Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Таскаев Сергей Валерьевич
Должность: Ректор
Дата подписания: 15.06.2026 12:30:22
Уникальный программный ключ:
04c19ed8bfb98f5b6cb77a486b9a8788b8522523

Фонд оценочных средств для промежуточной аттестации по дисциплине (модулю) Защита информации от утечки по техническим каналам

Направление подготовки (специальность)
10.05.01 Компьютерная безопасность

Специализация №6
Информационно-аналитическая и техническая экспертиза компьютерных систем

Присваиваемая квалификация (степень)
Специалист по защите информации

Форма обучения
Очная

Год набора 2026

Челябинск, 2026 г.

© ФГБОУ ВО «ЧелГУ»

Содержание

© ФГБОУ ВО «ЧелГУ»

1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

Специальность: 10.05.01 Компьютерная безопасность
Специализация: Информационно-аналитическая и техническая экспертиза компьютерных систем
Дисциплина: Защита информации от утечки по техническим каналам
Семестр: 8
Форма промежуточной аттестации: экзамен.
Система оценивания: оценивание результатов осуществляется в рамках 5-балльной системы.

2. ПЕРЕЧЕНЬ ФОРМИРУЕМЫХ КОМПЕТЕНЦИЙ

2.1. Компетенции, закреплённые за дисциплиной

Изучение дисциплины «Б1.О.28 Защита информации от утечки по техническим каналам» направлено на формирование следующих компетенций:

Коды компетенции (по ФГОС)	Содержание компетенций согласно ФГОС	Индикаторы достижения компетенций согласно ОПОП	Перечень планируемых результатов обучения по дисциплине
ОПК-6	Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	ОПК-6.1. Знает систему нормативных правовых актов и стандартов по лицензированию в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации; задачи органов защиты государственной тайны и служб защиты информации на предприятиях; систему организационных мер, направленных на защиту информации ограниченного доступа; нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации ограниченного доступа; основные угрозы безопасности информации и модели нарушителя компьютерных систем.	Для достижения индикатора ОПК-6.1: Знать систему нормативных правовых актов и стандартов по лицензированию в области технической защиты конфиденциальной информации; основные угрозы безопасности информации и модели нарушителя компьютерных систем. Для достижения индикатора ОПК-6.2: Уметь разрабатывать модели угроз и модели нарушителя компьютерных систем; определить политику контроля доступа работников к информации ограниченного доступа; формулировать основные требования, предъявляемые к физической защите объекта и пропускному режиму в организации; применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценивания защищенности компьютерной системы. Для достижения индикатора ОПК-6.2: Владеть навыками защиты информации от утечки по техническим каналам.

© ФГБОУ ВО «ЧелГУ»

		ОПК-6.2. Умеет разрабатывать модели угроз и модели нарушителя компьютерных систем; разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации; определить политику контроля доступа работников к информации ограниченного доступа; формулировать основные требования, предъявляемые к физической защите объекта и пропускному режиму в организации; применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценивания защищенности компьютерной системы.	
ОПК-9	Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации	ОПК-9.1. Знает технические каналы утечки информации; возможности технических средств перехвата информации; способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; организацию защиты информации от утечки по техническим каналам на объектах информатизации; возможности технических средств перехвата информации. ОПК-9.2. Умеет анализировать и оценивать угрозы информационной безопасности объекта; пользоваться нормативными документами в области технической защиты информации. ОПК-9.3. Владеет методами и средствами технической защиты информации.	Для достижения индикатора ОПК-9.1: Знать технические каналы утечки информации; возможности технических средств перехвата информации; организацию защиты информации от утечки по техническим каналам на объектах информатизации; основные характеристики сигналов электросвязи, спектры и виды модуляции; принципы построения и функционирования систем и сетей передачи информации; способы передачи и распределения информации в телекоммуникационных системах и сетях; основные телекоммуникационные протоколы. Для достижения индикатора ОПК-9.2: Уметь пользоваться нормативными документами в области технической защиты информации; анализировать тенденции развития систем и сетей электросвязи, внедрения новых служб и услуг связи. Для достижения индикатора ОПК-9.3: Владеть навыками решения задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации.

