МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Воронежский государственный технический университет»

УТВЕРЖДАЮ

Декан факультета ФИТКБ

_____ /Брюхин А.В./

28.08.2025 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Проектирование защищенных телекоммуникационных систем»

Специальность 10.05.02 Информационная безопасность телекоммуникационных систем

Специализация специализация № 9 "Управление безопасностью телекоммуникационных систем и сетей"

Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет и 6 м.

Форма обучения очная

Год начала подготовки 2025

Автор программы _____ В.О. Морозов

Заведующий кафедрой Систем информационной безопасности _____ А.Г. Остапенко

Руководитель ОПОП _____ С.С. Куликов

Воронеж 2025

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1. Цели дисциплины формирование у учащихся знания о базовых принципах и подходах к проектированию защищенных телекоммуникационных систем (ТКС), а также обеспечение развития практических навыков и способностей к решению прикладных задач проектирования.

1.2. Задачи освоения дисциплины

- ознакомление с методологическими основами организации защиты информации в ТКС, с технологиями восходящего, нисхо-дящего проектирования ТКС в защищенном исполнении, с поряд-ком формирования и содержанием требований по защите инфор-мации, предъявляемым действующими нормативными документа-ми, с характеристиками и способами применения мер и средств защиты информации;
- формирование представлений о системах защиты инфор-мации в составе ТКС и путях их построения;
- приобретение навыков обоснования требований к системам защиты информации в составе ТКС в защищенном исполнении, выбора целесообразных мер и средств защиты в зависимости от установленного класса защищенности ТКС.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Проектирование защищенных телекоммуникационных систем» относится к дисциплинам обязательной части блока Б1.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс изучения дисциплины «Проектирование защищенных телекоммуникационных систем» направлен на формирование следующих компетенций:

ОПК-13 - Способен оценивать технические возможности, анализировать угрозы и вырабатывать рекомендации по построению элементов информационно-телекоммуникационной инфраструктуры с учетом обеспечения требований информационной безопасности;

ОПК-16 - Способен проектировать защищенные телекоммуникационные системы и их элементы, проводить анализ проектных решений по обеспечению заданного уровня безопасности и требуемого качества обслуживания телекоммуникационных систем, разрабатывать необходимую техническую документацию с учетом действующих нормативных и методических документов, проводить подготовку исходных данных для технико-экономического обоснования соответствующих проектных решений

Компетенция	Результаты обучения, характеризующие сформированность компетенции
ОПК-13	знать угрозы безопасности информации в проектируемой ТКС и способы их реализации; характеристики и возможности средств защиты и порядок обоснования требований к ним; способы применения программных и программно-аппаратных средств защиты
	уметь оценивать технические возможности основных систем и сетей электрической связи
	владеть навыком оценки технических возможностей и подготовки рекомендаций по построению отдельных элементов информационно-телекоммуникационной инфраструктуры с учетом обеспечения требований информационной безопасности
ОПК-16	знать порядок установки, настройки, обслуживания, диагностики, эксплуатацию и восстановление работоспособности телекоммуникационного оборудования и приборов, которые могут быть подвержены угрозам безопасности информации; способы и средства контроля работоспособности и эффективности средств защиты
	умеет проектировать элементы защищенных телекоммуникационных систем; проводить подготовку исходных данных для технико-экономического обоснования проектируемых защищенных телекоммуникационных систем

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Проектирование защищенных телекоммуникационных систем» составляет 5 з.е.

Распределение трудоемкости дисциплины по видам занятий

очная форма обучения

Виды учебной работы	Всего часов	Семестры	
		9	10
Аудиторные занятия (всего)	108	36	72
В том числе:			
Лекции	54	18	36
Практические занятия (ПЗ)	54	18	36
Самостоятельная работа	81	72	9
Курсовой проект	+		+
Часы на контроль	27	-	27
Виды промежуточной аттестации - экзамен, зачет	+	+	+

Общая трудоемкость: академические часы зач.ед.	216 6	108 3	108 3

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1 Содержание разделов дисциплины и распределение трудоемкости по видам занятий

