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 №1
Анализ безопасности компьютерных систем

Присваиваемая квалификация (степень)
Специалист по защите информации

Форма обучения
Очная

Челябинск, 2025 г.

Содержание

1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

Специальность: 10.05.01 Компьютерная безопасность
Специализация: Анализ безопасности 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 «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. ОПК-6.2. Умеет	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.

		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.

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.	Вопросы к экзамену (№ 1)
		Раздел 2. Концепция инженерно-технической защиты информации	Собеседование и отчеты по лабораторным работам.	Вопросы к экзамену (№ 2, 3)
		Раздел 3. Теоретические основы инженерно-технической защиты информации	Собеседование и отчеты по лабораторным работам.	Вопросы к экзамену (№ 4)
		Раздел 4. Физические основы защиты информации	Собеседование и отчеты по лабораторным работам.	Вопросы к экзамену (№ 5)
		Раздел 5. Технические средства защиты информации	Собеседование и отчеты по лабораторным работам.	Вопросы к экзамену (№ 6)
		Раздел 6. Методическое обеспечение инженерно-технической защиты автоматизированных систем	Собеседование и отчеты по лабораторным работам.	Вопросы к экзамену (№ 7)

3.2 Содержание оценочных средств

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.
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.

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 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».

шифр: 10.05.01,
специализация N 1 "Анализ безопасности компьютерных систем",
специальность: Компьютерная безопасность,
название ФОС: Защита информации от утечки по техническим каналам,
год набора: 2025,
форма обучения: очная

Фонд оценочных средств дисциплины (модуля) одобрен и рекомендован:

Проректор по учебной работе	утверждено 24.02.25	А.А. Саламатов

Ученым советом математического факультета

Протокол заседания № 6 от 20.02.2025

Председатель Ученого совета математического факультета	согласовано	Е.А. Сбродова

Заседанием кафедры радиофизики и электроники

Протокол заседания № 07 от 04.02.2025

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

Структура рабочей программы соответствует приказу ректора ФГБОУ ВО «ЧелГУ» от «13» апреля 2021 г. № 247-1