МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФГБОУ ВО «Уральский государственный экономический университет»

Одобрена
на заседании кафедры

02.12.2025 г.

протокол № 3

Зав. кафедрой Назаров Д.М.

Утверждена
Советом по учебно-методическим вопросам и качеству образования

16 декабря 2025 г.

протокол № 4

Председатель ____ Карх Д.А.
(подпись)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Наименование дисциплины	Защита информации от утечки по техническим каналам
Направление подготовки	10.03.01 Информационная безопасность
Профиль	Информационно-аналитические системы финансового мониторинга
Форма обучения	очная
Год набора	2026

Разработана:
Профессор, д.э.н.
Назаров Д.М.

Екатеринбург
2025 г.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Рабочая программа дисциплины является частью основной профессиональной образовательной программы высшего образования - программы бакалавриата, разработанной в соответствии с ФГОС ВО

ФГОС ВО	Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 10.03.01 Информационная безопасность (приказ Минобрнауки России от 17.11.2020 г. № 1427)

1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины «Защита информации от утечки по техническим каналам» является теоретическая и практическая подготовленность бакалавра к организации и проведению мероприятий по защите информации от утечки по техническим каналам на объектах информатизации и в выделенных помещениях.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина относится к обязательной части учебного плана.

3. ОБЪЕМ ДИСЦИПЛИНЫ

Промежуточная аттестация	Часов					З.е.
	Всего за семестр	Контактная работа .(по уч.зан.)			Самостоятельная работа в том числе подготовка контрольных и курсовых	
		Всего	Лекции	Лабораторные		
Семестр 8						
Экзамен	180	64	32	32	89	5

4.ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ОПОП

В результате освоения ОПОП у выпускника должны быть сформированы компетенции, установленные в соответствии ФГОС ВО.

Шифр и наименование компетенции	Индикаторы достижения компетенций
ОПК-1 Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства;	ИД-1.ОПК-1 Знает основы информационной культуры

ОПК-1 Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства;	ИД-2.ОПК-1 Умеет решать стандартные задачи профессиональной деятельности с использованием информационных технологий с соблюдением требований информационной безопасности
	ИД-3.ОПК-1 Владеет навыками использования информационных технологий для поиска и обработки информации
ОПК-9 Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности;	ИД-1.ОПК-9 Знать: основные положения практики криптографической и технической защиты информации; основные проектные решения, средства и методы криптографической защиты информации, технические средства защиты информации
	ИД-2.ОПК-9 Уметь: решать типовые задачи с помощью методов криптологии, устанавливать, настраивать и обслуживать технические средства защиты информации
	ИД-3.ОПК-9 Владеть: навыками эксплуатации криптографических протоколов и схем, навыками применения средств технической защиты информации для решения задач профессиональной деятельности

ОПК-10 Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты;	ИД-1.ОПК-10 Знать: политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации
	ИД-2.ОПК-10 Уметь: определять подлежащие защите информационные ресурсы автоматизированных систем; контролировать эффективность принятых мер по защите информации в автоматизированных системах
	ИД-3.ОПК-10 Владеть навыками: обоснования, выбора, реализации и контроля результатов управленческого решения, навыками выявления и устранения угроз информационной безопасности
ОПК-6.3 Способен осуществлять эксплуатацию и проводить техническое обслуживание информационно-аналитических систем финансового мониторинга;	ИД-1.ОПК-6.3 Знать: основы функционирования информационно-аналитических систем финансового мониторинга; особенности эксплуатации и технического обслуживания информационно-аналитических систем финансового мониторинга
	ИД-2.ОПК-6.3 Уметь: ориентироваться в современных технологиях эксплуатации и технического обслуживания информационных и аналитических систем

ОПК-6.3 Способен осуществлять эксплуатацию и проводить техническое обслуживание информационно-аналитических систем финансового мониторинга;	ИД-3.ОПК-6.3 Владеть навыками: использования современных технологий эксплуатации и технического обслуживания информационных и аналитических систем
ОПК-6.4 Способен реализовывать комплекс мероприятий по защите информации в автоматизированных системах финансовых и экономических структур.	ИД-1.ОПК-6.4 Знать: перечень и содержание мероприятий по защите информации в автоматизированных системах; особенности программно-аппаратных средств защиты информации; особенности защиты информации в автоматизированных системах финансовых и экономических структур; основные подходы к выбору мероприятий по защите информации в автоматизированных системах финансовых и экономических структур с помощью современных методов и средств
	ИД-2.ОПК-6.4 Уметь: эффективно использовать современные программно-аппаратные средства защиты информации; обоснованно выбирать наиболее подходящие методы и средства защиты информации в автоматизированных системах финансовых и экономических структур; формулировать и реализовывать политику безопасности в системах финансовых и экономических структур
	ИД-3.ОПК-6.4 Владеть навыками: использования новых образцов программно-технических средств и информационных технологий, направленных на защиту информации в автоматизированных системах финансовых и экономических структур; методами и средствами выявления угроз безопасности автоматизированных систем; приемами и методами проведения мероприятий по защите информации в автоматизированных системах финансовых и экономических структур