очная форма обучения

№ п/п	Наименование темы	Содержание раздела	Лекц	Практ зан.	СРС	Всего, час
1	Основные понятия, касающиеся технологии проектирования ТКС в защищенном исполнении	Трактовка понятий «защита информации», «безопасность информации», «защищенность информации», «обеспечение безопасности информации», «информационная безопасность», «несанкционированный доступ», «эффективность защиты», «политика безопасности информации» или «политика информационной безопасности». Понятие системы защиты информации (СЗИ). Организационная, организационно-техническая и техническая СЗИ	10	8	13	31
2	Методология и технологическая схема проектирования ТКС в защищенном исполнении	Основные подходы к проектированию систем защиты информации (СЗИ): восходящее и нисходящее проектирование, проектирование на основе предварительного установления приоритетов и комбинированный подход. Порядок проектирования СЗИ в соответствии с ГОСТ Р 51583-2014. Содержание комплексов работ при проектировании. Общие требования к созданию СЗИ при модернизации ТКС. Стадии и этапы создания СЗИ для модернизируемой ТКС и содержание работ на них. Особенности проектирования СЗИ при создании новой ТКС в защищенном исполнении. Распределение ответственности организаций и должностных лиц при проектировании ТКС в защищенном исполнении	10	8	13	31
3	Классификация угроз безопасности в телекоммуникационных системах и основы методологии их анализа	Понятие угрозы безопасности информации. Структура описание угрозы безопасности информации. Внешние и внутренние источники угроз. Типы внешних и внутренних нарушителей. Общая характеристика программных и программно-аппаратных закладок. Понятие уязвимости, виды уязвимостей. Структура записи уязвимости в базе CVE. Содержание несанкционированных действий. Схема общей классификации угроз безопасности информации. Понятие сетевой атаки. Классификация сетевых атак. Понятие базовой и частной модели угроз. Порядок анализа угроз и формирования частных моделей угроз	10	8	13	31
4	Типовые сетевые атаки и способы из реализации в современных телекоммуникационных системах. Угрозы применения вредоносных программ (ВП) и способы защиты от них	Этапы реализации типовой сетевой атаки и содержание действий на каждом этапе. Классификационные схемы способов реализации атак. Содержание способов реализации сетевых атак на сетевом, системном и прикладном системно-технических уровнях с использованием протоколов типа FTP, Telnet, SMTP, HTTP, DNS, UDP, TCP, IP, ICMP, ARP, RIP и OSPF. Причины, обусловившие возможность реализации сетевых атак. Понятие	8	10	13	31

		вредоносной программы. Общая классификация и основные виды ВП. Краткая характеристика основных ВП: файловых, загрузочных вирусов и макровирусов, сетевых червей, программных закладок и иных вредоносных программ. Резидентные и нерезидентные вирусы. Приемы инфицирования ТКС. Способы скрытия факта инфицирования ТКС. Полиморфик-вирусы, стелс-вирусы, руткиты. Направления развития ВП				
5	Меры и средства защиты информации от угроз НСД в ТКС. Общая характеристика и классификация. Межсетевые экраны. Основы функционирования	Классы угроз безопасности информации, парируемых с использованием мер и средств защиты от НСД в ТКС. Общая классификационная схема для мер защиты информации в ТКС и ее элементах. Организационные, организационно-технические и технические меры защиты информации. Средства защиты от непосредственного виртуального доступа и воздействия вредоносными программами. Меры защиты информации от несанкционированного доступа, обусловленного применением сетевых технологий взаимодействия. Меры защиты информации при передаче по каналам связи Понятие межсетевого экрана (МЭ). Группы функций фильтрации и посредничества, реализуемые МЭ. Виды межсетевых экранов (экранирующие маршрутизаторы; шлюзы сеансового уровня; прикладные шлюзы) и реализуемые ими функции. Требования к МЭ и способы их применения	8	10	13	31
6	Нормативное обеспечение обоснования требований по защите информации от НСД в ТКС. Порядок задания требований по защите информации к ТКС, выбора мер и средств защиты и построения систем защиты	Система нормативных документов ФСТЭК России, регламентирующих требования по защите информации в ТКС. Основные аспекты защиты информации, регулируемые нормативными документами. Понятие класса (уровня) защищенности телекоммуникационной системы. Краткая характеристика и основные положения нормативных документов, введенных в действие приказами ФСТЭК России от 11 февраля 2013 г. №17, от 18 февраля 2013 г. №21, а также руководящих документов «Автоматизированные системы. Защита от НСД к информации. Классификация автоматизированных систем и требования по защите информации» и «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности». Порядок формирования требований по защите информации в соответствии с указанными документами. Порядок задания требований к мерам и средствам защиты информации в соответствии с действующими документами ФСТЭК России на примере нормативного правового акта, утвержденного приказом ФСТЭК России от 11 февраля 2013 г. №17. Базовый набор мер защиты, его адаптация, дополнение и уточнение, определение компенсирующих мер защиты. Понятие системы защиты информации. Состав возможных подсистем защиты	8	10	16	34
		Итого	**54**	**54**	**81**	**189**

5.2 Перечень лабораторных работ

Не предусмотрено учебным планом

6. ПРИМЕРНАЯ ТЕМАТИКА КУРСОВЫХ ПРОЕКТОВ (РАБОТ) И КОНТРОЛЬНЫХ РАБОТ

В соответствии с учебным планом освоение дисциплины предусматривает выполнение курсовых проектов в 10 семестрах для очной формы обучения.

Примерная тематика курсового проекта:

1) Проектирование структуры защищенной телекоммуникационной системы для предприятий нефтегазовой отрасли.

2) Проектирование структуры защищенной телекоммуникационной системы для органов местного самоуправления.

3) Проектирование структуры защищенной телекоммуникационной системы для предприятий банковской сферы.

4) Проектирование структуры защищенной телекоммуникационной системы для муниципальных предприятий.

5) Проектирование структуры защищенной телекоммуникационной системы для машиностроительной отрасли.

6) Проектирование структуры защищенной телекоммуникационной системы для энергетической отрасли.

7) Проектирование структуры защищенной телекоммуникационной системы для военизированной отрасли.

8) Проектирование структуры защищенной телекоммуникационной системы для строительной отрасли.

9) Проектирование структуры защищенной телекоммуникационной системы для металлургической отрасли

10) Проектирование структуры защищенной телекоммуникационной системы для жилищно-коммунальное хозяйства.

Курсовой проект включат в себя графическую часть и расчетно-пояснительную записку.