© ФГБОУ ВО «ЧелГУ»

3. СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

3.1 Виды оценочных средств

№ п/п	Код компетенции/ планируемые результаты обучения	Контролируемые темы/ разделы	Наименование оценочного средства для текущего контроля	Наименование оценочного средства на промежуточной аттестации/№ задания
1.	ОПК-6 ОПК-9	Раздел 1. Организационные основы инженерно-технической защиты информации	Собеседование и отчеты по лабораторным работам. Тестовые задания	Вопросы к экзамену (№ 1)
		Раздел 2. Концепция инженерно-технической защиты информации	Собеседование и отчеты по лабораторным работам. Тестовые задания	Вопросы к экзамену (№ 2, 3)
		Раздел 3. Теоретические основы инженерно-технической защиты информации	Собеседование и отчеты по лабораторным работам. Тестовые задания	Вопросы к экзамену (№ 4)
		Раздел 4. Физические основы защиты информации	Собеседование и отчеты по лабораторным работам. Тестовые задания	Вопросы к экзамену (№ 5)
		Раздел 5. Технические средства защиты информации	Собеседование и отчеты по лабораторным работам. Тестовые задания	Вопросы к экзамену (№ 6)
		Раздел 6. Методическое обеспечение инженерно-технической защиты автоматизированных систем	Собеседование и отчеты по лабораторным работам. Тестовые задания	Вопросы к экзамену (№ 7)

3.2 Содержание оценочных средств

Темы лабораторных работ:

1) Обнаружение и локализация источников радиоизлучений.
2) Оценка защищённости технических средств от утечки информации по каналу побочных электромагнитных излучений и наводок (ПЭМИН), анализатор спектра.
3) Защита информации по каналам ПЭМИН.
4) Оценка защищенности помещений от утечки информации по виброакустическому и акустическому каналам, защита акустической информации.
5) Проверка на наличие технических средств негласного получения информации в помещении.
6) Защита от НСД.

© ФГБОУ ВО «ЧелГУ»

Типовые вопросы для собеседования по лабораторным работам:

Основные проблемы инженерно-технической защиты информации.

Физическая природа побочных электромагнитных излучений. Основные уравнения электромагнитного поля.

Направления инженерно-технической защиты информации.

Защита конфиденциальной информации от несанкционированного доступа в автоматизированных системах.

Информация как предмет защиты.

Аттестация объектов информатизации.

Демаскирующие признаки.

Акустический и виброакустический каналы утечки информации.

Виды побочных опасных электромагнитных излучений.

Основные физические характеристики акустических волн и восприятие их человеком.

Технические каналы утечки информации.

Технические средства негласного съема информации, применяемые в радиоэлектронном диапазоне длин волн.

Методы инженерной защиты и технической охраны объекта.

Построение каналов утечки информации в радиоэлектронном диапазоне длин волн.

Методы скрытия информации и ее носителей.

Органы добывания информации, структура органов разведки и ее виды. разведки коммерческих структур.

Распространение сигналов в технических каналах утечки информации.

Виды угроз безопасности информации, принципы добывания и обработки информации.

Средства технической разведки.

Побочные излучения и наводки.

Государственная система защиты информации.

Источники функциональных сигналов. Фильтрация информационных сигналов.

Контроль эффективности инженерно-технической защиты информации.

Источники опасных сигналов (физические поля, электрические сигналы).

Методические рекомендации по оценке эффективности защиты информации.

Нормативные документы по противодействию технической разведке.

Моделирование инженерно-технической защиты информации.

Способы записи информации на различные виды носителей и принципы съема информации.

Средства предотвращения утечки информации по техническим каналам. Пространственное и линейное зашумление.

Основные демаскирующие признаки радиолокационных станций, лазерных излучений.

Средства инженерной защиты и технической охраны. Система охранно-тревожной сигнализации. Система контроля и управления доступом.

Особенности видовых признаков в видимом, инфракрасном и радиодиапазонах электромагнитных волн.

Физические основы побочных электромагнитных излучений и наводок.

Классификация сигналов по форме, физической природе, виду информации и регулярности появления. Параметры сигналов.

Физические процессы подавления опасных сигналов.

Демаскирующие признаки веществ.

Методы инженерно-технической защиты информации.

© ФГБОУ ВО «ЧелГУ»

Видовые, сигнальные и вещественные демаскирующие признаки. информационность признаков.
Каналы утечки информации за счет паразитных связей.
Классификация демаскирующих признаков. Опознавательные признаки и признаки деятельности объектов.
Характеристика технической разведки.
Объект защиты, носитель информации, информационные процессы.
Показатели эффективности инженерно – технической защиты информации.
Организационно – технические мероприятия по защите информации
Свойства информации, влияющие на ее безопасность.
Виды защищаемой информации. Защита информации от утечки, непреднамеренного и несанкционированного воздействия на нее.
Системный подход к защите информации.
Ценность информации.
Основные концептуальные положения инженерно-технической защиты информации.
Основные свойства информации как предмета защиты.
Технические средства защиты информации. Средства выявления каналов утечки информации.
Критерии оценивания собеседования и отчета по лабораторным работам:

В процессе выполнения лабораторной работы каждый студент составляет индивидуальный отчет, который включает расчетную часть, а также аналитическую часть и выводы. По подготовленному отчету проводится собеседование.