5. ТЕМАТИЧЕСКИЙ ПЛАН

Тема	Часов						
	Наименование темы	Всего часов	Контактная работа .(по уч.зан.)			Самост. работа	Контроль самостоятельной работы
			Лекции	Лабораторные	Практические занятия		
Семестр 8		23					
Тема 1.	Концепция технической защиты информации. Утечка информации по техническим каналам (ОПК-1, ОПК-10)	23	8	4		11	
Семестр 8		40					
Тема 2.	Основные принципы технической защиты информации. Организационные основы технической защиты информации (ОПК-9, ОПК-10)	40	8	8		24	
Семестр 8		32					
Тема 3.	Оценка угрозы утечки информации по техническим каналам и подавление опасных сигналов (ОПК-9, ОПК-6.3)	32	8	8		16	
Семестр 8		58					

Тема 4.	Методы противодействия утечке и добыванию информации. Моделирование процессов технической защиты информации (ОПК-9, ОПК-10, ОПК-6.3, ОПК-6.4)	58	8	12		38	

6. ФОРМЫ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ШКАЛЫ ОЦЕНИВАНИЯ

Раздел/Тема	Вид оценочного средства	Описание оценочного средства	Критерии оценивания
Текущий контроль (Приложение 4)			
Тема 1	Тест №1 (Приложение 4)	Тест состоит из 10 вопросов	<30 - не зачет 31<...<65 - 3 66<...<80 - 4 81<...<100 - 5
Тема 2	Доклад, сообщение (Приложение 4)	Продукт самостоятельной работы студента, представляющий собой публичное выступление по представлению полученных результатов решения определенной учебно-практической, учебно-исследовательской и научной темы.	<30 - не зачет 31<...<65 - 3 66<...<80 - 4 81<...<100 - 5
Тема 3	Контрольная работа № 1 (Приложение 4)	Контрольная работа состоит из 2 заданий по вариантам	<30 - не зачет 31<...<65 - 3 66<...<80 - 4 81<...<100 - 5
Тема 4	Контрольная работа № 2 (Приложение 4)	Контрольная работа состоит из 2 заданий по вариантам	<30 - не зачет 31<...<65 - 3 66<...<80 - 4 81<...<100 - 5
Промежуточная аттестация(Приложение 5)			
8 семестр (Эк)	Экзаменационный билет (Приложение 5)	В билете 2 теоретических и 1 практический вопрос	<30 - не зачет 31<...<65 - 3 66<...<80 - 4 81<...<100 - 5

ОПИСАНИЕ ШКАЛ ОЦЕНИВАНИЯ

Показатель оценки освоения ОПОП формируется на основе объединения текущего контроля и промежуточной аттестации обучающегося.

Показатель рейтинга по каждой дисциплине выражается в процентах, который показывает уровень подготовки студента.

Текущий контроль.Используется 100-балльная система оценивания. Оценка работы студента в течении семестра осуществляется преподавателем в соответствии с разработанной им системой оценки учебных достижений в процессе обучения по данной дисциплине.

В рабочих программах дисциплин и практик закреплены виды текущего контроля, планируемые результаты контрольных мероприятий и критерии оценки учебный достижений.

В течение семестра преподавателем проводится не менее 3-х контрольных мероприятий, по оценке деятельности студента. Если посещения занятий по дисциплине включены в рейтинг, то данный показатель составляет не более 20% от максимального количества баллов по дисциплине.

Промежуточная аттестация. Используется 5-балльная система оценивания. Оценка работы студента по окончанию дисциплины (части дисциплины) осуществляется преподавателем в соответствии с разработанной им системой оценки достижений студента в процессе обучения по данной дисциплине. Промежуточная аттестация также проводится по окончанию формирования компетенций.

Порядок перевода рейтинга, предусмотренных системой оценивания, по дисциплине, в пятибалльную систему.

Высокий уровень – 100% - 70% - отлично, хорошо.

Средний уровень – 69% - 50% - удовлетворительно.

