p>Уметь: анализировать научно-техническую информацию ИБ ТКС.</p> <p>Владеть навыками: оценки различных компонентов подсистем обеспечения ИБ ТКС.</p> | <p>Знать: принципы организации подсистем безопасности ТКС.</p> <p>Уметь: анализировать научно-техническую информацию и нормативные материалы ИБ ТКС.</p> <p>Владеть навыками: составления аналитического отчета о состоянии ИБ ТКС.</p> | <p>Знать: критерии соответствия функционала подсистем информационной безопасности ТКС угрозам для объектов информатизации.</p> <p>Уметь: анализировать научно-техническую информацию и нормативные и методические материалы ИБ ТКС.</p> <p>Владеть навыками: составления методических комплексов по ИБ ТКС.</p> |
| осуществлять анализ научно-технической информации, нормативных и ме- | <p>1. Доля освоенных обучающимся знаний, умений, навыков от общего объема ЗУН, установленных в п.1.3 РПД</p> | <p>Знать: основное понятие ИБ ТКС, основные её функции</p> <p>Уметь: анализировать научно-техническую информацию ИБ ТКС.</p> | <p>Знать: принципы организации подсистем безопасности ТКС.</p> <p>Уметь: анализировать научно-техническую информацию и нормативные</p> | <p>Знать: критерии соответствия функционала подсистем информационной безопасности ТКС угрозам для объектов информатизации.</p> <p>Уметь: анализиро-</p> |

| | | | | |
|---|---|---|--|---|
| <p>тодиче-ских мате-риалов по методам обеспе-чения ин-форма-ционной без-опасности телеком-муникаци-онных си-стем (ПК-1)</p> | <p>2.Качество осво-енных обучаю-щимся знаний, умений, навыков</p> <p>3.Умение приме-нять знания, уме-ния, навыки в типовых и нестандартных ситуациях</p> | <p>Владеть навы-ками: оценки различных ком-понентов подси-стем обеспе-чения ИБ ТКС.</p> | <p>материалы ИБ ТКС.</p> <p>Владеть навы-ками: составле-ния аналитиче-ского отчета о состоянии ИБ ТКС.</p> | <p>вать научно-техническую ин-формацию и нор-мативные и мето-дические материа-лы ИБ ТКС.</p> <p>Владеть навыка-ми: составления методических ком-плексов по ИБ ТКС.</p> |
| <p>способ-ность вы-полнять установку, настройку, обслужи-вание, диа-гностику, эксплуата-цию и вос-становле-ние рабо-тоспособ-ности телекомму-никацион-ного обо-рудования и прибо-ров, тех-нических и программ-но-аппарат-ных средств защиты телеком-муникаци-онных се-тей и си-стем (ПК-14)</p> | <p>1.Доля освоенных обу-чающимся зна-ний, умений, навыков от обще-го объема ЗУН, установленных в п.1.3 РПД</p> <p>2.Качество осво-енных обучаю-щимся знаний, умений, навыков</p> <p>3.Умение приме-нять знания, уме-ния, навыки в типовых и нестандартных ситуациях</p> | <p>Знать: основное понятие ИБ ТКС, основные её функции</p> <p>Уметь: выпол-нять сервисные мероприятия с системами про-граммно-аппаратной за-щиты информа-ции ТКС.</p> <p>Владеть навы-ками: эксплуа-тации различных компонентов подсистем обес-печения ИБ ТКС.</p> | <p>Знать: принци-пы организации подсистем без-опасности ТКС.</p> <p>Уметь: настраи-вать программ-но-аппаратные системы защиты информации ТКС.</p> <p>Владеть навы-ками: админи-стрирования программно-аппаратных СЗИ ТКС.</p> | <p>Знать: критерии соответствия функ-ционала подсистем информационной безопасности ТКС угрозам для объек-тов информатиза-ции.</p> <p>Уметь: выбирать требуемы политики безопасности при настройке про-граммно-аппаратных СЗИ.</p> <p>Владеть навыка-ми: реагировании на нештатные си-туации, возникаю-щие при эксплуа-тации программно-аппаратных СЗИ ТКС.</p> |