Лабораторная работа засчитывается студенту, если он представил правильно оформленный отчет, знает схему лабораторной установки и принцип ее работы; владеет методикой обработки экспериментальных данных; усвоил теоретический материал по данной теме (последовательно, грамотно и логически стройно его излагает, уверенно отвечает на вопросы). Допускаются несущественные неточности в оформлении и ответах на вопросы.

Лабораторная работа не засчитывается студенту в случаях: наличия ошибок в расчетах, неправильного оформления отчета, искажающего смысл задания, существенных ошибок при ответах на вопросы.

Перечень тестовых заданий для текущего контроля
Вариант №1

1. Какие основные угрозы могут быть связаны с технической защитой информации?
a) Вирусы и вредоносные программы
b) Физическое повреждение оборудования
c) Несанкционированный доступ к данным
d) Все перечисленное выше

2. Что такое уровень целостности данных?
a) Способность данных быть доступными только для авторизованных пользователей
b) Способность данных оставаться неизменными и быть защищенными от несанкционированного изменения
c) Способность данных быть достоверными и точными
d) Способность данных быть сохраненными и доступными в случае сбоя системы

3. Что такое политика безопасности информации?
a) Набор правил и регуляций, определяющих принципы и стратегию защиты информации

© ФГБОУ ВО «ЧелГУ»

b) Программное обеспечение для контроля и мониторинга доступа к информации
c) Способность системы автоматически обнаруживать и предотвращать вторжения
d) Все перечисленное выше

4. Какая роль играет обучение пользователей в обеспечении технической защиты информации?

a) Обучение помогает пользователям понять основные принципы безопасности и правила использования информационных систем
b) Обучение не играет роли в обеспечении технической защиты информации
c) Обучение позволяет пользователям настроить системные параметры для повышения безопасности
d) Обучение помогает идентифицировать и предотвращать кибератаки

5. Какие методы технической защиты информации могут использоваться для предотвращения несанкционированного доступа?

a) Аутентификация и авторизация
b) Фильтрация сетевого трафика
c) Контроль доступа к системным ресурсам
d) Все перечисленное выше

6. Что такое антивирусное программное обеспечение?

a) Программное обеспечение для защиты систем от вирусов
b) Программное обеспечение для шифрования данных
c) Программное обеспечение для контроля доступа
d) Программное обеспечение для аутентификации пользователей

7. Что такое бекапирование (резервное копирование) данных?

a) Процесс сохранения копии данных для их восстановления в случае потери или повреждения
b) Процесс шифрования данных для защиты их от несанкционированного доступа
c) Процесс аутентификации пользователей перед предоставлением им доступа к данным
d) Процесс контроля доступа к системным ресурсам

8. Какие меры безопасности могут быть связаны с физическими преградами?

a) Установка видеонаблюдения и систем контроля доступа
b) Использование мощных шифровальных алгоритмов для защиты данных
c) Усиление физической защиты зданий и помещений
d) Все перечисленное выше

9. Что такое техническая защита информации?

a) Защита информации с использованием криптографических методов
b) Защита информации с использованием технических, программных и программно-технических средств
c) Защита информации с использованием физических преград
d) Защита информации с использованием социальных мер безопасности

10. Какие задачи решает техническая защита информации?

a) Предотвращение утечки информации через технические каналы утечки информации
b) Предотвращение несанкционированного доступа к информации
c) Обеспечение целостности, конфиденциальности и доступности защищаемой информации
d) Все перечисленное выше

11. Кто является регулятором в области обеспечения технической защиты информации в Российской Федерации?

© ФГБОУ ВО «ЧелГУ»

a) Федеральная служба по техническому и экспортному контролю
b) Федеральная служба безопасности
c) Министерство обороны
d) Министерство связи и массовых коммуникаций

12. Что может являться объектом технической защиты информации?
a) Объект информатизации
b) Информационная система/автоматизированная система
c) Ресурсы информационной системы/автоматизированной системы
d) Все перечисленное выше

13. Какие основные цели имеет техническая защита информации?
a) Обеспечение целостности информации
b) Обеспечение конфиденциальности информации
c) Обеспечение доступности информации
d) Все перечисленное выше

14. Какие методы могут использоваться для обеспечения технической защиты информации?
a) Физические преграды
b) Криптографические методы
c) Технические средства
d) Все перечисленное выше

15. Какие определения информации существуют?
a) Единственное формальное определение информации
b) Множество определений информации в зависимости от контекста
c) Определение информации, основанное на законах информатики
d) Определение информации, основанное на социологии

16. Какие принципы включает в себя техническая защита информации?
a) Принцип обязательности
b) Принцип целесообразности
c) Принцип градации мер безопасности
d) Все перечисленное выше

17. Какие основные категории угроз информационной безопасности существуют?
a) Технические угрозы
b) Организационные угрозы
c) Персональные угрозы
d) Все перечисленное выше

18. Какие виды ресурсов информационной системы могут подлежать защите?
a) Аппаратные ресурсы
b) Программные ресурсы
c) Информационные ресурсы
d) Все перечисленное выше

19. Какие преимущества обеспечения безопасности сетевых соединений с помощью виртуальных частных сетей (VPN)?
a) Шифрование данных для защиты конфиденциальности
b) Обеспечение анонимности пользователя
c) Позволяет подключаться к защищенным сетям удаленно
d) Предотвращение перехвата данных в общественных Wi-Fi сетях

20. Что такое защита от атак по сети и почему она важна?

