МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Воронежский государственный технический университет»

УТВЕРЖДАЮ

Декан факультета ФИТКБ

_____ /Бредихин А.В./

28.08.2025 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Информационная безопасность 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 _____ О.В. Исаев

Заведующий кафедрой Систем информационной безопасности _____ А.Г. Остапенко

Руководитель ОПОП _____ С.С. Куликов

Воронеж 2025

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1. Цели дисциплины

Цель изучения дисциплины – формирование у учащихся знаний о способах, мерах и средствах защиты информации от угроз безопасности информации в телекоммуникационных системах (ТКС), развитие практических навыков обоснования требований к средствам и системам защиты, а также способностей к решению прикладных задач анализа и контроля защищенности ТКС.

1.2. Задачи освоения дисциплины

- освоение методологических основ анализа защищенности информации в ТКС,
- приобретение навыков формирования требований по защите информации в ТКС, предъявляемых действующими нормативными документами, и выбора мер и средств защиты информации;
- формирование представлений о системах защиты информации в составе ТКС, о способах контроля защищенности информации в ТКС и порядке его организации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Информационная безопасность телекоммуникационных систем» относится к дисциплинам части, формируемой участниками образовательных отношений блока Б1.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ОПОП

Компетенция	Результаты обучения, характеризующие сформированность компетенции
ПК-9.4	**Знать**: особенности построения защищённых телекоммуникационных комплексов; принципы обнаружения признаков компьютерных атак в высокоскоростных сетях. **Уметь**: разрабатывать системы и средства защиты телекоммуникационных комплексов, включая шлюзы безопасности и системы обнаружения вторжений. **Владеть**: навыками создания интегрированных решений для защиты сетей электросвязи с повышенными требованиями к безопасности.

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Информационная безопасность телекоммуникационных систем» составляет 14 з.е.

Распределение трудоемкости дисциплины по видам занятий,

очная форма обучения

Виды учебной работы	Всего часов	Семестры	
		9	10
Аудиторные занятия (всего)	126	36	90
В том числе:			
Лекции	54	18	36
Лабораторные работы (ЛР)	72	18	54
Самостоятельная работа	306	90	216
Часы на контроль	72	36	36
Виды промежуточной аттестации - экзамен	+	+	+

Общая трудоемкость: академические часы зач.ед.	504 14	162 4.5	342 9.5

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	Лаб. зан.	СРС	Всего, час
1	Основные направления защиты информации в ТКС и их общая характеристика	Понятия «комплексной защиты информации» и «системы защиты информации» в ТКС. Модели безопасности информации в ТКС (КДЦ, гексада Паркера, модель STRIDE). Основные направления защиты информации от угроз антропогенного и неантропогенного характера, связанные с перехватам трафика в ТКС, проникновения в операционные среды хостов ТКС и др.	3	4	19	26
2	Стратегии защиты информации в ТКС и их общая характеристика	Понятие стратегии защиты и классификация возможных стратегий по признакам организации защиты, направленности действий, адаптивности. Характеристика существующих и перспективных стратегий защиты информации в ТКС	3	4	19	26
3	Принципы построения системы защиты информации (СЗИ) в ТКС и разграничения доступа	Основные принципы создания СЗИ в ТКС: системности, комплексности, непрерывности защиты, разумной достаточности, гибкости управления, открытости алгоритмов и механизмов защиты, простоты применения защитных мер и средств. Типовая структура системы защиты информации в ТКС. Принципы централизованного, децентрализованного построения СЗИ и смешанный принцип построения. Принципы разграниче-	3	4	19	26
		ния доступа (дискреционный, мандатный, ролевой, разграничения информационных потоков и изолированной среды) и их краткая характеристика				
4	Модели разграничения доступа к информации в информационных системах и обеспечения ее целостности	Назначение формальных моделей разграничения доступа к информации. Модель Харрисона-Руззо-Ульмана для дискреционного принципа разграничения доступа и ее характеристика. Модель Белла-ЛаПадула для мандатного принципа разграничения доступа и ее характеристика. Содержание основной теоремы безопасности. Понятие целостности данных. Формальные модели Биба и Кларка-Вилсона и их краткая характеристика. Теоретические принципы обеспечения целостности данных Д.Кларка и Д. Вилсона	3	4	19	26
5	Состав и структура систем защиты информации (СЗИ) в ТКС с использованием централизованного принципа построения	СЗИ в ТКС на основе централизации управления ею. Понятие эшелонированной защиты и пути ее построения. Роль администратора безопасности при решении задач защиты информации в ТКС. Достоинства и недостатки СЗИ с централизованным принципом постреония.	3	4	19	26
6	Подсистемы защиты информации от угроз непосредственного несанкционированного доступа (НСД)	Разделение НСД на физический и виртуальный. Основные функции подсистем защиты от физического доступа. Основные классы устройств защиты от физического НСД и их характеристика. Средства защиты от непосредственного виртуального НСД, реализуемые операционной системой компьютера, и специальные программы, программные и программно-аппаратные комплексы и их характеристика	3	4	19	26