7.3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Таблица 7.3 – Паспорт комплекта оценочных средств для текущего контроля

| п/п | Раздел (тема) дисциплины | Код контролируемой компетенции (или её части) | Технология формирования | Оценочные средства | | Описание шкал оценивания |
|-----|--|---|-----------------------------------|----------------------------|------------|--------------------------|
| | | | | наименование | №№ заданий | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 1. | Основные положения, предмет дисциплины «Информационная безопасность телекоммуникационных систем» | ПК-1 | Лекция, СРС | Собеседование | 1-6 | Согласно табл.7.2 |
| 2. | Доктрина информационной безопасности РФ | ПК-1 | Лекция, СРС | Собеседование | 1-6 | Согласно табл.7.2 |
| 3. | Угрозы информационной безопасности | ПК-1 | Лекция, СРС | Собеседование | 1-6 | Согласно табл.7.2 |
| 4. | Классификация угроз по компонентам | ПК-1 | Лекция, СРС | Собеседование | 1-6 | Согласно табл.7.2 |
| 5. | Методы оценки уязвимостей ТКС | ПК-14 | Лекция, СРС | Собеседование | 1-3 | Согласно табл.7.2 |
| 6. | Системы электросвязи, угрозы безопасности и методы их защиты | ПК-14 | Лекция, СРС, практическое занятие | Собеседование | 1-3 | Согласно табл.7.2 |
| | | | | Контрольные вопросы к ПР№1 | 1-14 | |
| 7. | Общие методы организации защищенной | ПК-14 | Лекция, СРС, практическое занятие | Собеседование | 1-6 | Согласно табл.7.2 |

| | | | | | | |
|-----|---|-------|---|--|------|----------------------|
| | речевой связи в телефонной сети | | | Контроль ные во- просы к ПР№2 | 1-3 | |
| 8. | Методы защиты информации в телефонном канале связи | ПК-14 | Лекция, СРС, практическое занятие | Собеседов ание | 1-4 | Согласно табл.7.2 |
| | | | | Контроль ные во- просы к ПР№3 | 1-5 | |
| 9. | Рекомендации по ограничению физического доступа к оборудованию связи | ПК-14 | Лекция, СРС, практическое занятие | Собеседов ание | 1-5 | Согласно табл.7.2 |
| | | | | Контроль ные во- просы к ПР№4 | 1-6 | |
| 10. | Защита речевой информации в канале связи путем преобразования сигнала | ПК-14 | Лекция, СРС, практическое занятие | Собеседов ание | 1-6 | Согласно табл.7.2 |
| | | | | Контроль ные во- просы к ПР№5 | 1-10 | |
| 11. | Информационная безопасность телефонной связи | ПК-1 | Лекция, СРС, практическое занятие | Собеседов ание | 1-6 | Согласно табл.7.2 |
| | | | | Контроль ные во- просы к ПР№6 | 1-8 | |
| 12. | Современные криптографические алгоритмы | ПК-1 | Лекция, СРС | Собеседов ание | 1-6 | Согласно табл.7.2 |

| | | | | | | |
|-----|---|-------|-------------|---------------|-----|-------------------|
| 13. | Защита информации в системах волоконно-оптической связи | ПК-14 | Лекция, СРС | Собеседование | 1-6 | Согласно табл.7.2 |
| 14. | Факторы, влияющие на надежность и конфиденциальность передачи информации в ВОЛС | ПК-1 | Лекция, СРС | Собеседование | 1-6 | Согласно табл.7.2 |
| 15. | Пути утечки информации из ВОЛС | ПК-1 | Лекция, СРС | Собеседование | 1-6 | Согласно табл.7.2 |
| 16. | Методы защиты информации, передаваемой по ВОЛС | ПК-14 | Лекция, СРС | Собеседование | 1-6 | Согласно табл.7.2 |
| 17. | Защита ВОЛС | ПК-14 | Лекция, СРС | Собеседование | 1-6 | Согласно табл.7.2 |
| 18. | Виртуальные частные сети | ПК-1 | Лекция, СРС | Собеседование | 1-6 | Согласно табл.7.2 |

Примеры типовых контрольных заданий для текущего контроля

Вопросы собеседования по разделу (теме) 1. «Основные положения, предмет дисциплины «Информационная безопасность телекоммуникационных систем»».

1. Что такое информация?
2. На какие группы подразделяют виды информации?
3. Что такое информационная безопасность?
4. Что понимается под утечкой информации?
5. На какие системы разделяют системы передачи информации?
6. Как называется информация, предназначенная для использования ограниченным кругом лиц?

Контрольные вопросы к практической работе по теме «Обработка тональных сигналов набора номера»

1. Привести схему нерайонированной и районированной ГТС.
2. Что такое сигнализация, система сигнализации и протокол сигнализации.
3. Привести виды сигнализации в телефонных сетях по их функциональному назначению.
4. Привести классы систем межстанционной сигнализации.
5. Какие используются виды кодирования набора номера.
6. Чем характеризуются импульсный и тональный набор номера.

Полностью оценочные средства представлены в учебно-методическом комплексе дисциплины.

Типовые задания для промежуточной аттестации.

Промежуточная аттестация по дисциплине проводится в форме зачета. Зачет проводится в форме тестирования (бланкового и/или компьютерного).

Для тестирования используются контрольно-измерительные материалы (КИМ)

– задания в тестовой форме, составляющие банк тестовых заданий (БТЗ) по дисциплине, утвержденный в установленном в университете порядке.