© ФГБОУ ВО «ЧелГУ»

a) Обеспечение безопасности сетевых соединений и защита от несанкционированного доступа
b) Защита от физических угроз и контроль доступа в помещения
c) Шифрование данных и защита от вредоносного программного обеспечения
d) Отслеживание активности пользователей и аудит безопасности

Вариант №2

1. Какие основные угрозы могут быть связаны с технической защитой информации?
a) Вирусы и вредоносные программы
b) Физическое повреждение оборудования
c) Несанкционированный доступ к данным
d) Все перечисленное выше

2. Что такое уровень целостности данных?
a) Способность данных быть доступными только для авторизованных пользователей
b) Способность данных оставаться неизменными и быть защищенными от несанкционированного изменения
c) Способность данных быть достоверными и точными
d) Способность данных быть сохраненными и доступными в случае сбоя системы

3. Что такое политика безопасности информации?
a) Набор правил и регуляций, определяющих принципы и стратегию защиты информации
b) Программное обеспечение для контроля и мониторинга доступа к информации
c) Способность системы автоматически обнаруживать и предотвращать вторжения
d) Все перечисленное выше

4. Какая роль играет обучение пользователей в обеспечении технической защиты информации?
a) Обучение помогает пользователям понять основные принципы безопасности и правила использования информационных систем
b) Обучение не играет роли в обеспечении технической защиты информации
c) Обучение позволяет пользователям настроить системные параметры для повышения безопасности
d) Обучение помогает идентифицировать и предотвращать кибератаки

5. Какие методы технической защиты информации могут использоваться для предотвращения несанкционированного доступа?
a) Аутентификация и авторизация
b) Фильтрация сетевого трафика
c) Контроль доступа к системным ресурсам
d) Все перечисленное выше

6. Какие методы защиты от атак по сети могут использоваться?
a) Файрволлы, сетевые прокси, виртуальные частные сети (VPN)
b) Антивирусное программное обеспечение, межсетевые экраны, IDS/IPS
c) Шифрование данных, аутентификация и контроль доступа
d) Межсетевые экраны, виртуальные частные сети (VPN), IDS/IPS

7. Что такое защита от вредоносного программного обеспечения и какие методы защиты можно применить?
a) Обеспечение безопасности от вирусов, троянов и других вредоносных программ
b) Аутентификация и шифрование данных
c) Контроль доступа и мониторинг активности пользователей
d) Физическая защита и контроль угроз в реальном времени

© ФГБОУ ВО «ЧелГУ»

8. Что такое аудит безопасности и какая роль у него в обеспечении информационной безопасности?
a) Систематическая оценка и проверка безопасности информационных систем
b) Предотвращение хищения и утечек конфиденциальной информации
c) Мониторинг и обнаружение вторжений и несанкционированной активности
d) Определение уязвимостей и предотвращение атак по сети
9. Какие основные меры безопасности могут помочь защитить информацию от угроз в реальном времени?
a) Бэкап данных, контроль доступа и шифрование
b) Межсетевые экраны, IDS/IPS и аутентификация пользователей
c) Антивирусное программное обеспечение, файрволлы и виртуальные частные сети (VPN)
d) Физическая защита, контроль угроз и мониторинг активности
10. Что такое аутентификация и зачем она используется?
a) Подтверждение подлинности и идентификация пользователей
b) Защита от вредоносного программного обеспечения
c) Шифрование конфиденциальной информации
d) Обеспечение целостности данных
11. Какие методы аутентификации могут использоваться для проверки подлинности пользователя?
a) Логин и пароль, биометрические данные, одноразовые коды
b) Антивирусное программное обеспечение, файрволлы, VPN
c) Криптографические алгоритмы, сетевые протоколы, защитные меры
d) Контроль доступа, системы мониторинга, физические барьеры
12. Что такое авторизация и почему она важна в контексте информационной безопасности?
a) Проверка прав доступа пользователя к определенным ресурсам
b) Шифрование данных для защиты от несанкционированного доступа
c) Контроль целостности информации и предотвращение ее изменения
d) Анализ угроз и реагирование на них в реальном времени
13. Какие принципы безопасности помогают обеспечить аутентификацию и авторизацию пользователей?
a) Необходимость знания и секретность
b) Принцип наименьших привилегий и разделение обязанностей
c) Отслеживание активности и контроль доступа
d) Физическая безопасность и защита от внутренних угроз
14. Какой вид защиты информации является одним из видов инженерно-технической защиты?
a) Физическая защита
b) Криптографическая защита
c) Компьютерная защита
d) Юридическая защита
15. Что такое информационная безопасность?
a) Защита от хищения информации
b) Защита информационных технологий
c) Обеспечение конфиденциальности информации
d) Комплекс мер по предотвращению угроз информации
16. Какие основные принципы информационной безопасности существуют?