7	Основы обеспечения безопасности информации в ТКС от сетевых атак.	Классификация мер защиты от сетевых атак. Меры защиты информации от перехвата при передаче по сетям. Меры защиты информации от сетевых атак, реализуемых на системном и прикладном уровнях путем проникновения в операционную среду элементов ТКС. Три группы методов обнаружения вторжений в операционную среду хостов ТКС: сигнатурные, выявления аномалий и комбинированные. Классификация систем обнаружения вторжений (СОВ). Требования к СОВ определены в нормативно-правовом акте «Требования к системам обнаружения вторжений», утвержденном приказом ФСТЭК России от 6 декабря 2011 г. № 638	3	4	19	26
8	Средства и системы обнаружения вторжений при реализации сетевых атак в ТКС	Классификация систем обнаружения вторжений (СОВ). Требования к СОВ, определенные в нормативно-правовом акте «Требования к системам обнаружения вторжений», утвержденном приказом ФСТЭК России от 6 декабря 2011 г. № 638. Основы построения СОВ.	3	4	19	26
9	Средства антивирусной защиты, требования к ним и способы применения	Понятие средства защиты от вредоносных программ (СЗВП) и средства антивирусной защиты (САВЗ). Классификация мер и средств антивирусной защиты. Задачи, решаемые с применением СЗВП. Типы САВЗ и классы защиты СЗВП. Требования к СЗВП и САВЗ, определенные в нормативно-правовом акте ФСТЭК России, утвержденном приказом ФСТЭК России от 20.03.2012 г. №28	3	4	19	26
10	Система нормативных правовых документов, содержащих требования по защиты информации в ТКС	Общий порядок обоснования требований по защите информации в ТКС. Состав и структура системы документов по технической защите информации в ТКС ФСТЭК России и их краткая характеристика. Классификация ТКС по классам защищенности. Порядок выбора нормативных документов при организации защиты информации в ТКС.	6	8	19	33
11	Нормативное регулирование требований к средствам защиты информации в ТКС	Состав и структура системы документов, содержащих требования к средствам защиты информации в ТКС. Классы защиты. Общий порядок обоснования требований к средствам защиты информации в ТКС.	3	4	19	26
12	Государственный стандарт ИСО/МЭК 15408 «Общие критерии»	Краткая история разработки международного стандарта ИСО/МЭК 15408 «Общие критерии», его назначение и структура. Основные понятия, введенные стандартом (задача защиты, профиль защиты, задание по безопасности). Структура профиля защиты и задания по безопасности. Понятие функционального требования и требования доверия. Классы функциональных требований и требований доверия	3	4	20	27
13	Технологии мониторинга и пресечения инцидентов информационной безопасности в ТКС	Понятие инцидента информационной безопасности в ТКС и краткая характеристика возможных инцидентов. Способы и средства своевременного выявления инцидентов безопасности в распределенных ТКС. Понятие скрытного канала несанкционированной передачи данных во внешние сети и пути его построения. Особенности выявления скрытных каналов передачи данных с использованием стеганографии. Перспективные SIEM и SOC-системы и их краткая характеристика	6	8	20	34
14	Существующие и перспективные системы защиты с использованием децентрализованного принципа построения.	Краткая характеристика систем защиты информации в ТКС с использованием децентрализованного принципа построения. Основные представления о технологиях «Тонкий клиент» и «Многоагентная система защиты».	3	4	19	26

15	Технологии создания доверенных сред и перспективы их развития	Понятие доверенной среды. Общая классификационная схема современных технологий создания доверенных вычислительных сред. Доверенный платформенный модуль и его применение в интересах формирования доверенной среды. Перспективы внедрения новых технологий типа Vpro, Presidio. Варианты построения терминальных систем на базе «Тонкого клиента». Применение нейросетевой биометрической идентификации для создания доверенных сред	3	4	19	26
16	Организация и порядок проведения контроля эффективности защиты информации в телекоммуникационных системах	Понятие контроля эффективности защиты информации в ТКС. Основные виды контроля. Организационный и технический контроль эффективности. Задачи контроля и порядок его организации. Средства контроля и возможности их применения на функционирующих ТКС	3	4	19	26
		Итого	**54**	**72**	**306**	**432**

5.2 Перечень лабораторных работ

1. Формирование правил дискреционного и мандатного разграничения доступа к защищаемой информации в хостах ИТКС на основе требований моделей Харрисона-Руззо-Ульмана и Белла ЛаПадулла.