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

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

7.1.1 Этап текущего контроля

Результаты текущего контроля знаний и межсессионной аттестации оцениваются по следующей системе:

«аттестован»; «не аттестован».

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Аттестован	Не аттестован
ОПК-13	знать угрозы безопасности информации в проектируемой ТКС	знание угроз безопасности информации в проектируе-	Выполнение работ в срок,	Невыполнение работ

	и способы их реализации; характеристики и возможности средств защиты и порядок обоснования требований к ним; способы применения программных и программно-аппаратных средств защиты	мой ТКС и способы их реализации; характеристики и возможности средств защиты и порядок обоснования требований к ним; способы применения программных и программно-аппаратных средств защиты	предусмотренный в рабочих программах	в срок, предусмотренный в рабочих программах
	уметь оценивать технические возможности основных систем и сетей электрической связи	умение оценивать технические возможности основных систем и сетей электрической связи	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть навыком оценки технических возможностей и подготовки рекомендаций по построению отдельных элементов информационно-телекоммуникационной инфраструктуры с учетом обеспечения требований информационной безопасности	владение навыком оценки технических возможностей и подготовки рекомендаций по построению отдельных элементов информационно-телекоммуникационной инфраструктуры с учетом обеспечения требований информационной безопасности	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ОПК-16	знать порядок установки, настройки, обслуживания, диагностики, эксплуатацию и восстановление работоспособности телекоммуникационного оборудования и приборов, которые могут быть подвержены угрозам безопасности информации; способы и средства контроля работоспособности и эффективности средств защиты	знание порядка установки, настройки, обслуживания, диагностики, эксплуатацию и восстановление работоспособности телекоммуникационного оборудования и приборов, которые могут быть подвержены угрозам безопасности информации; способы и средства контроля работоспособности и эффективности средств защиты	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	умеет проектировать элементы защищенных телекоммуникационных систем; проводить подготовку исходных данных для технико-экономического обоснования проектируемых защищенных телекоммуникационных систем	умение проектировать элементы защищенных телекоммуникационных систем; проводить подготовку исходных данных для технико-экономического обоснования проектируемых защищенных телекоммуникационных систем	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

7.1.2 Этап промежуточного контроля знаний

Результаты промежуточного контроля знаний оцениваются в 9, 10 семестре для очной формы обучения по двух/четырехбалльной системе:

«зачтено»

«не зачтено»

Компетенция	Результаты обучения, характеризующие	Критерии оценивания	Зачтено	Не зачтено

	сформированность компетенции			
ОПК-13	знать угрозы безопасности информации в проектируемой ТКС и способы их реализации; характеристики и возможности средств защиты и порядок обоснования требований к ним; способы применения программных и программно-аппаратных средств защиты	Тест	Выполнение теста на 70-100%	Выполнение менее 70%
	уметь оценивать технические возможности основных систем и сетей электрической связи	Решение стандартных практических задач	Продемонстрирова н верный ход решения в большинстве задач	Задачи не решены
	владеть навыком оценки технических возможностей и подготовки рекомендаций по построению отдельных элементов информационно-телекоммуникационной инфраструктуры с учетом обеспечения требований информационной безопасности	Решение прикладных задач в конкретной предметной области	Продемонстрирова н верный ход решения в большинстве задач	Задачи не решены
ОПК-16	знать порядок установки, настройки, обслуживания, диагностики, эксплуатацию и восстановление работоспособности телекоммуникационного оборудования и приборов, которые могут быть подвержены угрозам безопасности информации; способы и средства контроля работоспособности и эффективности средств защиты	Тест	Выполнение теста на 70-100%	Выполнение менее 70%
	умеет проектировать элементы защищенных телекоммуникационных систем; проводить подготовку исходных данных для технико-экономического обоснования проектируемых защищенных телекоммуникационных систем	Решение стандартных практических задач	Продемонстрирова н верный ход решения в большинстве задач	Задачи не решены

или «отлично»; «хорошо»; «удовлетворительно»; «неудовлетворительно».

Компе-тенция	**Результаты обучения, характеризующие сформированность компетенции**	**Критерии оценивания**	**Отлично**	**Хорошо**	**Удовл.**	**Неудовл.**
ОПК-13	знать угрозы безопасности информации в проектируемой ТКС и способы их реализации; характеристики и возможности средств защиты и порядок обоснования требований к ним; спо-	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70- 80%	В тесте менее 70% правильных ответов

	собы применения программных и программно-аппаратных средств защиты					
	уметь оценивать технические возможности основных систем и сетей электрической связи	Решение стандартных практических задач	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
	владеть навыком оценки технических возможностей и подготовки рекомендаций по построению отдельных элементов информационно-телекоммуникационной инфраструктуры с учетом обеспечения требований информационной безопасности	Решение прикладных задач в конкретной предметной области	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
ОПК-16	знать порядок установки, настройки, обслуживания, диагностики, эксплуатацию и восстановление работоспособности телекоммуникационного оборудования и приборов, которые могут быть подвержены угрозам безопасности информации; способы и средства контроля работоспособности и эффективности средств защиты	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70- 80%	В тесте менее 70% правильных ответов
	умеет проектировать элементы защищенных телекоммуникационных систем; проводить подготовку исходных данных для технико-экономического обоснования проектируемых защищенных телекоммуникационных систем	Решение стандартных практических задач	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены

7.2 Примерный перечень оценочных средств (типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности)

7.2.1 Примерный перечень заданий для подготовки к тестированию

1. Канал передачи – это:

A. совокупность технических средств и среды обеспечивающих передачу сигнала ограниченной мощности в определенной области частот между двумя абонентами независимо от используемых физических линий передачи.