© ФГБОУ ВО «ЧелГУ»

a) Конфиденциальность, целостность, доступность
b) Аутентификация, авторизация, аудит
c) Защита от внешних и внутренних угроз
d) Профилактика, реагирование, восстановление

17. Что представляют собой объекты защиты информации?
a) Физические лица, имеющие доступ к информации
b) Технические средства защиты информации
c) Компьютерные программы и алгоритмы
d) Материальные носители информации и информационные системы

18. Какие виды конфиденциальной информации выделяются в зависимости от области деятельности человека?
a) Служебная, профессиональная, промышленная, коммерческая, государственная, военная
b) Личная, рабочая, техническая, финансовая
c) Секретная, закрытая, открытая, публичная
d) Внутренняя, внешняя, секретная, публичная

19. Какими свойствами обладает информация?
a) Масса, размеры, энергия
b) Физические параметры
c) Уникальность, отсутствие физических параметров
d) Существование только на материальном носителе

20. Какие объекты защиты информации существуют с точки зрения защиты?
a) Материальные средства
b) Материальные носители информации
c) Физические поля
d) Источники информации

Вариант №3

1. Что такое антивирусное программное обеспечение?
a) Программное обеспечение для защиты систем от вирусов
b) Программное обеспечение для шифрования данных
c) Программное обеспечение для контроля доступа
d) Программное обеспечение для аутентификации пользователей

2. Что такое бекапирование (резервное копирование) данных?
a) Процесс сохранения копии данных для их восстановления в случае потери или повреждения
b) Процесс шифрования данных для защиты их от несанкционированного доступа
c) Процесс аутентификации пользователей перед предоставлением им доступа к данным
d) Процесс контроля доступа к системным ресурсам

3. Какие меры безопасности могут быть связаны с физическими преградами?
a) Установка видеонаблюдения и систем контроля доступа
b) Использование мощных шифровальных алгоритмов для защиты данных
c) Усиление физической защиты зданий и помещений
d) Все перечисленное выше

4. Что такое техническая защита информации?
a) Защита информации с использованием криптографических методов
b) Защита информации с использованием технических, программных и программно-технических средств

© ФГБОУ ВО «ЧелГУ»

c) Защита информации с использованием физических преград
d) Защита информации с использованием социальных мер безопасности

5. Какие задачи решает техническая защита информации?

a) Предотвращение утечки информации через технические каналы утечки информации
b) Предотвращение несанкционированного доступа к информации
c) Обеспечение целостности, конфиденциальности и доступности защищаемой информации
d) Все перечисленное выше

6. Какие принципы включает в себя техническая защита информации?

a) Принцип обязательности
b) Принцип целесообразности
c) Принцип градации мер безопасности
d) Все перечисленное выше

7. Какие основные категории угроз информационной безопасности существуют?

a) Технические угрозы
b) Организационные угрозы
c) Персональные угрозы
d) Все перечисленное выше

8. Какие виды ресурсов информационной системы могут подлежать защите?

a) Аппаратные ресурсы
b) Программные ресурсы
c) Информационные ресурсы
d) Все перечисленное выше

9. Какие преимущества обеспечения безопасности сетевых соединений с помощью виртуальных частных сетей (VPN)?

a) Шифрование данных для защиты конфиденциальности
b) Обеспечение анонимности пользователя
c) Позволяет подключаться к защищенным сетям удаленно
d) Предотвращение перехвата данных в общественных Wi-Fi сетях

10. Что такое защита от атак по сети и почему она важна?

a) Обеспечение безопасности сетевых соединений и защита от несанкционированного доступа
b) Защита от физических угроз и контроль доступа в помещения
c) Шифрование данных и защита от вредоносного программного обеспечения
d) Отслеживание активности пользователей и аудит безопасности

11. Какие методы аутентификации могут использоваться для проверки подлинности пользователя?

a) Логин и пароль, биометрические данные, одноразовые коды
b) Антивирусное программное обеспечение, фаерволы, VPN
c) Криптографические алгоритмы, сетевые протоколы, защитные меры
d) Контроль доступа, системы мониторинга, физические барьеры