2. Определения перечня уязвимостей системного программного обеспечения на примере операционной системы «Windows 8.1» с использованием базы уязвимостей ФСТЭК России.

3. Формирование состава актуальных угроз безопасности информации в ИТКС предприятия (организации) с использованием базы данных угроз ФСТЭК России по вариантам: а) предприятия кредитно-финансовой сферы; б) муниципального органа; в) лечебного учреждения.

4. Определение путей построения эшелонированной защиты информации от угроз безопасности информации, реализуемых из сети Internet, в государственной информационно-телекоммуникационной системе.

5. Определение путей построения эшелонированной защиты информации от угроз безопасности информации, реализуемых из сети Internet, в информационной системе персональных данных промышленного предприятия.

6. Определение путей построения подсистемы защиты информации от угроз, реализуемых внутренним нарушителем в ИТКС органа власти.

7. Определение требований и функционального облика подсистемы антивирусной защиты в государственной ИТКС.

8. Определение требований и путей построения централизованной подсистемы обнаружения вторжений в составе информационной системы государственной поликлиники.

9. Разработка предложений по построению децентрализованной системы обнаружения вторжений с использованием технологии «многоагентной системы».

10. Обоснование класса защищенности и состава мер и средств защиты для системы пресечения несанкционированной передачи информации в сеть Internet в составе корпоративной ИТКС предприятия.

11. Определение требований и функционального облика подсистемы защиты информации от угроз, реализуемых внешним нарушителем в ИТКС органа власти.

12. Формирование профиля защиты информации от угроз, реализуемых внешним нарушителем в ИТКС предприятия, на основе стандарта ИСО/ МЭК 15408.

13. Формирование системы защиты информации в ИТКС предприятия на основе реализации технологии «Тонкий клиент».

14. Формирование системы защиты информации в ИТКС предприятия на основе реализации технологии «многоагентной системы».

15. Определение функционального облика SIEM-системы для защиты от несанкционированной передачи информации из ТКС органа власти во внешние сети.

16. Построение доверенной среды в хосте ТКС на основе средств нейросетевой идентификации.

17. Способы применения средств контроля защищенности персональных данных в ТКС лечебного учреждения.

18. Определение состава и структуры подсистемы контроля защищенности информации в информационной системе промышленного предприятия.

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

В соответствии с учебным планом освоение дисциплины не предусматривает выполнение курсового проекта (работы) или контрольной работы.

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
ПК-9.4	Знать: особенности построения защищённых телекоммуникационных комплексов; принципы обнаружения признаков компьютерных атак в высокоскоростных сетях.	Тест	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Уметь: разрабатывать системы и средства защиты телекоммуникационных комплексов, включая шлюзы безопасности и системы обнаружения вторжений.	Решение стандартных практических задач	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Владеть навыками: навыками создания интегрированных решений для защиты сетей электросвязи с повышенными требованиями к безопасности.	Решение прикладных практических задач	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

Тестирование осуществляется путем задания вопросов и устных ответов на них студента как в ходе лекций, так и при проведении практических занятий, а стандартные и прикладные практические задачи решаются в ходе практических занятий в течение семестра

Для определения показателей начисляется количество баллов за ответы на вопросы при тестировании и за решение стандартных и прикладных практических задач следующим образом:

при тестировании за N % правильных ответов от общего количества вопросов выставляется N баллов, при этом правильным считается полный ответ без ошибок (если ответ неполный или содержит ошибки, то он не засчитывается);

при решении стандартных практических задач за M % правильно решенных задач выставляется M баллов;

при решении прикладных практических задач за D % правильно решенных задач выставляется D баллов;

Далее вычисляется приведенная сумма:

$S = \dfrac{N + M + D}{K}$, где K – количество формируемых компетенций (в данном случае $K = 4$)

Принятие решения об аттестации осуществляется по следующему критерию:

если $S \geq 70$, то принимается положительное решение об аттестации;

если $S < 70$, то студент не аттестуется.

7.1.2 Этап промежуточного контроля знаний

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

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

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Отлично	Хорошо	Удовл.	Неудовл.
ПК-9.5	Знать: особенности построения защищённых телекоммуникационных комплексов; принципы обнаружения признаков компьютерных атак в высокоскоростных сетях.	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70- 80%	В тесте менее 70% правильных ответов

	Уметь: разрабатывать системы и средства защиты телекоммуникационных комплексов, включая шлюзы безопасности и системы обнаружения вторжений.	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: навыками создания интегрированных решений для защиты сетей электросвязи с повышенными требованиями к 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

