МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Кузбасский государственный технический университет имени Т. Ф. Горбачева»

Филиал КузГТУ в г. Новокузнецке

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 71B13ADF852F0D849D78875814FBEF47
Владелец: Баранов Юрий Александрович
Действителен: с 15.10.2025 до 08.01.2027

УТВЕРЖДЕНО

Заместитель директора,
совмещающий обязанности директора
филиала КузГТУ в г. Новокузнецке

_____Баранов Ю.А.

«29» мая 2026г.

Рабочая программа дисциплины

Техническая защита информации

Направление подготовки 10.05.03 Информационная безопасность автоматизированных систем

Направленность (профиль) Анализ безопасности информационных систем

Присваиваемая квалификация «Специалист по защите информации»

Формы обучения: очная

Год набора 2026

Новокузнецк 2026 г.

Рабочая программа обсуждена на заседании учебно-методического совета филиала КузГТУ в г. Новокузнецке

Протокол № 6 от 29.05.2026

Зав. Кафедрой ИТиЭД _____ В. В. Шарлай
подпись

СОГЛАСОВАНО:

Заместитель директора по УР _____ Т. А. Евсина
подпись

1 Перечень планируемых результатов обучения по дисциплине "Техническая защита информации", соотнесенных с планируемыми результатами освоения образовательной программы

Освоение дисциплины направлено на формирование:

общепрофессиональных компетенций:

ОПК-9 - Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации;

Результаты обучения по дисциплине определяются индикаторами достижения компетенций

Индикатор(ы) достижения:

Применяет знания в области технической защиты информации, применяет их в работе с техническими каналами утечки информации, знает возможности технических разведок, знает способы и средства защиты информации от утечки по техническим каналам.

Результаты обучения по дисциплине:

Знать технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам.

Уметь анализировать и оценивать угрозы информационной безопасности объекта; применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем, пользоваться нормативными документами по защите информации.

Владеть методами и средствами выявления угроз безопасности автоматизированным системам; методами технической защиты информации; методами формирования требований по защите информации; методами расчета и инструментального контроля показателей технической защиты информации.

2 Место дисциплины "Техническая защита информации" в структуре ОПОП специалитета

Для освоения дисциплины необходимы знания умения, навыки и (или) опыт профессиональной деятельности, полученные в рамках изучения следующих дисциплин: Организационное и правовое обеспечение информационной безопасности, Основы информационной безопасности, Управление информационной безопасностью, Программно-аппаратные средства защиты информации, Нормативные требования по защите информации, Основы информатики, организации ЭВМ, вычислительных и информационных систем, Информационные угрозы, Классификация защищаемой информации и информационных систем, Методы и средства защиты информационных систем, Методы обнаружения угроз безопасности информационных систем.

Дисциплина входит в Блок 1 «Дисциплины (модули)» ОПОП. Цель дисциплины - получение обучающимися знаний, умений, навыков и (или) опыта профессиональной деятельности, необходимых для формирования компетенций, указанных в пункте 1.

3 Объем дисциплины "Техническая защита информации" в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам занятий) и на самостоятельную работу обучающихся

Общая трудоемкость дисциплины "Техническая защита информации" составляет 6 зачетных единиц, 216 часов.

Форма обучения	Количество часов		
	ОФ	ЗФ	ОЗФ
Курс 4/Семестр 8			
Всего часов	216		
Контактная работа обучающихся с преподавателем (по видам учебных занятий):			
Аудиторная работа			

Форма обучения	Количество часов		
	ОФ	ЗФ	ОЗФ
Лекции			
Лабораторные занятия	32		
Практические занятия	64		
Внеаудиторная работа			
Индивидуальная работа с преподавателем:			
Консультация и иные виды учебной деятельности			
Самостоятельная работа под руководством преподавателя	16		
Самостоятельная работа	68		
Форма промежуточной аттестации	экзамен /36		

4 Содержание дисциплины "Техническая защита информации", структурированное по разделам (темам)