B. различные преобразователи сигналов, коммутирующие устройства, промежуточные усилители

C. средства связи соединяющий абонентов не только в переделах города, региона, но и в пределах всей страны и между странами.

2. Мультиплексированием (группообразованием) называется

A. процесс объединения нескольких каналов

B. Процесс уплотнения нескольких каналов

C. процесс уплотнения физических линии связи

3. С ростом частоты сигнала затухание в линии связи

A. уменьшается

B. не изменяется

C. всегда растёт

4. Линейный спектр ПГ в 12 каналах ТЧ равняется

A. 0,3-3,4 кГц

B. 60□108 кГц

C. 312-552 кГц

5. Качество передачи сигналов передачи данных оцениваются

A. искажениями формы сигналов

B. отсутствием искажения в принятой информации

C. числом ошибок в принятой информации, т.е. верностью передачи.

6. Для чего нужна развязывающее устройство в системе передачи?

A. для подключения двухпроводного окончания к четырехпроводному окончанию

B. для подключения абонентской линии к системе передачи

C. для подключения передающей части оборудования к приемному

7. Норма затухании для телефонного канала на входе АТС

A. — 12 дБ

B. — 7 дБ

C. — 0 дБ

8. Дуплексной передачи связью называется

A. осуществляется передача сигналов в одной паре проводников в одном направлении

B. осуществляется передача сигналов в одном направлении в четырехпроводной линии связи

C. одновременной передачи сигналов между абонентами в обоих направлениях, т.е. канал связи должен быть двустороннего действия.

9. Совпадающие помехи в ТЛФ тракте порождаются:

A. за счёт линейных переходов на передающем и приёмном концах усилительных участков за счёт конечной балансировки развязывающих устройств,

B. по цепям питания и за счёт электромагнитных наводок внутри кабеля от соседних проводников

C. оба ответы верны

10. Увеличение число уровней квантования приведет к чему

A. к увеличению скорости передачи и возрастает вероятность ошибки .

B. к уменьшению вероятности ошибки

C. к уменьшению скорости передачи

11. К чему равна скорость передачи в системе ИКМ-30 (скорость пер-

вичного уплотнения)?

A. 1024 кбит/с

B. 2048 кбит/с

C. 5048 кбит/с.

12. Радиорелейная станция (РРС) состоит:

A. антенны мачтового сооружения

B. из узкого пучка радиоволн.

C. из оборудования, состоящие из передатчика, приемника и антенны

13. метод система передачи с частотным разделением каналов (СП с ЧРК).

A. с помощью мультиплексора все каналы объединяются в общий групповой поток с различными несущими частотами.

B. передается боковая полоса модулированного сигнала с несущей.

C. Каждый канал занимает весь спектр канала, но передается поочерёдно.

14. К чему равна динамический диапазон сигнала для ТЧ канала :

A. 50 дБ

B. 40 дБ

C. 48 дБ

15. Какая цифровая система передачи предназначена для организации пучков каналов ТЧ на местной и внутризоновой первичных сетях, обеспечивая передачу всех видов сигналов электросвязи?

A. магистральная цифровая система

B. $ первичная цифровая система

C. вторичная цифровая система

16. Что называется процессом восстановления формы импульса его амплитуды и длительности

A. Регенерацией

B. Кодированием

C. Дискретизацией

17. Какая скорость передачи стандартного цифрового канала?

A. 16 кбит/сек

B. 32 кбит/сек

C. 64 кбит/сек

18. Какая система исчисления используется для передачи цифровых сигналов?

A. Восьмеричная

B. Двоичная

C. шестнадцатеричная

19. Процесс преобразования во времени аналогового сигнала в последовательность импульсов называется

A. Дискретизацией

B. Модуляцией

C. Синхронизацией

20. назначение декодера

A. выполняет функцию дискретизации

B. выделяет полосу частот

C. преобразует цифровой сигнал в аналоговый

21. линейное затухание представляет собой:

A. равномерное уменьшение амплитуды сигнала, не зависящее от его частоты.

B.затухание, связанное с многолучевым прохождением сигнала;

C. методологию измерения радиочастотного тракта;

22. Процесс дискретизации сигнала по уровню носит название:

A. преобразованием

B. квантованием

C. дискретизацией

23. Погрешности при квантовании называют

A. уровни квантования

B. отсчеты квантования

C. шумы квантования

24. Совокупность сетевых узлов, сетевых станций и линий связи, образующих сеть групповых трактов и каналов передачи

A. первичная сеть электросвязи

B. сеть электросвязи

C. вторичная сеть электросвязи

25. Тип кабеля и схема организации связи являются определяющим фактором для определения

A. помехоустойчивости

B. дальности

C. качественной связи

26. Разность между значениями квантованного и неквантованного сигналов называется

A. Шагом квантования

B. Ошибкой квантования

C. Помехой квантования

27. Что такое синхронизация

A. процесс обеспечения равенства фазовых сдвигов и временных канальных интервалов

B. процесс установления и поддержания определенных временных соотношений между двумя и более процессами

C. процесс согласования различных узлов системы передачи

28. В состав тракта входят:

A. анализатор, ретранслятор и модем;

B. генератор и передатчик;

C. усилитель, фильтр и модулятор.

29. линейное затухание представляет собой:

A. равномерное уменьшение амплитуды сигнала, не зависящее от его частоты.

B. затухание, связанное с многолучевым прохождением сигнала;

C. методологию измерения радиочастотного тракта;

30. Какая наиболее важная характеристика качества цифровой системы передачи?