Проверяемыми на промежуточной аттестации элементами содержания являются темы дисциплины, указанные в разделе 4 настоящей программы. Все темы дисциплины отражены в КИМ в равных долях (%). БТЗ включает в себя не менее 100 заданий и постоянно пополняется.

Для проверки *знаний* используются вопросы и задания в различных формах:

- закрытой (с выбором одного или нескольких правильных ответов),

- открытой (необходимо вписать правильный ответ),
- на установление правильной последовательности,
- на установление соответствия.

Умения, навыки и компетенции проверяются с помощью задач (ситуационных, производственных или кейсового характера) и различного вида конструкторов. Все задачи являются многоходовыми. Некоторые задачи, проверяющие уровень сформированности компетенций, являются многовариантными. Часть умений, навыков и компетенций прямо не отражена в формулировках задач, но они могут быть проявлены обучающимися при их решении.

В каждый вариант КИМ включаются задания по каждому проверяемому элементу содержания во всех перечисленных выше формах и разного уровня сложности. Такой формат КИМ позволяет объективно определить качество освоения обучающимися основных элементов содержания дисциплины и уровень сформированности компетенций.

7.4. Рейтинговый контроль изучения учебной дисциплины

Процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций, регулируются следующими нормативными актами университета:

- Положение П 02.016–2015 «О балльно-рейтинговой системе оценки качества освоения образовательных программ»;
- методические указания, используемые в образовательном процессе, указанные в списке литературы.

Для *текущего контроля* по дисциплине в рамках действующей в университете балльно-рейтинговой системы применяется следующий порядок начисления баллов:

Таблица 7.4 – Порядок начисления баллов в рамках БРС

| Форма контроля | Минимальный балл | | Максимальный балл | |
|---|------------------|---------------------------|-------------------|----------------------|
| | балл | примечание | балл | примечание |
| Практическая работа №1 «Общие вопросы обработки сигналов в программе Adobe Audition»; | 2 | Выполнил, но «не защитил» | 4 | Выполнил и «защитил» |
| Практическая работа №2 «Маскировка тонального телефонного сигнала путем его зашумления»; | 2 | Выполнил, но «не защитил» | 4 | Выполнил и «защитил» |
| Практическая работа №3 «Определение неизвестного номера абонента аналоговой телефонной сети путем спектральной оценки частотных параметров его сигналов»; | 2 | Выполнил, но «не защитил» | 4 | Выполнил и «защитил» |

| | | | | |
|---|----|---------------------------|-----|----------------------|
| Практическая работа №4 «Обработка тональных сигналов набора номера»; | 2 | Выполнил, но «не защитил» | 4 | Выполнил и «защитил» |
| Практическая работа №5 «Модификация тонального сигнала набора номера»; | 4 | Выполнил, но «не защитил» | 6 | Выполнил и «защитил» |
| Практическая работа №6 «Маскировка телефонного сигнала методом статической перестановки его временных сегментов»; | 4 | Выполнил, но «не защитил» | 6 | Выполнил и «защитил» |
| СРС | 8 | | 20 | |
| ИТОГО | 24 | | 48 | |
| Посещаемость | 0 | | 16 | |
| Зачёт | 0 | | 36 | |
| ИТОГО | 24 | | 100 | |

При итоговом контроле в форме бланкового теста студенту предлагается 15 вопросов по различным темам курса. Полученную итоговую сумму условных баллов (максимум 15) переводят в баллы на зачете (максимум 36) путём умножения на 2.4 и округления до целого значения.

8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

8.1. Основная учебная литература

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. Сеницын, 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.

8.2. Дополнительная литература

1) **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.

2) **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.

3) **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.

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

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

6) **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.

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

8.3. Перечень методических указаний

1) **Общие вопросы обработки сигналов в программе Adobe Audition:** 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. 13 с.: ил., Библиогр.: с. 12.

2) **Маскировка тонального телефонного сигнала путем его зашумления:** 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

3) **Определение неизвестного номера абонента аналоговой телефонной сети путем спектральной оценки частотных параметров его сигналов:** 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. 11 с.: ил., Библиогр.: с. 11.

4) **Обработка тональных сигналов набора номера:** 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. 13 с.: ил., Библиогр.: с. 12

5) Модификация тонального сигнала набора номера: 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. 11 с. Библиогр.: с. 11.

6) Маскировка телефонного сигнала методом статической перестановки его временных сегментов: 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. Библиогр.: с. 12.

8.4 Другие учебно-методические материалы

Отраслевые научно-технические журналы в библиотеке университета:
Проблемы информационной безопасности. Компьютерные технологии.
Защита информации. Инсайд.

Информационные системы и технологии.

Вестник компьютерных и информационных технологий.