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

8.2.1 Примерный перечень заданий для подготовки к тестированию

Содержание задания	Варианты ответа
1. Что понимается под комплексным обеспечением безопасности информации	Варианты ответов: 1) под комплексным обеспечением безопасности информации понимается совокупность мер кадрового, технического, программного, материального и т.д. видов обеспечения; 2) под комплексным обеспечением безопасности информации понимается совокупность мер, во-первых, охватывающих все актуальные для данной ТКС угрозы безопасности информации, во-вторых, реализуемых на нескольких этапах жизненного цикла ТКС и согласованных по цели, задачам, месту и времени проведения; Правильный ответ – ответ №2
2. Какие аспекты организации защиты информации охватывает комплексное обеспечение безопасности информации в ТКС	Варианты ответов: 1) комплексное обеспечение безопасности информации в ТКС охватывает следующие основные аспекты организации: подготовку кадров, создание системы защиты от совокупности угроз, ее аттестацию и принятие в эксплуатацию; 2) комплексное обеспечение безопасности информации в ТКС охватывает следующие основные аспекты организации: оценку обстановки (анализ угроз безопасности информации, оценку защищенности ТКС, оценку достаточности принятых мер защиты информации), обоснование требований по защите инфор-
	мации, формирование замысла защиты и выбор целесообразных мер защиты, построение системы защиты информации в ТКС, ее аттестацию и принятие в эксплуатацию. Правильный ответ – ответ №2

3. Какие учитываемые нарушения безопасности отличают гексаду Паркера от модели КДЦ?	Варианты ответа: 1) гексада Паркера охватывает те же нарушения, что и модель КДЦ, то есть нарушения конфиденциальности, целостности и доступности; 2) гексада Паркера охватывает те же нарушения, что и модель КДЦ, а также нарушения аутентичности, владения/ контроля, а также нарушение полезности. Правильный ответ – ответ №2
4. Какая стратегия направлена на защиту от внешнего нарушителя: периметровая или эшелонированная?	Варианты ответа: 1) только периметровая; 2) только эшелонированная: 3) и периметровая и эшелонированная. Правильный ответ – ответ №3
5. Что отличает систему защиты информации от комплекса средств защиты информации?	Варианты ответа: 1) Это одно и то же; 2) В системе защиты обязательной подсистемой является подсистема управления защитой. Если в комплексе средств защиты есть подсистема управления, то такой комплекс является системой Правильный ответ – ответ №2
6. Чем отличается управление защитой при централизованном и при децентрализованном принципах построения системы защиты	Варианты ответа: 1) при централизованном принципе управления решения по управлению защитой принимаются администратором безопасности, а при децентрализованном – пользователями рабочих станций; 2) при централизованном принципе управления средства и подсистемы защиты связаны с консолью администратора сети или администратора безопасности, откуда осуществляется управление настройками, конфигурациями. При децентрализованном принципе управления Средства и подсистемы защиты связаны с консолью администратора сети или администратора безопасности лишь для передачи сигнализационной информации, функционируют по заранее определенным алгоритмам. Управление осуществляется программными компонентами, установленными как в средствах, так и в подсистемах защиты. Правильный ответ – ответ №2
7. Что относится к атрибутивным средствам контроля доступа?	Варианты ответа: 1) к атрибутивным средствам контроля доступа относятся те, которые имеют сертификаты; 2) к атрибутивным средствам контроля доступа относятся специальные карты, документы, ключи и жетоны. Правильный ответ – ответ №2
8. Зачем нужны формальные модели разграничения доступа?	Варианты ответа: 1) для того, чтобы количественно обосновывать возможность доступа к информации; 2) для того, чтобы на формальной основе доказывать принципиальную возможность несанкционированного доступа к защищаемой информации. Правильный ответ – ответ №2
9. Какие абстрактные теоретические принципы сохранения целостности данных Вы знаете?	Ответ: В соответствии с моделью Кларка и Вилсона существует 9 абстрактных теоретических принципа: корректность транзакций; аутентификация пользователей; минимизация привилегий; разграничение функциональных обязанностей; аудит произошедших событий; объективный контроль; управление передачей привилегий; обеспечение непрерывной работоспособности; простота использования защитных механизмов
10. Чем отличается профиль защиты от задания по безопасности?	Варианты ответа: 1) ничем; 2) составом требований; 3) задание по безопасности, наряду с разделами, имеющимися в профиле защиты имеет также спецификации средств защиты, обоснование соответствия ИТ-продукта задачам защиты из Профиля защиты и указанным в нем требованиям «Общих критериев» Правильный ответ – ответ №3
11. Сколько классов функциональных требований определено в стандарте ИСО/МЭК 15408?	Варианты ответов: 1) 6 классов; 2) 4 класса; 3) 11 классов. Правильный ответ – ответ №3