A. параметр ошибки;

B. мощность шумов;

C. АЧХ;

1	2	3	4	5	6	7	8	9
A	B	C	B	C	A	B	C	C
11	12	13	14	15	16	17	18	19
B	C	A	B	C	A	C	B	A
21	22	23	24	25	26	27	28	29
A	B	C	A	B	B	A	C	A

7.2.2 Примерный перечень заданий для решения стандартных задач

1. Определите, в соответствии с каким документом необходимо формировать требования по защите информации, не содержащей сведения, составляющие государственную тайну, если проектируемая ТКС в защищенном исполнении является государственной системой 1) В соответствии с законом РФ «Об информации, информационных технологиях и о защите информации», 2) В соответствии с нормативным правовым актом, введенным в действие приказом ФСТЭК России от 11 февраля 2013 г.№17.

Правильный – ответ №2

2. Определите, в соответствии с какими документами необходимо формировать требования по защите информации, не содержащей сведения, составляющие государственную тайну, если проектируемая ТКС является государственной системой и в ней будут обрабатываться персональные данные граждан 1) В соответствии с нормативным правовым актом, введенным в действие приказом ФСТЭК России от 11 февраля 2013 г.№17.

2) В соответствии с нормативным правовым актом, введенным в действие приказом ФСТЭК России от 18 февраля 2013 г.№21.

3) Выбираются наиболее жесткие требования, определенные в нормативно-правовых актах, утвержденных приказами ФСТЭК России от 11 фев-

раля 2013 г.№17 и от 18 февраля 2013 г. №21.

Правильный – ответ №3

3. ТКС относится к государственной информационной системе. Определите, какой класс защищенности она должна иметь, если в ней обрабатывается информация высокого уровня значимости и система относится к региональной 1) К1;

2) К2;

3) К3.

Правильный – ответ №1

4. В модернизируемой государственной ТКС обрабатывается информация, содержащая сведения, составляющие коммерческую тайну. Класс защищенности системы установлен К3. Межсетевой экран какого класса защиты должен быть установлен в ТКС, если она подключены к сети Internet

1) Третий;

2) Четвертый;

3) Пятый;

4) Шестой.

Правильный – ответ №4

5. В ТКС, обеспечивающей деятельность органа государственной власти, обрабатывается информация конфиденциального характера, содержащая сведения, составляющие служебную тайну. Можно ли в такой системе реализовать выход пользователей в сеть Internet 1) Нельзя,

2) Подключение к сети Internet допускается только с использованием специально предназначенных для этого средств защиты информации, в том числе шифровальных (криптографических) средств, прошедших в установленном законодательством Российской Федерации порядке сертификацию в ФСБ России

Правильный ответ №2

6. Укажите, на какой стадии проектирования новой ТКС и кто определяет перечень подлежащей защите информации1) При разработке замысла защиты разработчик СЗИ;

2) В ходе концептуального проектирования разработчик совместно с заказчиком;

3) Перечень информации, подлежащей защите, определяется на стадии формирования требований к СЗИ и, при необходимости, уточняется на последующих стадиях ее создания. Применительно к конкретной СЗИ перечень защищаемой информации устанавливает заказчик.

Правильный – ответ №3

7. Организацию посещают сотрудники обслуживающего предприятия, которые могут быть потенциальными нарушителями. К внешнему или внутреннему нарушителю относятся посетитель, если они попытался, используя компьютер сотрудника организации, получить доступ к базе данных организации 1) Внешний, так как он сотрудник другого предприятия;

2) Внутреннний, так как он действует внутри организации в пределах контролируемой территории.

Правильный – ответ №3

8. В организации оказался неблагонадежный сотрудник, который из своего дома попытался без разрешения проникнуть через Internet в компьютерную сеть организации. К внешнему или внутреннему нарушителю относится сотрудник организации 1) К внутреннему, так как он знает пароли доступа в операционную среду компьютерной сети;

2) К внешнему нарушителю, так как он действует извне, из-за пределов контролируемой зоны организации.

Правильный – ответ №2

9. В ТКС установлен межсетевой экран. Может ли внешний абонент связаться через сеть Internet с пользователем ТКС 1) Нет не может, так как МЭ будет блокировать попытки установления такой связи, если в его настройках отсутствует перечень разрешенных сетевых адресов;

2) В любом случае может, если внешний абонент ранее связывался с данным пользователем.