12. Что такое авторизация и почему она важна в контексте информационной безопасности?

a) Проверка прав доступа пользователя к определенным ресурсам
b) Шифрование данных для защиты от несанкционированного доступа
c) Контроль целостности информации и предотвращение ее изменения
d) Анализ угроз и реагирование на них в реальном времени

© ФГБОУ ВО «ЧелГУ»

13. Какие принципы безопасности помогают обеспечить аутентификацию и авторизацию пользователей?

a) Необходимость знания и секретность
b) Принцип наименьших привилегий и разделение обязанностей
c) Отслеживание активности и контроль доступа
d) Физическая безопасность и защита от внутренних угроз

14. Какой вид защиты информации является одним из видов инженерно-технической защиты?

a) Физическая защита
b) Криптографическая защита
c) Компьютерная защита
d) Юридическая защита

15. Что такое информационная безопасность?

a) Защита от хищения информации
b) Защита информационных технологий
c) Обеспечение конфиденциальности информации
d) Комплекс мер по предотвращению угроз информации

16. Какие основные угрозы могут быть связаны с технической защитой информации?

a) Вирусы и вредоносные программы
b) Физическое повреждение оборудования
c) Несанкционированный доступ к данным
d) Все перечисленное выше

17. Что такое уровень целостности данных?

a) Способность данных быть доступными только для авторизованных пользователей
b) Способность данных оставаться неизменными и быть защищенными от несанкционированного изменения
c) Способность данных быть достоверными и точными
d) Способность данных быть сохраненными и доступными в случае сбоя системы

18. Что такое политика безопасности информации?

a) Набор правил и регуляций, определяющих принципы и стратегию защиты информации
b) Программное обеспечение для контроля и мониторинга доступа к информации
c) Способность системы автоматически обнаруживать и предотвращать вторжения
d) Все перечисленное выше

19. Какая роль играет обучение пользователей в обеспечении технической защиты информации?

a) Обучение помогает пользователям понять основные принципы безопасности и правила использования информационных систем
b) Обучение не играет роли в обеспечении технической защиты информации
c) Обучение позволяет пользователям настроить системные параметры для повышения безопасности
d) Обучение помогает идентифицировать и предотвращать кибератаки

20. Какие методы технической защиты информации могут использоваться для предотвращения несанкционированного доступа?

a) Аутентификация и авторизация
b) Фильтрация сетевого трафика
c) Контроль доступа к системным ресурсам
d) Все перечисленное выше

© ФГБОУ ВО «ЧелГУ»

Вариант №4

1. Какие основные принципы информационной безопасности существуют?
a) Конфиденциальность, целостность, доступность
b) Аутентификация, авторизация, аудит
c) Защита от внешних и внутренних угроз
d) Профилактика, реагирование, восстановление

2. Что представляют собой объекты защиты информации?
a) Физические лица, имеющие доступ к информации
b) Технические средства защиты информации
c) Компьютерные программы и алгоритмы
d) Материальные носители информации и информационные системы

3. Какие виды конфиденциальной информации выделяются в зависимости от области деятельности человека?
a) Служебная, профессиональная, промышленная, коммерческая, государственная, военная
b) Личная, рабочая, техническая, финансовая
c) Секретная, закрытая, открытая, публичная
d) Внутренняя, внешняя, секретная, публичная

4. Какими свойствами обладает информация?
a) Масса, размеры, энергия
b) Физические параметры
c) Уникальность, отсутствие физических параметров
d) Существование только на материальном носителе

5. Какие объекты защиты информации существуют с точки зрения защиты?
a) Материальные средства
b) Материальные носители информации
c) Физические поля
d) Источники информации

6. Какие методы защиты от атак по сети могут использоваться?
a) Файрволы, сетевые прокси, виртуальные частные сети (VPN)
b) Антивирусное программное обеспечение, межсетевые экраны, IDS/IPS
c) Шифрование данных, аутентификация и контроль доступа
d) Межсетевые экраны, виртуальные частные сети (VPN), IDS/IPS

7. Что такое защита от вредоносного программного обеспечения и какие методы защиты можно применить?
a) Обеспечение безопасности от вирусов, троянов и других вредоносных программ
b) Аутентификация и шифрование данных
c) Контроль доступа и мониторинг активности пользователей
d) Физическая защита и контроль угроз в реальном времени

8. Что такое аудит безопасности и какая роль у него в обеспечении информационной безопасности?
a) Систематическая оценка и проверка безопасности информационных систем
b) Предотвращение хищения и утечек конфиденциальной информации
c) Мониторинг и обнаружение вторжений и несанкционированной активности
d) Определение уязвимостей и предотвращение атак по сети

9. Какие основные меры безопасности могут помочь защитить информацию от угроз в реальном времени?
a) Бэкап данных, контроль доступа и шифрование