Показатель оценки	По 5-балльной системе	Характеристика показателя
100% - 85%	отлично	обладают теоретическими знаниями в полном объеме, понимают, самостоятельно умеют применять, исследовать, идентифицировать, анализировать, систематизировать, распределять по категориям, рассчитать показатели, классифицировать, разрабатывать модели, алгоритмизировать, управлять, организовать, планировать процессы исследования, осуществлять оценку результатов на высоком уровне
84% - 70%	хорошо	обладают теоретическими знаниями в полном объеме, понимают, самостоятельно умеют применять, исследовать, идентифицировать, анализировать, систематизировать, распределять по категориям, рассчитать показатели, классифицировать, разрабатывать модели, алгоритмизировать, управлять, организовать, планировать процессы исследования, осуществлять оценку результатов. Могут быть допущены недочеты, исправленные студентом самостоятельно в процессе работы (ответа и т.д.)
69% - 50%	удовлетворительно	обладают общими теоретическими знаниями, умеют применять, исследовать, идентифицировать, анализировать, систематизировать, распределять по категориям, рассчитать показатели, классифицировать, разрабатывать модели, алгоритмизировать, управлять, организовать, планировать процессы исследования, осуществлять оценку результатов на среднем уровне. Допускаются ошибки, которые студент затрудняется исправить самостоятельно.
49 % и менее	неудовлетворительно	обладают не полным объемом общих теоретическими знаниями, не умеют самостоятельно применять, исследовать, идентифицировать, анализировать, систематизировать, распределять по категориям, рассчитать показатели, классифицировать, разрабатывать модели, алгоритмизировать, управлять, организовать, планировать процессы исследования, осуществлять оценку результатов. Не сформированы умения и навыки для решения профессиональных задач
100% - 50%	зачтено	характеристика показателя соответствует «отлично», «хорошо», «удовлетворительно»
49 % и менее	не зачтено	характеристика показателя соответствует «неудовлетворительно»

7. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

7.1. Содержание лекций

Тема 1. Концепция технической защиты информации. Утечка информации по техническим каналам (ОПК-1, ОПК-10) Основные принципы концепции технической защиты информации. Технические каналы утечки информации (ТКУИ)
Тема 2. Основные принципы технической защиты информации. Организационные основы технической защиты информации (ОПК-9, ОПК-10) Принципы, меры и мероприятия по технической защиты информации.
Тема 3. Оценка угрозы утечки информации по техническим каналам и подавление опасных сигналов (ОПК-9, ОПК-6.3) Угрозы утечки информации по техническим каналам. Способы и методы подавления опасных сигналов.
Тема 4. Методы противодействия утечке и добыванию информации. Моделирование процессов технической защиты информации (ОПК-9, ОПК-10, ОПК-6.3, ОПК-6.4) Обзор методов противодействия утечке по техническим каналам. Основные методики моделирования процессов технической защиты информации.

7.2 Содержание практических занятий и лабораторных работ

Тема 2. Основные принципы технической защиты информации. Организационные основы технической защиты информации (ОПК-9, ОПК-10) Организационные и технические меры защиты информации
Тема 3. Оценка угрозы утечки информации по техническим каналам и подавление опасных сигналов (ОПК-9, ОПК-6.3) Утечки по акустическому и визуальному каналам. Побочные электромагнитные излучения и наводки.
Тема 4. Методы противодействия утечке и добыванию информации. Моделирование процессов технической защиты информации (ОПК-9, ОПК-10, ОПК-6.3, ОПК-6.4) Обеспечение защиты информации от утечек по техническим каналам

7.3. Содержание самостоятельной работы

Тема 2. Основные принципы технической защиты информации. Организационные основы технической защиты информации (ОПК-9, ОПК-10) Изучение методов инженерно-технической защиты информации. Государственная система защиты информации.

Тема 3. Оценка угрозы утечки информации по техническим каналам и подавление опасных сигналов (ОПК-9, ОПК-6.3) Изучение способов распространения сигналов в технических каналах утечки информации. Физические процессы подавления опасных сигналов.
Тема 4. Методы противодействия утечке и добыванию информации. Моделирование процессов технической защиты информации (ОПК-9, ОПК-10, ОПК-6.3, ОПК-6.4) Изучение средства предотвращения утечек информации по техническим каналам. Инженерно-техническая защита информации. Проектирование и оптимизация систем защиты.

7.3.1. Примерные вопросы для самостоятельной подготовки к зачету/экзамену
Приложение 1

7.3.2. Практические задания по дисциплине для самостоятельной подготовки к зачету/экзамену
Приложение 2

7.3.3. Перечень курсовых работ
Курсовые работы не предусмотрены

7.4. Электронное портфолио обучающегося
Материалы не размещаются

7.5. Методические рекомендации по выполнению контрольной работы
не предусмотрено

7.6 Методические рекомендации по выполнению курсовой работы
не предусмотрено

8. ОСОБЕННОСТИ ОРГАНИЗАЦИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

По заявлению студента

В целях доступности освоения программы для лиц с ограниченными возможностями здоровья при необходимости кафедра обеспечивает следующие условия:

- особый порядок освоения дисциплины, с учетом состояния их здоровья;
- электронные образовательные ресурсы по дисциплине в формах, адаптированных к ограничениям их здоровья;
- изучение дисциплины по индивидуальному учебному плану (вне зависимости от формы обучения);
- электронное обучение и дистанционные образовательные технологии, которые предусматривают возможности приема-передачи информации в доступных для них формах.
- доступ (удаленный доступ), к современным профессиональным базам данных и информационным справочным системам, состав которых определен РПД.

9. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ УЧЕБНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Сайт библиотеки УрГЭУ
http://lib.usue.ru/

Основная литература:

2. Сычев Ю.Н. Защита информации и информационная безопасность [Электронный ресурс]:Учебное пособие. - Москва: ООО "Научно-издательский центр ИНФРА-М", 2022. - 201 – Режим доступа: https://znanium.com/catalog/product/1844364

Дополнительная литература:

2. Баранова Е.К., Бабаш А.В. Информационная безопасность и защита информации [Электронный ресурс]:учебное пособие. - Москва: Издательский Центр РИО, 2022. - 336 – Режим доступа: https://znanium.ru/catalog/product/1861657

10. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ВКЛЮЧАЯ ПЕРЕЧЕНЬ ЛИЦЕНЗИОННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ, ОНЛАЙН КУРСОВ, ИСПОЛЬЗУЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Перечень лицензионного программного обеспечения:

СЗИ от НСД "Страж NT" версия 4.0. Договор № 73700092 от 04.08.2017,Товарная накладная № 73700092 от 11.10.2017.

Secret Net 7. Клиент (автономный режим работы). Договор № 73700092 от 04.08.2017, Товарная накладная № 73700092 от 11.10.2017.

Astra Linux Common Edition. Договор №0417-ПО/2019 от 08.05.2019, Акт №Sk000343 от 24.05.2019 и Контракт № 35-У/2018 от 13.06.2018, Акт № УТ213 от 17.12.2018. Срок действия лицензии - без ограничения срока.

Перечень информационных справочных систем, ресурсов информационно-телекоммуникационной сети «Интернет»:

Справочно-правовая система Гарант. Договор № 58419 от 22 декабря 2015. Срок действия лицензии -без ограничения срока

Справочно-правовая система Консультант +. Договор № 143/223-У/2025 от 02.12.2025 Срок действия лицензии до 31.12.2026

11. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Реализация учебной дисциплины осуществляется с использованием материально-технической базы УрГЭУ, обеспечивающей проведение всех видов учебных занятий и научно-исследовательской и самостоятельной работы обучающихся:

Специальные помещения представляют собой учебные аудитории для проведения всех видов занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду УрГЭУ.

Все помещения укомплектованы специализированной мебелью и оснащены мультимедийным оборудованием спецоборудованием (информационно-телекоммуникационным, иным компьютерным), доступом к информационно-поисковым, справочно-правовым системам, электронным библиотечным системам, базам данных действующего законодательства, иным информационным ресурсам служащими для представления учебной информации большой аудитории.

Для проведения занятий лекционного типа презентации и другие учебно-наглядные пособия, обеспечивающие тематические иллюстрации.

Приложение 1
к рабочей программе

7.3.1. Примерные вопросы для самостоятельной подготовки к зачету/экзамену

Примерный перечень вопросов к экзамену:

1. Стоимостные характеристики информации и их соотношения.
2. Internet как среда для компьютерных преступлений.
3. Основные задачи информационной безопасности.
4. Основные методы обеспечения защиты информационной системы.
5. Определение и классификация угроз.
6. Потенциальные противники: классификация и характеристика.
7. Каналы утечки информации.
8. Классификация атак и их характеристики.
9. Сетевые атаки: основные виды.
10. Основные положения информационной безопасности.
11. Принципы обеспечения информационной безопасности.
12. Формальные модели доступа к данным.
13. Приведите убедительные доводы того, что информационная безопасность - одна из важнейших проблем современной жизни.
14. Что понимается под системой безопасности?
15. Какие вопросы, касающиеся информационной безопасности, содержатся в Конституции РФ?
16. Дайте определение информационной системы. Перечислите структурные компоненты информационных систем. Что понимают под информационными ресурсами и процесами?
17. Перечислите основные компоненты концептуальной модели ИБ. Изобразите графически схему концептуальной модели системы ИБ.
18. Какие вопросы, касающиеся информационной безопасности, содержатся в Гражданском кодексе РФ?
19. Какая информация является предметом защиты? Перечислите основные свойства информации как предмета защиты. Охарактеризуйте секретную и конфиденциальную информацию.
20. Что такое объекты угроз ИБ? В чем выражаются угрозы информации? Каковы основные источники угроз защищаемой информации? Каковы цели угроз информации со стороны злоумышленников?
21. Какие статьи Уголовного кодекса напрямую касаются информационной безопасности?
22. Охарактеризуйте свойства информации. Что такое признаковая информация? Почему семантическая информация по отношению к признаковой является вторичной? Какие признаки объектов являются демаскирующими? Назовите основные способы неправомерного овладения конфиденциальной информацией.
23. Какие основные понятия рассматриваются в Законе РФ "Об информации, информатизации и защите информации"?
24. Что такое «источник конфиденциальной информации»? Перечислите основные источники конфиденциальной информации.
25. Дайте определение и перечислите основные способы НСД к конфиденциальной информации. Охарактеризуйте обобщенную модель взаимодействия способов НСД источников конфиденциальной информации.
26. Дайте определение лицензирования. Кто такие лицензиат и лицензирующие органы? Почему лицензирование и сертификация выступают в качестве средства защиты информации?