9. Перечень ресурсов информационно-телекоммуникационной сети Интернет

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>)

10. Методические указания для обучающихся по освоению дисциплины

Основными видами аудиторной работы студента при изучении дисциплины «Информационная безопасность телекоммуникационных систем» являются лекции и практические занятия. Студент не имеет права пропускать занятия без уважительных причин.

На лекциях излагаются и разъясняются основные понятия темы, свя-

занные с ней теоретические и практические проблемы, даются рекомендации для самостоятельной работы. В ходе лекции студент должен внимательно слушать и конспектировать материал.

Изучение наиболее важных тем или разделов дисциплины завершают практические занятия, которые обеспечивают: контроль подготовленности студента; закрепление учебного материала; приобретение опыта устных публичных выступлений, ведения дискуссии, в том числе аргументации и защиты выдвигаемых положений и тезисов.

Практическому занятию предшествует самостоятельная работа студента, связанная с освоением материала, полученного на лекциях, и материалов, изложенных в учебниках и учебных пособиях, а также литературе, рекомендованной преподавателем.

Качество учебной работы студентов преподаватель оценивает по результатам собеседования, защиты отчетов по практическим работам.

Преподаватель уже на первых занятиях объясняет студентам, какие формы обучения следует использовать при самостоятельном изучении дисциплины «Информационная безопасность телекоммуникационных систем»: конспектирование учебной литературы и лекции, составление словарей понятий и терминов и т. п.

В процессе обучения преподаватели используют активные формы работы со студентами: чтение лекций, привлечение студентов к творческому процессу на лекциях, промежуточный контроль путем отработки студентами пропущенных лекции, участие в групповых и индивидуальных консультациях (собеседовании). Эти формы способствуют выработке у студентов умения работать с учебником и литературой. Изучение литературы и справочной документации составляет значительную часть самостоятельной работы студента. Это большой труд, требующий усилий и желания студента. В самом начале работы над книгой важно определить цель и направление этой работы. Прочитанное следует закрепить в памяти. Одним из приемов закрепление освоенного материала является конспектирование, без которого немислима серьезная работа над литературой. Систематическое конспектирование помогает научиться правильно, кратко и четко излагать своими словами прочитанный материал.

Самостоятельную работу следует начинать с первых занятий. От занятия к занятию нужно регулярно прочитывать конспект лекций, знакомиться с соответствующими разделами учебника, читать и конспектировать литературу по каждой теме дисциплины. Самостоятельная работа дает студентам возможность равномерно распределить нагрузку, способствует более глубокому и качественному усвоению учебного материала. В случае необходимости студенты обращаются за консультацией к преподавателю по вопросам дисциплины «Информационная безопасность телекоммуникационных систем» с целью усвоения и закрепления компетенций.

Основная цель самостоятельной работы студента при изучении дисциплины «Информационная безопасность телекоммуникационных систем» -

закрепить теоретические знания, полученные в процессе лекционных занятий, а также сформировать практические навыки самостоятельного анализа особенностей дисциплины.

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

- 1) Libreoffice (Бесплатная, GNU General Public License) - <https://ru.libreoffice.org/> ;
- 2) Microsoft Office 2016 Лицензионный договор №S0000000722 от 21.12.2015 г. с ООО «АйТи46», лицензионный договор №K0000000117 от 21.12.2015 г. с ООО «СМСКанал»;
- 3) Операционная система Windows, договор IT000012385;
- 4) Kaspersky Endpoint Security Russian Edition, лицензия 156A-140624-192234;
- 5) Adobe Audition (Бесплатная пробная версия) - <https://creative.adobe.com/ru/products/download/audition> .

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Учебная аудитория для проведения занятий лекционного типа и лаборатории кафедры информационной безопасности, оснащенные учебной мебелью: столы, стулья для обучающихся; стол, стул для преподавателя; доска. Компьютеры (10 шт) Компьютер NORBEL C239264Ц-AMD/2x8Gb/2ТВ/DVDRW/LCD 20";

- Система виброакустического шумления «Шорох-2», виброакустический датчик КПВ-2, акустический излучатель OMS -2000
- Подавитель «жучков» и беспроводных видеокамер “BigHunter Spy”
- Комбинированный поисковый прибор “D008”
- Генератор шума Соната-С1

Для проведения промежуточной аттестации необходимо следующее материально-техническое оборудование:

1. Проекционный экран на штативе; Мультимедиа центр: ноутбук ASUS X50VL PMD-T2330/1471024Mb/160Gb/ сумка/ проектор inFocus IN24

13. Лист дополнений и изменений, внесенных в рабочую программу дисциплины

| Номер изменения | Номера страниц | | | | Всего страниц | Дата | Основание для изменения и под- пись лица, прово- дившего |
|--------------------|----------------|------------|----------------|-------|------------------|------|---|
| | изменённых | заменённых | аннулированных | новых | | | |
| | | | | | | | |