Правильный – ответ №1

10. Укажите, по каким признакам программу можно отнести к вредоносной 1) Любая программа, с помощью которой можно не санкционировано копировать, уничтожать, модифицировать защищаемую информации относится к вредоносной;

2) Программой с потенциально опасными последствиями или вредоносной программой называют некоторую самостоятельную программу (набор инструкций), которая способна выполнять любое непустое подмножество следующих функций:

- скрытия признаков своего присутствия в программной среде компьютера;

- самодублирования, ассоциирования себя с другими программами и (или) переноса своих фрагментов в иные области оперативной или внешней памяти;

- разрушения кода программы;

- выполнения без инициирования со стороны пользователя (пользовательской программы в штатном режиме ее выполнения) деструктивных функций (копирования, уничтожения, блокирования, запуска приложений и т.п.);

- сохранения фрагментов информации из оперативной памяти в некоторых областях внешней памяти прямого доступа;

- искажения произвольным образом, блокирования и (или) подмены выводимого во внешнюю память или в канал связи массива информации, образовавшегося в результате работы прикладных программ, или уже находящихся во внешней памяти массивов данных;

- подавления информационного обмена в ИС

Правильный – ответ №2

7.2.3 Примерный перечень заданий для решения прикладных задач

1. В проектируемой ТКС будут подлежать защите подлежат общедоступные персональные данные менее 1000 сотрудников. Определите требуемый уровень защищенности ТКС

1) Первый;
2) Второй;
3) Третий;
4) Четвертый

Правильный – ответ №4

2. ТКС относится к муниципальной информационной системе. Нарушение конфиденциальности, целостности или доступности обрабатываемой в ней информации может вызвать негативные (умеренные) социальные последствия в городе. Определите требуемый класс защищенности этой системы

1) К1;
2) К2;
3) К3.

Правильный – ответ №2

3. Проектируемая ТКС относится к государственной информационной системе и имеет 2 класс защищенности. Определите, какой класс защиты должен иметь устанавливаемый в ней межсетевой экран 1) Первый;

2) Второй;
3) Третий;
4) Четвертый;
5) Пятый;
6) Шестой.

Правильный – ответ №5

4. Укажите задачи, которые могут решаться при защите от вредоносных программ (ВП) на системном и прикладном системно-технических уровнях

Основными задачами, которые решаются средствами защиты от ВП, являются:

-активный аудит функционирования всех элементов ТКС, в том числе контроль и анализ действий пользователей, операционной системы, СУБД, других приложений, формирование статистических данных о функционировании;

-анализ элементов ТКС на наличие известных уязвимостей, определение ошибок в конфигурации и (возможно) их исправление;

-распознавание сигнатур ВП и оповещение о факте попытки внедрения или внедрения ВП;

-оценка целостности операционной системы, СУБД, файлов баз данных, в частности, выявление изменений файлов данных;

-хранение и постоянное обновление сигнатур известных ВП;

-обеспечение администраторов безопасности информации данными об уже происшедших попытках внедрения ВП, с целью ускорить диагностику функционирования оборудования и программного обеспечения, а при необходимости и восстановления рабочего состояния подвергшейся воздействию

отдельной рабочей станции или сети в целом;

-тестирование средств защиты от ВП;

5. оперативное блокирование функционирования элементов ТКС при обнаружении опасных ВП

В проектируемой ТКС обрабатывается информация конфиденциального характера, являющаяся государственным информационным ресурсом. Какой класс защищенности должна иметь система обнаружения вторжений

1)Первый;

2)Второй;

3)Третий;

4)Четвертый;

5)Пятый;

6)Шестой.

Правильный – ответ № 4

6. В проектируемой ТКС необходимо разграничить доступ пользователей к информации, не содержащей сведения, составляющие государственную тайну, и к функциям ее обработки. Определите, какую технологию целесообразно использовать для разграничения доступа

1) Ввести пароли для пользователей;

2) Установить и настроить соответствующим образом межсетевые экраны рабочих станций;

3) Применить технологию «Тонкий клиент».

Правильный – ответ №3

7. В модернизируемой ТКС обрабатывается информация, содержащая сведения, составляющие государственную тайну. Каким образом можно обеспечить работу пользователей этой системы в сети Internet.

1) Нельзя,

2) Применить межсетевой экран 1 класса защищенности;

3) Установить средства криптографической защиты трафика, сертифицированные ФСБ России.

Правильный - ответ №3

8. В проектируемой ТКС для скрытия трафика, передаваемого через сеть Internet, предполагается применить технологию VPN, при этом конечными точками защищенного туннеля выступают провайдеры сети Internet. Определите, при каком условии такое решения является допустимым

1) Ни при каких условиях;

2) Если канал от абонента до провайдера при передаче трафика и от провайдера до абонента при его приеме не считается необходимым защищать или он является защищенным.

Правильный – ответ №2

9. Как определяется класс защищенности проектируемой ТКС, относящей к государственной, в которой обрабатывается информация, не содержащая сведения, составляющие государственную тайну

1) По решению обладателя ТКС;

2) В соответствии с нормативным правовым актом «Требования о за-

щите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденный приказом ФСТЭК России от 11 февраля 2013 г. №17 и следующей таблицей

Правильный – ответ №2

10. Определите состав функциональных подсистем, которые Вы бы включили в систему защиты проектируемой ТКС органа государственной власти, имеющей выход в Internet

1) Подсистемы регистрации и учета, контроля целостности, контроля доступа, антивирусной защиты;

2) Подсистемы регистрации и учета, контроля целостности, разграничения доступа, сигнализации и блокирования, антивирусной защиты, обнаружения вторжений, тестирования и анализа защищенности, доверенной загрузки, защиты информации от ее утечки во внешние сети.