27. Перечислите перечень видов деятельности, касающихся ИБ, на осуществление которых требуются лицензии.
28. Дайте определение информационной безопасности, прокомментируйте его составляющие. Перечислите основные категории информационной безопасности.
29. Что такое утечка конфиденциальной информации? Как осуществляется утечка конфиденциальной информации?
30. Какие Вам известны американские законы, напрямую связанные с ИБ? Что можно сказать о законодательстве ФРГ по вопросам ИБ?
31. Что такое защита информации?
32. Определите понятие «несанкционированный доступ» к конфиденциальной информации, как он реализуется?
33. Какие недостатки российского законодательства, на Ваш взгляд, необходимо устранять в первую очередь?
34. Охарактеризуйте понятия доступности, целостности и конфиденциальности информации.
35. Дайте определение угроз конфиденциальной информации. Какие действия определяют угрозы конфиденциальной информации?
36. Приведите основные направления деятельности по вопросам ИБ на законодательном уровне.
37. Прокомментируйте основные составляющие информационной безопасности РФ.
38. Что такое атака? Что такое окно опасности? Какие события происходят во время существования окна опасности?
39. Назовите главную цель мер административного уровня ИБ. Что понимается под политикой безопасности?
40. Приведите примерный список решений верхнего уровня политики безопасности.
41. Перечислите важнейшие задачи обеспечения информационной безопасности РФ.
42. Что такое угрозы утечки информации? Какие угрозы называются преднамеренными и случайными?
43. Что такое программа безопасности, ее уровни.
44. Классифицируйте угрозы ИБ РФ для личности, для общества, для Государства по общей направленности.
45. Что такое канал НСД? Назовите типовые причины их возникновения.
46. Что такое управление рисками? Почему управление рисками рассматривается на административном уровне ИБ? В чем заключается суть мероприятий по управлению рисками?
47. Охарактеризуйте государственную структуру органов, обеспечивающих информационную безопасность.
48. Назовите основные способы добывания конфиденциальной информации злоумышленником.
49. В чем заключается основная специфика процедурного уровня ИБ? Перечислите основные классы мер процедурного уровня ИБ. Почему вопросы поддержания работоспособности ИС являются принципиальными на процедурном уровне ИБ?
50. В чем специфика деятельности Межведомственной комиссии по защите государственной тайны?
51. Что такое канал утечки информации? Что такое технический канал утечки информации? Охарактеризуйте случайный и организованный канал утечки информации.
52. Перечислите направления повседневной деятельности системного администратора, обеспечивающие поддержание работоспособности ИС.
53. В чем специфика деятельности ФСТЭК России?
54. Что такое источник угроз безопасности информации? Назовите основные источники преднамеренных угроз.