12. Зачем нужна дифференциация требования к системам обнаружения атак?	Варианты ответов: 1) для того, чтобы можно было подобрать средства зашиты; 2) в соответствии с действующими документами дифференциация требований осуществляется для информационной системы в целом в зависимости от ее масштаба, и важности обрабатываемой в ней информации по классам защищенности. Избыточность или завышенность требований может привести к излишним затратам. Правильный ответ – ответ №2
13. Чем контроль организации защиты информации отличается от организационного контроля?	1) Разницы нет; 2) Контроль организации заключается в проверке организации работ по защите информации, наличия органов (подразделений) защиты информации, включения задач защиты информации в положения о подразделениях и в функциональные обязанности должностных лиц, наличия и содержания организационно-распорядительных документов (приказов, руководств, положений, инструкций) на соответствие требованиям правовых и нормативных документов в области защиты информации, порядка и своевременности их доведения до исполнителей и подведомственных организаций, наличия и полноты планов работ по технической защите информации и контролю ее эффективности, а также состояния их выполнения. Организационный контроль эффективности защиты информации заключается в проверке полноты и обоснованности мероприятий по защите информации требованиям организационно-распорядительных и нормативных документов в области защиты информации.

8.2.2. Примерный перечень заданий для решения стандартных задач

№№ п/п	Задание при решении стандартных практических задач	Варианты ответа
1.	Определите, какую модель безопасности следует рассматривать, если в качестве нарушения фигурирует несанкционированное повышение привилегий	Варианты ответа: 1) таких моделей безопасности не существует; 2) нужно рассматривать модель STRIDE, учитывающую этот вид нарушения. Правильный ответ – ответ №2
2.	Определите, какие подсистемы защиты информации в ТКС сегодня рассматриваются в составе СЗИ по сравнению с тем их составом, который описан в РД АС 1992 г.	Варианты ответа: 1) сегодня состав подсистем дополнился только подсистемами антивирусной защиты и обнаружения вторжений; 2) сегодня дополнительно рассматриваются целый ряд подсистемы, к основным из которых относятся такие как подсистемы защиты от физического доступа, сигнализации и блокирования, защиты от вредоносных программ, обнаружения вторжений, антивирусной защиты, отвлечения на ложный информационный ресурс, защиты от несанкционированной передачи информации во внешние сети, обеспечения доверенной загрузки операционной среды, контроля съемных носителей информации Правильный ответ – ответ №2
3.	ТКС относится к государственной информационной системе , в которой обрабатывается конфиденциальная информации, не относящаяся к государственной тайне, но являющаяся государственным информационным ресурсом. Определите, какой класс защищенности системы обнаружения вторжений должен быть для установки в эту ТКС	Варианты ответа: 1) 5 класс; 2) 4 класс. Правильный ответ – ответ №2
4.	ТКС относится к информационной системе персональных данных класса К1. Определите, какие типы средств антивирусной защиты должны быть установлены в ТКС и какого класса защиты.	Варианты ответа 1) необходимо установить серверные средства антивирусной защиты, то есть типа Б класса защиты 1; 2) необходимо установить средства антивирусной защиты типа Б и В четвертого класса защиты Правильный ответ №2

5.	В ТКС 3 класса защищенности обрабатывается информация конфиденциального характера, содержащая сведения, составляющие служебную тайну. Определите, какие меры защиты должны быть в ней реализованы при наличии выхода в сеть Internet	Варианты ответов: 1) – использовать сеть Internet 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 – ответ №2
6.	Укажите основные принципы разграничения доступа к информации в ТКС	Варианты ответа: 1 – принцип обладателя информации, принцип наличия у пользователя разрешение на ознакомление с информацией; 2 – дискреционный, мандатный, ролевой принципы и принцип изолированной среды. Правильный ответ – ответ №2
7.	В ТКС установлена система обнаружения вторжений. Выясните нужно ли защищать саму СОВ от угроз безопасности информации и от каких.	Ответ: 1) такую систему защищать невозможно и не нужно. Она сама себя защитит; 2) СОВ нужно в соответствии с требованиями НПА «Требования к системам обнаружения вторжений», утвержденном приказом ФСТЭК России от 6 декабря 2011 г. № 638 защищать от угроз: - нарушение целостности программного обеспечения СОВ; - нарушение целостности данных, собранных или созданных СОВ; - отключение или блокирование нарушителями компонентов СОВ; - несанкционированное изменение конфигурации СОВ; - несанкционированное внесение изменений в логику функционирования СОВ через механизм обновления базы решающих правил. Правильный ответ – ответ №2
8.	Определите, от каких угроз нужно защищать система защиты от вредоносных программ	Варианты ответа: 1) такую систему защищать невозможно и не нужно. Она сама себя защитит; 2) СЗВП нужно в соответствии с требованиями НПА «Требования к средствам антивирусной защиты», утвержденном приказом ФСТЭК России от 20 марта 2012 г. № 28, защищать от угроз: - нарушение целостности программного обеспечения СЗВП; - отключение и блокирование СЗВП; несанкционированное изменение конфигурации СЗВП; - несанкционированное внесение изменений в логику функционирования СЗВП через механизм обновления баз данных сигнатур СЗВП. Правильный ответ – ответ №2
9.	Определите критерии, по которым операционную среду можно относить к доверенной	Варианты ответа: 1) доверенность среды определяется владельцем ИС экспертно. Четких критериев нет; − операционная среда считается доверенной, если в ней имеют место: доверенность конфигурации и настройки; целостность всех элементов; подконтрольность всех действий; документированность всех событий; доверенное окружение и субъекты; доверенные правила разграничения доступа, обеспечения целостности и доступности информации (политики безопасности); доверенная аппаратная платформа; доверенная программная платформа; доверенные каналы передачи информации. Правильный ответ – ответ №2