© ФГБОУ ВО «ЧелГУ»

b) Межсетевые экраны, IDS/IPS и аутентификация пользователей
c) Антивирусное программное обеспечение, файрволлы и виртуальные частные сети (VPN)
d) Физическая защита, контроль угроз и мониторинг активности

10. Что такое аутентификация и зачем она используется?
a) Подтверждение подлинности и идентификация пользователей
b) Защита от вредоносного программного обеспечения
c) Шифрование конфиденциальной информации
d) Обеспечение целостности данных

11. Кто является регулятором в области обеспечения технической защиты информации в Российской Федерации?
a) Федеральная служба по техническому и экспортному контролю
b) Федеральная служба безопасности
c) Министерство обороны
d) Министерство связи и массовых коммуникаций

12. Что может являться объектом технической защиты информации?
a) Объект информатизации
b) Информационная система/автоматизированная система
c) Ресурсы информационной системы/автоматизированной системы
d) Все перечисленное выше

13. Какие основные цели имеет техническая защита информации?
a) Обеспечение целостности информации
b) Обеспечение конфиденциальности информации
c) Обеспечение доступности информации
d) Все перечисленное выше

14. Какие методы могут использоваться для обеспечения технической защиты информации?
a) Физические преграды
b) Криптографические методы
c) Технические средства
d) Все перечисленное выше

15. Какие определения информации существуют?
a) Единственное формальное определение информации
b) Множество определений информации в зависимости от контекста
c) Определение информации, основанное на законах информатики
d) Определение информации, основанное на социологии

16. Какие основные угрозы могут быть связаны с технической защитой информации?
a) Вирусы и вредоносные программы
b) Физическое повреждение оборудования
c) Несанкционированный доступ к данным
d) Все перечисленное выше

17. Что такое уровень целостности данных?
a) Способность данных быть доступными только для авторизованных пользователей
b) Способность данных оставаться неизменными и быть защищенными от несанкционированного изменения
c) Способность данных быть достоверными и точными
d) Способность данных быть сохраненными и доступными в случае сбоя системы

18. Что такое политика безопасности информации?

© ФГБОУ ВО «ЧелГУ»

a) Набор правил и регуляций, определяющих принципы и стратегию защиты информации
b) Программное обеспечение для контроля и мониторинга доступа к информации
c) Способность системы автоматически обнаруживать и предотвращать вторжения
d) Все перечисленное выше

19. Какая роль играет обучение пользователей в обеспечении технической защиты информации?

a) Обучение помогает пользователям понять основные принципы безопасности и правила использования информационных систем
b) Обучение не играет роли в обеспечении технической защиты информации
c) Обучение позволяет пользователям настроить системные параметры для повышения безопасности
d) Обучение помогает идентифицировать и предотвращать кибератаки

20. Какие методы технической защиты информации могут использоваться для предотвращения несанкционированного доступа?

a) Аутентификация и авторизация
b) Фильтрация сетевого трафика
c) Контроль доступа к системным ресурсам
d) Все перечисленное выше

Ключи к тесту

№ п/п	Вариант № 1	Вариант № 2	Вариант №3	Вариант №4
1	d	d	a	a
2	b	b	a	d
3	a	a	c	a
4	a	a	b	c
5	d	d	d	b
6	a	a, b	d	a, b
7	a	a	d	a
8	b	a, c	d	a, c
9	d	b	a, c, d	b
10	a	a	a	a
11	d	a	a	a
12	d	a	a	d
13	d	b	b	d
14	b	a	a	d
15	d	d	d	b
16	d	a	d	d
17	d	d	b	b
18	a, c, d	a	a	a
19	a	c	a	a
20	d	b	d	d

Критерии оценивания теста:

Тест - система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося. Важнейшими достоинствами тестов являются:

© ФГБОУ ВО «ЧелГУ»

1) экономия времени преподавателя
2) возможность поставить всех студентов в одинаковые условия
3) возможность разработки равноценных по трудности вариантов вопросов
4) возможность проверить обоснованность оценки
5) уменьшение субъективного подхода к оценке подготовки студента, обусловленного его индивидуальными особенностями

За тест ставится оценка "зачтено", если выполнено правильно более половины заданий.

Вопросы к экзамену:

1. Организационные основы инженерно-технической защиты информации.
2. Основные свойства информации как предмета защиты.
3. Концепции инженерно-технической защиты информации.
4. Теоретические основы инженерно-технической защиты информации.
5. Физические основы защиты информации.
6. Технические средства защиты информации.
7. Методическое обеспечение инженерно-технической защиты автоматизированных систем.