55. Перечислите основные причины важности программно-технического уровня ИБ. Назовите основные сервисы ИБ программно-технического уровня.
56. Почему уровень ИБ в России в настоящее время не соответствует жизненно важным потребностям личности, общества и государства и какие ключевые проблемы необходимо решить безотлагательно, чтобы обеспечить достаточный уровень ИБ в России?
57. Прокомментируйте наиболее распространенные угрозы доступности. Охарактеризуйте программные атаки на доступность.
58. Какие аспекты современных ИС с точки зрения безопасности наиболее существенны?
59. Раскройте содержание политических, Экономических и организационно-технических факторов, влияющих на состояние информационной безопасности РФ.
60. Что такое вредоносное программное обеспечение? Дайте определение «бомбы», «червя», «вируса». Какие негативные последствия в функционировании ИС вызывает вредоносное ПО?
61. Что такое идентификация? Дайте толкование понятия «аутентификация». Из-за каких причин затруднена надежная идентификация?
62. Дайте определение защищаемой информации и охарактеризуйте ее основные признаки.
63. Охарактеризуйте основные угрозы целостности конфиденциальной информации. Прокомментируйте парольную идентификацию. Какие меры позволяют повысить надежность парольной защиты?
64. Что такое государственная тайна? Перечислите сведения, которые могут быть отнесены к государственной тайне. Приведите классификацию сведений, составляющих государственную тайну, по степеням секретности
65. Перечислите основные угрозы конфиденциальности информации.
66. Прокомментируйте возможности биометрической идентификации (аутентификации).
67. Перечислите основные виды конфиденциальной информации, нуждающейся в защите.
68. Дайте определение способа защиты информации. Охарактеризуйте основные способы защиты. Перечислите основные защитные действия при реализации способов ЗИ.
69. В чем заключается основная задача логического управления доступом? Что такое матрица доступа? Какая информация анализируется при принятии решения о предоставлении доступа?
70. Каким требованиям должна отвечать коммерческая тайна? Охарактеризуйте основные субъекты права на коммерческую тайну. Какая информация не может быть отнесена к коммерческой тайне?
71. Что такое защита от разглашения?
72. Перечислите и охарактеризуйте основные объекты профессиональной тайны. Каким требованиям должна удовлетворять информация, чтобы ее можно было бы отнести к профессиональной тайне?
73. Перечислите и прокомментируйте защитные действия от утечки конфиденциальной информации.
74. Каким требованиям должна удовлетворять информация, чтобы ее можно было бы отнести к служебной тайне? Приведите перечень сведений, которые не могут быть отнесены к служебной информации ограниченного распространения.
75. Перечислите и охарактеризуйте защитные действия от НСД к конфиденциальной информации.
76. Охарактеризуйте экранирование в качестве основного сервиса безопасности ИС. Что такое firewall и как он функционирует?
77. Дайте определение персональных данных. Какие сведения могут быть

78. Для каких целей служит сервис анализа защищенности? В чем заключается специфика управления, как сервиса безопасности?
79. Политика безопасности информационных систем.
80. Таксономия нарушений информационной безопасности вычислительной системы.
81. Уровни правового обеспечения информационной безопасности.
82. Доктрина информационной безопасности России.
83. Основные аппаратные средства защиты. Основные программные средства защиты.
84. Основные методы идентификации и аутентификации.
85. Сервисы управления доступом.
86. Протоколирование и аудит. Задачи аудита.
87. Основы защиты Internet-подключений.
88. Стандарты обеспечения информационной безопасности.
89. Общие принципы построения защищенных систем.

Задачи в экзаменационных билетах:

1. Методы поиска и сбора информации.
2. Методика устранения компьютерной информации.
3. Уязвимости Windows.
4. Уязвимости UNIX
5. Защита от копирования переносных носителей.
6. Аппаратные ключи защиты.
7. Современные криптосистемы
8. Виды шифров. Методика кодирования
9. Навесная защита
10. Антивирусное программное обеспечение.
11. Особенности защиты информации при работе в сети.
12. Безопасная работа в Internet.
13. Целесообразность усиления обороны.
14. Защита от побочного электромагнитного излучения и наводок
15. Алгоритмы распределения ключей.

Приложение 2
к рабочей программе

7.3.2. Практические задания по дисциплине для самостоятельной подготовки к зачету/экзамену

ОПК-1: Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства

Закрытые задания:

Вопрос №1:
Что является выходами системы защиты информации?
(Отметьте один правильный вариант ответа.)
Вариант 1 средства и методы защиты
Вариант 2 злоумышленники и владельцы информации
Вариант 3 сведения
Вариант 4 внешние и внутренние угрозы

Вопрос №2:
Как называется совокупность условий и факторов, создающих потенциальную угрозу или реально существующую опасность нарушения безопасности информации?
(Отметьте один правильный вариант ответа.)
Вариант 1 цель злоумышленника
Вариант 2 источник угрозы
Вариант 3 угроза
Вариант 4 атака

Вопрос № 3:
Если злоумышленник внедрил в компьютер вредоносную программу и получил доступ к личной информации пользователя, какое свойство информации было нарушено?
(Отметьте один правильный вариант ответа.)
Вариант 1 неотказуемость
Вариант 2 целостность
Вариант 3 доступность
Вариант 4 конфиденциальность

Вопрос №4:
Если в результате DDOS-атаки новостной сайт на какое-то время вышел из строя и был недоступен для пользователей, какое свойство информации было нарушено?
(Отметьте один правильный вариант ответа.)
Вариант 1 доступность
Вариант 2 конфиденциальность
Вариант 3 целостность
Вариант 4 неотказуемость

Вопрос №5:
Регламентация доступа в защищаемое помещение относится к:
(Отметьте один правильный вариант ответа.)
Вариант 1 физическим мерам обеспечения безопасности
Вариант 2 морально-этическим мерам обеспечения безопасности
Вариант 3 организационным мерам обеспечения безопасности

Вариант 4 техническим мерам обеспечения безопасности

Открытые задания:

1. Перечислите основные виды конфиденциальной информации, нуждающейся в защите.
2. Дайте определение способа защиты информации.
3. Охарактеризуйте основные способы защиты.
4. Перечислите основные защитные действия при реализации способов ЗИ.
5. Что такое источник угроз безопасности информации?