10.	В ходе проверки организации в ТКС выявлено нарушение второй категории. Определите дальнейшие действия контрольной комиссии	Варианты ответа: 1) запретить работу ТКС; 2) сообщить руководству организации и составить акт проверки с указанием нарушения; 3) нарушение не связано с утечкой информации, составляющей государственную тайну. Председатель комиссии доводит результаты контроля до руководства организации, докладывает их руководителю органа контроля, по указанию которого проводилась проверка, совместно со службой безопасности составляется проект плана устранения недостатков и утверждает его у руководителя организации. Материалы контроля вместе с копией плана устранения недостатков направляются в орган контроля. Правильный ответ – ответ №3

8.2.3 Примерный перечень заданий для решения прикладных задач

№№ п/п	Задание при решении прикладных практических задача	Варианты ответа
1.	ТКС относится к информационной системе, в которой защите подлежат специальные категории персональных данных. Определите, нужна ли в такой системе СОВ и какого класса защиты	Варианты: нет не нужна. Правильный ответ – нужна с 4 классом защиты
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 защиты для устанавливаемых в ней средств антивирусной защиты	Варианты ответов: К1, К2 или К3. Правильный ответ – К2
3.	ТКС относится к государственной информационной системе и имеет 3 класс защищенности. Определите, какой класс защиты должен иметь установленный в ней межсетевой экран	Варианты ответа: 1 – 6 класс. Правильный ответ – 5 класс
4.	В ТКС обрабатывается информация, содержащая сведения, составляющие служебную тайну. Определите, в соответствии с каким документом нужно определять требований к ТКС по защите информации.	Варианты ответов:1) – нельзя, 2) применить межсетевой экран 1 класса защищенности; 3) установить средства криптографической защиты трафика, сертифицированные ФСБ России. Правильный ответ - ответ №3
5.	В ТКС необходимо разграничить доступ пользователей к информации, не содержащей сведения, составляющие государственную тайну, и к функциям ее обработки. Определите, какую технология окажется более эффективной для разграничения доступа пользователей к информации и к функциям ее обработки	Варианты ответа: 1 – ввести пароли для пользователей, 2 – установить и настроить соответствующим образом межсетевые экраны рабочих станций; 3 – применить технологию «Тонкий клиент». Правильныйответ – ответ №3
6.	ТКС относится к информационной системе персональных данных 4 класса защиты. Определите класс защиты для устанавливаемых в ней средств антивирусной защиты	Варианты ответа: 1) 3, 4 или 5 классы защиты; 2) 6 класс защиты; Правильный ответ – ответ №2
7.	В ТКС выявлены угрозы утечки информации по скрытным каналам. Определите дальнейшие действия службы безопасности по парированию выявленных угроз	Правильный ответ – ответ №3
8.	В ТКС для скрытия трафика, передаваемого через сеть Internet, применена технология VPN, при этом конечными точками защищенного туннеля выступают провайдеры сети Internet. Определите, при каком	Варианты ответа: 1 – ни при каких условиях; 2 – если канал от абонента до провайдера при передаче трафика и от провайдера до абонента при его приеме не
	условии такое решения является допустимым	считается необходимым защищать или он является защищенным. Правильный ответ – ответ №2

9.	В ТКС по результатам контроля выявлено нарушение, связанной с невыполнением требований по защите информации, в результате чего создаются предпосылки к несанкционированному доступу к ней. Определите категорию нарушению	Варианты ответа: 1 – нельзя осуществить передачу, нужен маршрутизируемый протокол; 2 – инкапсулировать пакеты протокола NetBEUI в пакеты IP. Правильный ответ – ответ №2
10.	Определите состав функциональных подсистем, которые Вы бы включили в систему защиты телекоммуникационной системы органа государственной власти, имеющей выход в Internet	Варианты ответа: 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 – ответ №2

8.2.4 Примерный перечень вопросов для подготовки к зачету

Не предусмотрено учебным планом.