Правильный – ответ №2

7.2.4 Примерный перечень вопросов для подготовки к зачету

Трактовка понятий «защита информации», «безопасность информации», «защищенность информации», «обеспечение безопасности информации», «информационная безопасность», «несанкционированный доступ», «эффективность защиты», «политика безопасности информации» или «политика информационной безопасности». Понятие системы защиты информации (СЗИ). Организационная, организационно-техническая и техническая СЗИ

Основные подходы к проектированию систем защиты информации (СЗИ): восходящее и нисходящее проектирование, проектирование на основе предварительного установления приоритетов и комбинированный подход. Порядок проектирования СЗИ в соответствии с ГОСТ Р 51583-2014. Содержание комплексов работ при проектировании. Общие требования к созданию СЗИ при модернизации ТКС. Стадии и этапы создания СЗИ для модернизируемой ТКС и содержание работ на них. Особенности проектирования СЗИ при создании новой ТКС в защищенном исполнении. Распределение ответственности организаций и должностных лиц при проектировании ТКС в защищенном исполнении

Понятие угрозы безопасности информации. Структура описание угрозы безопасности информации. Внешние и внутренние источники угроз. Типы внешних и внутренних нарушителей. Общая характеристика программных и программно-аппаратных закладок. Понятие уязвимости, виды уязвимостей. Структура записи уязвимости в базе CVE. Содержание несанкционированных действий. Схема общей классификации угроз безопасности информации. Понятие сетевой атаки. Классификация сетевых атак. Понятие базовой и частной модели угроз. Порядок анализа угроз и формирования частных моделей угроз.

7.2.5 Примерный перечень заданий для решения прикладных задач

Этапы реализации типовой сетевой атаки и содержание действий на каждом этапе. Классификационные схемы способов реализации атак. Содержание способов реализации сетевых атак на сетевом, системном и прикладном системно-технических уровнях с использованием протоколов типа FTP, Telnet, SMTP, HTTP, DNS, UDP, TCP, IP, ICMP, ARP, RIP и OSPF. Причины, обусловившие возможность реализации сетевых атак. Понятие вредоносной программы. Общая классификация и основные виды ВП. Краткая характеристика основных ВП: файловых, загрузочных вирусов и макровирусов, сетевых червей, программных закладок и иных вредоносных программ. Резидентные и нерезидентные вирусы. Приемы инфицирования ТКС. Способы скрытия факта инфицирования ТКС. Полиморфик-вирусы, стелс-вирусы, руткиты. Направления развития ВП

Классы угроз безопасности информации, парируемых с использованием мер и средств защиты от НСД в ТКС. Общая классификационная схема для мер защиты информации в ТКС и ее элементах. Организационные, организационно-технические и технические меры защиты информации. Средства защиты от непосредственного виртуального доступа и воздействия вредоносными программами. Меры защиты информации от несанкционированного доступа, обусловленного применением сетевых технологий взаимодействия. Меры защиты информации при передаче по каналам связи Понятие межсетевого экрана (МЭ). Группы функций фильтрации и посредничества, реализуемые МЭ. Виды межсетевых экранов (экранирующие маршрутизаторы; шлюзы сеансового уровня; прикладные шлюзы) и реализуемые ими функции. Требования к МЭ и способы их применения

Система нормативных документов ФСТЭК России, регламентирующих требования по защите информации в ТКС. Основные аспекты защиты информации, регулируемые нормативными документами. Понятие класса (уровня) защищенности телекоммуникационной системы. Краткая характеристика и основные положения нормативных документов, введенных в действие приказами ФСТЭК России от 11 февраля 2013 г. №17, от 18 февраля 2013 г. №21, а также руководящих документов «Автоматизированные системы. Защита от НСД к информации. Классификация автоматизированных систем и требования по защите информации» и «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности». Порядок формирования требований по защите информации в соответствии с указанными документами. Порядок задания требований к мерам и средствам защиты информации в соответствии с действующими документами ФСТЭК России на примере нормативного правового акта, утвержденного приказом ФСТЭК России от 11 февраля 2013 г. №17. Базовый набор мер защиты, его адаптация, дополнение и уточнение, определение компенсирующих мер защиты. Понятие системы защиты информации. Состав возможных подсистем защиты.

7.2.6. Методика выставления оценки при проведении промежу-

точной аттестации

Экзамен проводится по тест-билетам, каждый из которых содержит 10 вопросов и задачу. Каждый правильный ответ на вопрос в тесте оценивается 1 баллом, задача оценивается в 10 баллов (5 баллов верное решение и 5 баллов за верный ответ). Максимальное количество набранных баллов – 20.

1. Оценка «Неудовлетворительно» ставится в случае, если студент набрал менее 6 баллов.

2. Оценка «Удовлетворительно» ставится в случае, если студент набрал от 6 до 10 баллов

3. Оценка «Хорошо» ставится в случае, если студент набрал от 11 до 15 баллов.

4. Оценка «Отлично» ставится, если студент набрал от 16 до 20 баллов.)