ОПК-9: Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности

Закрытые задания:

Вопрос №1:
Установка генератора шума для создания эффекта маскировки речевого сигнала в защищаемом помещении относится к:
(Отметьте один правильный вариант ответа.)
Вариант 1 организационным мерам обеспечения безопасности
Вариант 2 морально-этическим мерам обеспечения безопасности
Вариант 3 физическим мерам обеспечения безопасности
Вариант 4 техническим мерам обеспечения безопасности

Вопрос №2:
Какие документы определяют общие отношение и политику государства в заданной области, а также служат основой для создания нормативно–правовых документов?
(Отметьте один правильный вариант ответа.)
Вариант 1 международные стандарты
Вариант 2 федеральные законы
Вариант 3 ГОСТЫ
Вариант 4 концептуальные

Вопрос №3:
Как называется состояние защищенности личности, общества и государства от внутренних и внешних угроз, которое позволяет обеспечить конституционные права, свободы, достойные качество и уровень жизни граждан, суверенитет, территориальную целостность и устойчивое развитие Российской Федерации, оборону и безопасность государства?
(Отметьте один правильный вариант ответа.)
Вариант 1 информационная безопасность
Вариант 2 государственная безопасность
Вариант 3 национальная безопасность
Вариант 4 общественная безопасность

Вопрос №4:
Доктрина информационной безопасности относится к:
(Отметьте один правильный вариант ответа.)
Вариант 1 международным стандартам
Вариант 2 ГОСТам
Вариант 3 нормативно-методическим документам
Вариант 4 концептуальным документам

Вопрос №5:
Какие из приведенных ниже документов можно отнести к организационным?
(Ответ считается верным, если отмечены все правильные варианты ответов.)
Вариант 1 доктрины
Вариант 2 федеральные законы
Вариант 3 распоряжения Президента
Вариант 4 уставы
Вариант 5 инструкции
Вариант 6 указы Президента

Открытые задания:

1. Назовите основные источники преднамеренных угроз.
2. Охарактеризуйте государственную структуру органов, обеспечивающих информационную безопасность
3. Что такое идентификация и аутентификация при входе в информационную систему.
4. Приведите пример атаки на систему информационной безопасности
5. Опишите биометрические средства идентификации и аутентификации пользователей

ОПК-10: Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты

Закрытые задания:

Вопрос №1:
Установка генератора шума для создания эффекта маскировки речевого сигнала в защищаемом помещении относится к:
(Отметьте один правильный вариант ответа.)
Вариант 1 организационным мерам обеспечения безопасности
Вариант 2 морально-этическим мерам обеспечения безопасности
Вариант 3 физическим мерам обеспечения безопасности
Вариант 4 техническим мерам обеспечения безопасности

Вопрос №2:
Какие документы определяют общие отношение и политику государства в заданной области, а также служат основой для создания нормативно–правовых документов?
(Отметьте один правильный вариант ответа.)
Вариант 1 международные стандарты
Вариант 2 федеральные законы
Вариант 3 ГОСТЫ
Вариант 4 концептуальные

Вопрос №3:
Как называется состояние защищенности личности, общества и государства от внутренних и внешних угроз, которое позволяет обеспечить конституционные права, свободы, достойные качество и уровень жизни граждан, суверенитет, территориальную целостность и устойчивое развитие Российской Федерации, оборону и безопасность государства?
(Отметьте один правильный вариант ответа.)
Вариант 1 информационная безопасность

Вариант 2 государственная безопасность
Вариант 3 национальная безопасность
Вариант 4 общественная безопасность

Вопрос №4:
Доктрина информационной безопасности относится к:
(Отметьте один правильный вариант ответа.)
Вариант 1 международным стандартам
Вариант 2 ГОСТам
Вариант 3 нормативно-методическим документам
Вариант 4 концептуальным документам

Вопрос №5:
Какие из приведенных ниже документов можно отнести к организационным?
(Ответ считается верным, если отмечены все правильные варианты ответов.)
Вариант 1 доктрины
Вариант 2 федеральные законы
Вариант 3 распоряжения Президента
Вариант 4 уставы
Вариант 5 инструкции
Вариант 6 указы Президента

Открытые задания:

1. Разработать концептуальный план защиты
2. Что такое вирусы и методы борьбы с ними
3. Опишите процесс анализа бизнес-требований к информационной безопасности
4. Назовите основные этапы разработки защищенной системы
5. Приведите примеры угрозы отказа служб (угроза отказа в доступе).