8.2.5 Примерный перечень заданий для промежуточной аттестации

Для проведения промежуточной аттестации в форме зачета выдаются задания в виде следующих вопросов:

1. Краткая характеристика моделей безопасности информации КДЦ, гексады Паркера и модели STRIDE.
2. Понятие системы защиты информации в ТКС. Организационные, организационно-технические и технические системы защиты информации.
3. Классификация стратегий защиты информации в информационных системах и их краткая характеристика.
4. Основные направления защиты информации в ТКС.
5. Типовая структура системы защиты информации и ее характеристика.
6. Принципы построения систем защиты информации. Многоагентные системы защиты информации и перспективы их применения.
7. Подсистемы защиты ТКС от физического доступа.
8. Формальная модель Харрисона-Руззо-Ульмана, назначение и краткая характеристика.
9. Формальная модель Белла-ЛаПадулла, назначение и краткая характеристика.
10. Формальные модели Биба и Кларка-Вилсона, назначение и краткая характеристика.
11. Международный стандарт ИСО/ МЭК 15408. Понятия функциональных требований и требований доверия.
12. Меры и средства защиты информации от сетевых атак и от несанкционированной передачи во внешние сети. Общая характеристика.
13. Классификация систем обнаружения вторжений и краткая характеристика нормативного правового акта «Требования к системам обнаружения

вторжений», утвержденным приказом ФСТЭК России от 6 декабря 2011 г. № 638.

14. Средства антивирусной защиты и краткая характеристика нормативного правового акта «Требования к средствам антивирусной защиты», утвержденным приказом ФСТЭК России от 20 марта 2012 г. № 28.

15. Понятие доверенной среды. Технологии создания доверенных сред.

16. Организация и порядок проведения контроля эффективности защиты информации в телекоммуникационных системах.

8.2.6. Методика выставления оценки при проведении промежуточной аттестации

Зачет проводится по билетам, каждый из которых содержит 2 вопроса из разных разделов, одну стандартную и одну прикладную задачи. Сначала оценка ставится раздельно: а) по ответам на вопросы; б) по результату решения стандартной практической задачи; в) по решению прикладной практической задачи. Далее используется методика, аналогичная той, которая применялась при текущем контроле (см. раздел 7.1.1).

8.2.7 Паспорт оценочных материалов

Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции	Наименование оценочного средства	Контролируемые разделы (темы) дисциплины
Стратегии и основные направления защиты информации в телекоммуникационных системах и их общая характеристика	ПК-9.5	Тест, решение стандартных и прикладных задач	Стратегии и основные направления защиты информации в телекоммуникационных системах и их общая характеристика
Принципы создания и общая структура системы защиты информации в ТКС		Тест, решение стандартных и прикладных задач	Принципы создания и общая структура системы защиты информации в ТКС
Подсистемы защиты информации от угроз непосредственного несанкционированного доступа (НСД)		Тест, решение стандартных и прикладных задач	Подсистемы защиты информации от угроз непосредственного несанкционированного доступа (НСД)
Формальные модели разграничения доступа к информации в информационных системах и обеспечения ее целостности		Тест, решение стандартных и прикладных задач	Формальные модели разграничения доступа к информации в информационных системах и обеспечения ее целостности
Государственный стандарт ИСО/МЭК 15408 «Общие критерии»		Тест, решение стандартных и прикладных задач	Государственный стандарт ИСО/МЭК 15408 «Общие критерии»
Основы обеспечения безопасности информации в ТКС от сетевых атак. Средства обнаружения сетевых атак		Тест, решение стандартных и прикладных задач	Основы обеспечения безопасности информации в ТКС от сетевых атак. Средства обнаружения сетевых атак

8.3. 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 бу-

мажном носителе. Время тестирования 30 мин. Затем осуществляется проверка теста экзаменатором и выставляется оценка согласно методики выставления 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.

9. УЧЕБНО МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ)

Основная литература

Язов Ю.К., Соловьев С.В. Организация защиты информации в информационных системах от несанкционированного доступа. Монография. – Воронеж: Кварта, 2018. – 588с.

Информационная безопасность открытых систем: Учебник для вузов. В 2-х томах. Том 1 – Угрозы, уязвимости, атаки и подходы к защите/ С.В. Запечников, Н.Г. Милославская, А.И. Толстой, Д.А. Ушаков. – М.: Горячая линия – Телеком, 2006. – 536 с.: ил.

В.Г. Олифер, Н.А. Олифер. Безопасность компьютерных сетей. – М.: Горячая линия – Телеком. 2017. – 644 с.: ил.

Дополнительная литература

Казарин О.В. Безопасность программного обеспечения компьютерных систем. Монография. М.: МГУЛ. 2003. – 212 с.