4. ПОРЯДОК ПРОВЕДЕНИЯ И КРИТЕРИИ ОЦЕНИВАНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

4.1. Порядок проведения промежуточной аттестации

Студент допускается к экзамену по дисциплине в случае выполнения им учебного плана по дисциплине: выполненных и защищенных работ. В случае наличия учебной задолженности студент отрабатывает пропущенные занятия в форме, предложенной преподавателем и представленной в настоящей программе.

Экзамен проводится по билетам в устной форме. При проведении экзамена экзаменуемый выбирает билет в случайном порядке. Экзаменатору предоставляется право по ходу экзамена задавать экзаменуемому уточняющие и дополнительные вопросы. Время подготовки студента для устного ответа на экзамене должно составлять не менее 40 минут, время ответа экзаменуемого – не более 20 минут. При подготовке и ответе на вопросы билета экзаменуемый должен вести необходимые записи в листе устного ответа, который по окончании экзамена подписывается студентом, сдаётся экзаменатору и сохраняется им до окончания экзаменационной сессии. Студент, испытавший затруднения при подготовке к ответу по выбранному билету, вправе выбрать второй билет с продлением времени на подготовку. При этом окончательная оценка студента снижается на один балл. Выбор студентом третьего билета не допускается.

Проявленные студентом в ходе экзамена знания оцениваются оценками «отлично», «хорошо», «удовлетворительно» и «неудовлетворительно».

4.2. Критерии оценивания промежуточной аттестации по видам оценочных средств

Критерии оценивания ответа (устного опроса) на экзамене:

Оценка «отлично» выставляется:

Дан полный, развернутый ответ на поставленный вопрос, показана совокупность осознанных знаний по дисциплине, доказательно раскрыты основные положения вопросов; в ответе прослеживается четкая структура, логическая последовательность, отражающая

© ФГБОУ ВО «ЧелГУ»

сущность раскрываемых понятий, теорий, явлений. Знания по предмету демонстрируется на фоне понимания его в системе данной науки и междисциплинарных связей. Ответ изложен литературным языком с использованием современной терминологии. Могут быть допущены недочеты в определении понятий, исправленные студентом самостоятельно в процессе ответа.

Оценка «хорошо» выставляется:

Дан полный, развернутый ответ на поставленный вопрос, показано умение выделить существенные и несущественные признаки, причинно-следственные связи. Ответ четко структурирован, логичен, изложен литературным языком с использованием современной терминологии. Могут быть допущены некоторые неточности или незначительные ошибки, исправленные студентом с помощью преподавателя.

Оценка «удовлетворительно» выставляется:

Дан недостаточно полный и недостаточно развернутый ответ. Логика и последовательность изложения имеют нарушения. Допущены ошибки в раскрытии понятий, употреблении терминов. Студент не способен самостоятельно выделить существенные и несущественные признаки и причинно-следственные связи. В ответе отсутствуют выводы. Умение раскрыть значение обобщенных знаний не показано. Речевое оформление требует поправок, коррекции.

Оценка «неудовлетворительно» выставляется:

1) Ответ представляет собой разрозненные знания с существенными ошибками по вопросу. Присутствуют фрагментарность, нелогичность изложения. Студент не осознает связь обсуждаемого вопроса по билету с другими объектами дисциплины. Отсутствуют выводы, конкретизация и доказательность изложения. Речь неграмотная. Дополнительные и уточняющие вопросы преподавателя не приводят к коррекции ответа студента.

2) Ответ на вопрос полностью отсутствует.

3) Отказ от ответа.

Особенности проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья обозначены в рабочей программе дисциплины (модуля).

4.3. Результаты промежуточной аттестации и уровни сформированности компетенций

1. Высокий уровень сформированности компетенций соответствует оценке «отлично».
2. Средний уровень сформированности компетенций соответствует оценке «хорошо».
3. Базовый уровень сформированности компетенций соответствует оценке «удовлетворительно».
4. Низкий уровень сформированности компетенций соответствует оценке «неудовлетворительно».

© ФГБОУ ВО «ЧелГУ»

шифр: 10.05.01,
специализация N 6 "Информационно-аналитическая и техническая экспертиза компьютерных систем",
специальность: Компьютерная безопасность,
название ФОС: Защита информации от утечки по техническим каналам,
год набора: 2026,
форма обучения: очная

Фонд оценочных средств дисциплины (модуля) одобрен и рекомендован:

Проректор по учебной работе	утверждено 27.02.26	А.А. Саламатов

Ученым советом математического факультета

Протокол заседания № 8 от 19.02.2026

Председатель Ученого совета математического факультета	согласовано	А. С. Скорынин

Заседанием кафедры радиофизики и электроники

Протокол заседания № 07 от 03.02.2026

Заведующий кафедрой	согласовано	А.В. Бутаков
Автор (составитель)		И.С. Зотов

Структура фондов оценочных средств соответствует приказу ректора ФГБОУ ВО «ЧелГУ» от 27 сентября 2022 №573-1