ОПК-6.3: Способен осуществлять эксплуатацию и проводить техническое обслуживание информационно-аналитических систем финансового мониторинга

Закрытые задания:

Вопрос №1:
Установка генератора шума для создания эффекта маскировки речевого сигнала в защищаемом помещении относится к:
(Отметьте один правильный вариант ответа.)
Вариант 1 организационным мерам обеспечения безопасности
Вариант 2 морально-этическим мерам обеспечения безопасности
Вариант 3 физическим мерам обеспечения безопасности
Вариант 4 техническим мерам обеспечения безопасности

Вопрос №2:
Какие документы определяют общие отношение и политику государства в заданной области, а также служат основой для создания нормативно–правовых документов?
(Отметьте один правильный вариант ответа.)
Вариант 1 международные стандарты
Вариант 2 федеральные законы
Вариант 3 ГОСТЫ

Вариант 4 концептуальные

Вопрос №3:
Как называется состояние защищенности личности, общества и государства от внутренних и внешних угроз, которое позволяет обеспечить конституционные права, свободы, достойные качество и уровень жизни граждан, суверенитет, территориальную целостность и устойчивое развитие Российской Федерации, оборону и безопасность государства?
(Отметьте один правильный вариант ответа.)
Вариант 1 информационная безопасность
Вариант 2 государственная безопасность
Вариант 3 национальная безопасность
Вариант 4 общественная безопасность

Вопрос №4:
Если в результате DDOS-атаки новостной сайт на какое-то время вышел из строя и был недоступен для пользователей, какое свойство информации было нарушено?
(Отметьте один правильный вариант ответа.)
Вариант 1 доступность
Вариант 2 конфиденциальность
Вариант 3 целостность
Вариант 4 неотказуемость

Вопрос №5:
Регламентация доступа в защищаемое помещение относится к:
(Отметьте один правильный вариант ответа.)
Вариант 1 физическим мерам обеспечения безопасности
Вариант 2 морально-этическим мерам обеспечения безопасности
Вариант 3 организационным мерам обеспечения безопасности
Вариант 4 техническим мерам обеспечения безопасности

Открытые задания:

1. Что такое разграничение доступа к данным в ОС семейства UNIX
2. Дайте анализ бизнес-требований к информационной безопасности
3. Поясните административный уровень защиты информации
4. Опишите проблемы обеспечения безопасности почтовых сервисов и их решения
5. Что такое зашита DNS

ОПК-6.4: Способен реализовывать комплекс мероприятий по защите информации в автоматизированных системах финансовых и экономических структур

Закрытые задания:

Вопрос №1:
Что является выходами системы защиты информации?
(Отметьте один правильный вариант ответа.)
Вариант 1 средства и методы защиты
Вариант 2 злоумышленники и владельцы информации
Вариант 3 сведения
Вариант 4 внешние и внутренние угрозы

Вопрос №2:
Как называется совокупность условий и факторов, создающих потенциальную угрозу или реально существующую опасность нарушения безопасности информации?
(Отметьте один правильный вариант ответа.)
Вариант 1 цель злоумышленника
Вариант 2 источник угрозы
Вариант 3 угроза
Вариант 4 атака

Вопрос №3:
Как называется состояние защищенности личности, общества и государства от внутренних и внешних угроз, которое позволяет обеспечить конституционные права, свободы, достойные качество и уровень жизни граждан, суверенитет, территориальную целостность и устойчивое развитие Российской Федерации, оборону и безопасность государства?
(Отметьте один правильный вариант ответа.)
Вариант 1 информационная безопасность
Вариант 2 государственная безопасность
Вариант 3 национальная безопасность
Вариант 4 общественная безопасность

Вопрос №4:
Доктрина информационной безопасности относится к:
(Отметьте один правильный вариант ответа.)
Вариант 1 международным стандартам
Вариант 2 ГОСТам
Вариант 3 нормативно-методическим документам
Вариант 4 концептуальным документам

Вопрос №5:
Регламентация доступа в защищаемое помещение относится к:
(Отметьте один правильный вариант ответа.)
Вариант 1 физическим мерам обеспечения безопасности
Вариант 2 морально-этическим мерам обеспечения безопасности
Вариант 3 организационным мерам обеспечения безопасности
Вариант 4 техническим мерам обеспечения безопасности

Открытые задания:

1. Опишите процедурный уровень обеспечения безопасности
2. Приведите пример применения сертификатов для аутентификации и авторизации
3. Что такое электронная цифровая подпись
4. Опишите процесс проектирования защиты границ сети
5. Назовите основные типы политики безопасности доступа к данным