7.2.7 Паспорт оценочных материалов

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции	Наименование оценочного средства
1	Основные понятия, касающиеся технологии проектирования ТКС в защищенном исполнении	ОПК-13, ОПК-16	Тест, контрольная работа, защита практических работ, требования к курсовому проекту
2	Методология и технологическая схема проектирования ТКС в защищенном исполнении	ОПК-13, ОПК-16	Тест, контрольная работа, защита практических работ, требования к курсовому проекту
3	Классификация угроз безопасности в телекоммуникационных системах и основы методологии их анализа	ОПК-13, ОПК-16	Тест, контрольная работа, защита практических работ, требования к курсовому проекту
4	Типовые сетевые атаки и способы из реализации в современных телекоммуникационных системах. Угрозы применения вредоносных программ (ВП) и способы защиты от них	ОПК-13, ОПК-16	Тест, контрольная работа, защита практических работ, требования к курсовому проекту
5	Меры и средства защиты информации от угроз НСД в ТКС. Общая характеристика и классификация. Межсетевые экраны. Основы функционирования	ОПК-13, ОПК-16	Тест, контрольная работа, защита практических работ, требования к курсовому проекту
6	Нормативное обеспечение обоснования требований по защите информации от НСД в ТКС. Порядок задания требований по защите информации к ТКС, выбора мер и средств защиты и построения систем защиты	ОПК-13, ОПК-16	Тест, контрольная работа, защита практических работ, требования к курсовому проекту

7.3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Тестирование осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных тест-заданий на бумажном носителе. Время тестирования 30 мин. Затем осуществляется проверка теста экзаменатором и выставляется оценка согласно методики вы-

ставления оценки при проведении промежуточной аттестации.

Решение стандартных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

Решение прикладных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

Защита курсовой работы, курсового проекта или отчета по всем видам практик осуществляется согласно требованиям, предъявляемым к работе, описанным в методических материалах. Примерное время защиты на одного студента составляет 20 мин.

8 УЧЕБНО МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ)

8.1 Перечень учебной литературы, необходимой для освоения дисциплины

Основная литература

1. Крук Б.И, Попантонопуло В.Н., Шувалов В.П. Телекоммуникационные системы и сети: Учебное пособие. В 3 томах. Том 1 – Современные технологии. Под ред. профессора Шувалова В.П. – М.: Горячая линия–Телеком, 2003. –647 с.: ил.

2. Олифер В., Олифер Н. Компьютерные сети: принципы, технологии, протоколы. – СПб: Издательство: Питер, 2016. – 991 с.

3. Таненбаум Э. Компьютерные сети. – СПб: Издательство: Питер, 2016. – 955 с.

Дополнительная литература

1. Голиков, А. М. Основы проектирования защищенных телекоммуникационных систем: учебное пособие / А. М. Голиков. — Москва: ТУСУР, 2016. — 396 с. — Текст: электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/110273

2. Голиков, А. М. Системы цифровой радиосвязи: учебник / А. М. Голиков. — Москва: Ай Пи Ар Медиа, 2022. — 340 с. — ISBN 978-5-4497-1532-6. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/117865.html

8.2 Перечень информационных технологий, используемых при

осуществлении образовательного процесса по дисциплине, включая перечень лицензионного программного обеспечения, ресурсов информационно-телекоммуникационной сети «Интернет», современных профессиональных баз данных и информационных справочных систем:

http://eios.vorstu.ru/
http://www.studentlibrary.ru/
http://znanium.com/
http://ibooks.ru/
http://e.lanbook.com/;
http://www.iprbookshop.ru/

9 МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

Компьютерный класс, оснащенный рабочими местами на базе вычислительной техники с установленным программным обеспечением, предназначенным для моделирования компьютерных сетей.

10. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

По дисциплине «Проектирование защищенных телекоммуникационных систем» читаются лекции, проводятся практические занятия, выполняется курсовой проект.

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

Практические занятия направлены на приобретение практических навыков расчета и измерения характеристик элементов современных систем связи; проектирования и разработки отдельных типовых элементов защищенных телекоммуникационных систем; защитt информации и каналов связи в различных условиях.

Занятия проводятся путем решения конкретных задач в аудитории.

Методика выполнения курсового проекта изложена в учебно-методическом пособии. Выполнять этапы курсового проекта должны своевременно и в установленные сроки.

Контроль усвоения материала дисциплины производится проверкой курсового проекта, защитой курсового проекта.

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. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначение вопросов, терминов, материала, которые вызывают трудности, поиск ответов в рекомендуемой литературе. Если само-

	стоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на лекции или на практическом занятии.
Практическое занятие	Конспектирование рекомендуемых источников. Работа с конспектом лекций, подготовка ответов к контрольным вопросам, просмотр рекомендуемой литературы. Прослушивание аудио- и видеозаписей по заданной теме, выполнение расчетно-графических заданий, решение задач по алгоритму.
Самостоятельная работа	Самостоятельная работа студентов способствует глубокому усвоения учебного материала и развитию навыков самообразования. 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; - участие в работе студенческих научных конференций, олимпиад; - подготовка к промежуточной аттестации.
Подготовка к промежуточной аттестации	Готовиться к промежуточной аттестации следует систематически, в течение всего семестра. Интенсивная подготовка должна начаться не позднее, чем за месяц-полтора до промежуточной аттестации. Данные перед зачетом, экзаменом три дня эффективнее всего использовать для повторения и систематизации материала.