Корченко А.Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения – К.: «МК-Пресс», 2006. – 320с., ил.

Шелухин О.И., Сакалема Д.Ж., Филинова А.С. Обнаружение вторжений в компьютерной сети (сетевые аномалии). Учебное пособие для вузов/ Под ред. профессора О.И Шелухина. – М.: Горячая линия – Телеком.2018. – 220с., ил.

Жуматий В.П., Будников С.А., Паршин Н.В. Угрозы программно-математического воздействия. Учебное пособие. – Воронеж: ГУП ВО «Воронежская областная типография – издательство им. Е.А.Волховитинова», 2010. – 231 с.

Зима В.М., Молдовян А.А., Молдовян Н.А. Безопасность глобальных сетевых технологий. – 2-е изд.- СПб.: БХВ-Петербург, 2014. – 368 с.:ил.

Учебно-методическая литература

Технология проектирования систем защиты информации в информационно-телекоммуникационных системах [Электронный ресурс] [Электронный ресурс] : учеб. пособие / Ю. К. Язов. - Электрон.дан. (1 файл). - Воронеж : ВГТУ, 2004. - 1 электрон. опт. диск (CD-ROM). - Имеется вариант на бумажном носителе. - 30.00.

Волкова Т.В. Разработка систем распределенной обработки данных [Электронный ресурс]: учебно-методическое пособие/ Волкова Т.В., Насейкина Л.Ф.— Электрон.текстовые данные.— Оренбург: Оренбургский государственный университет, ЭБС АСВ, 2012.- 330 с.- Режим доступа: http://www.iprbookshop.ru/30127.— ЭБС «IPRbooks».

9.2 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:

9.2.1. Электронная информационная образовательная среда ВГТУ, код доступа:

Банк данных угроз безопасности информации. Электрон. дан. - Режим доступа: http://www.bdu.fstec.ru

Стандарт Common Vulnerabilities and Exposures. Электрон. дан. - Режим доступа: http://cve.mitre.org

База данных с информационными бюллетенями (Secunia Advisories), содержащими сведения об обнаруженных угрозах и уязвимостях ПО Secunia Advisory and Vulnerability Database Электрон. дан. - Режим доступа: https://secuniaresearch.flexerasoftware.com/community/advisories

База уязвимостей VND (Vulnerability Notes Database Электрон. дан. - Режим доступа: https://www.kb.cert.org/vuls

База сценариев эксплуатации уязвимостей Exploit Database Электрон. дан. - Режим доступа: https://www.exploit-db.com

Агрегатор информации об уязвимостях CVEDetails. Электрон. дан. - Режим доступа: https://www.cvedetails.com

Information Security Информационная безопасность. Электрон. дан. - Режим доступа: http://www.itsec.ru

Securitylab.ru by Positive Technologies. Электрон. дан. - Режим доступа: https://www.securitylab.ru/

Anti-Malware.ru. Электрон. дан. - Режим доступа: https://www.anti-malware.ru/news

Iso27000.ru Искусство управления информационной безопасностью. Электрон. дан. - Режим доступа: http://www.iso27000.ru/

SecurityPolicy.ru Документы по информационной безопасности. Электрон. дан. -

Режим доступа: http://securitypolicy.ru/
SearchInform – Информационная безопасность. Электрон. дан. - Режим доступа: https://searchinform.ru/informatsionnaya-bezopasnost/
Информационная безопасность предприятия. Электрон. дан. - Режим доступа: Ekrost.ru

http://eios.vorstu.ru/

9.2.2. Программное обеспечение компьютеров для самостоятельной и аудиторной работы:

- лаборатория программно-аппаратных средств защиты информации/

9.2.3. Используемые электронные библиотечные системы:

– Университетская библиотека онлайн, код доступа: http://biblioclub.ru/;
научная электронная библиотека eLIBRARY.RU, код доступа: http://elibrary.ru/

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

Компьютеры с установленной на них операционной системой типа Windows-8.1 и выше.

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

По дисциплине «Информационная безопасность телекоммуникационных систем» читаются лекции, проводятся лабораторные работы.

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

Лабораторные работы выполняются на лабораторном оборудовании в соответствии с методиками, приведенными в указаниях к выполнению работ.

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 самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать его преподавателю на лекции или на практическом занятии.
Лабораторная работа	Лабораторные работы позволяют научиться применять теоретические знания, полученные на лекции при решении конкретных задач. Чтобы наиболее рационально и полно использовать все возможности лабораторных для подготовки к ним необходимо: разобрать лекцию по соответствующей теме, ознакомится с соответствующим разделом учебника, проработать дополнительную литературу и источники, решить задачи и выполнить другие письменные задания.
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 экзаменом, экзаменом три дня эффективнее всего использовать для повторения и систематизации материала.