4.1. Лекционные занятия

Раздел дисциплины, темы лекций и их содержание	Трудоемкость в часах
	ОФ
1. Концепция инженерно-технической защиты информации.	4
2. Теоретические основы инженерно-технической защиты информации.	4
3. Физические основы защиты информации	4
4. Технические средства добывания и инженерно-технической защиты информации.	6
5. Организационные основы инженерно-технической защиты информации	6
6. Методическое обеспечение инженерно-технической защиты информации	8
Итого	**32**

4.2. Лабораторные занятия

Наименование работы	Трудоемкость в часах
	ОФ
4. Технические средства добывания и инженерно-технической защиты информации: Защита телефонного канала от утечки информации. Локация полупроводниковых приборов. Видеонаблюдение. Скремблеры. Селективный металлодетектор.	4
4. Технические средства добывания и инженерно-технической защиты информации: Средства инженерной защиты и технической охраны. Средства предотвращения утечки информации по техническим каналам.	4
5. Организационные основы инженерно-технической защиты информации: Контроль эффективности инженерно-технической защиты информации.	4

6. Методическое обеспечение инженерно-технической защиты информации: Моделирование инженерно-технической защиты информации. Методические рекомендации по оценке эффективности защиты информации.	4
Итого	**16**

4.3 Практические (семинарские) занятия

Тема занятия	**Трудоемкость в часах**
	ОФ
1. Концепция инженерно-технической защиты информации: Системный подход к защите информации. Основные проблемы инженерно-технической защиты информации. Основные концептуальные положения инженерно-технической защиты информации. Направления инженерно-технической защиты информации. Показатели эффективности инженерно-технической защиты информации.	2
2. Теоретические основы инженерно-технической защиты информации: Информация как предмет защиты. Свойства информации, влияющие на ее безопасность. Демаскирующие признаки. Источники опасных сигналов. Виды побочных опасных электромагнитных излучений. Характеристика технической разведки. Технические каналы утечки информации. Методы инженерно-технической защиты информации. Методы инженерной защиты и технической охраны объекта. Методы скрытия информации и ее носителей.	2
3. Физические основы защиты информации: Многоканальный комплекс радиоконтроля «Квадрат». Рекомендации по применению фильтров Локализация радиомикрофонных закладных устройств с помощью метода акустической локации. Оценка защищенности речевой информации на базе аппаратно-программного комплекса VNK-012GL. Защита от скрытой звукозаписи посредством диктофона.	4
3. Физические основы защиты информации: Физические основы побочных электромагнитных излучений и наводок. Распространение сигналов в технических каналах утечки информации. Физические процессы подавления опасных сигналов.	6
4. Технические средства добывания и инженерно-технической защиты информации: Средства технической разведки. Средства инженерной защиты и технической охраны. Средства предотвращения утечки информации по техническим каналам.	6
5. Организационные основы инженерно-технической защиты информации: Государственная система защиты информации. Контроль эффективности инженерно-технической защиты информации.	4
Раздел 6. Методическое обеспечение инженерно-технической защиты информации: Моделирование инженерно-технической защиты информации. Методические рекомендации по оценке эффективности защиты информации.	4
Итого	**32**

4.4 Самостоятельная работа обучающегося и перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Вид СРС	**Трудоемкость в часах**
	ОФ
Ознакомление с содержанием основной и дополнительной литературы, методических материалов, конспектов лекций для подготовки к занятиям	16
Оформление отчетов по практическим и(или) лабораторным работам	26
Подготовка к защите отчетов по лабораторным/практическим работам	16
Подготовка к промежуточной аттестации	6
Итого	**64**
Самостоятельная работа под руководством преподавателя	16
Экзамен	36

5 Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине "Техническая защита информации"

5.1 Паспорт фонда оценочных средств

Планируемые результаты обучения по дисциплине (модулю)
Дисциплина направлена на формирование следующих компетенций выпускника:

Форма(ы) текущего контроля	**Компетенции, формируемые в результате освоения дисциплины (модуля)**	**Индикатор(ы) достижения компетенции**	**Результаты обучения по дисциплине (модулю)**	**Уровень**

Опрос по контрольным вопросам или тестирование, подготовка отчетов по практическим и(или) лабораторным работам	ОПК-9 - Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации	Применяет знания в области технической защиты информации, применяет их в работе с техническими каналами утечки информации, знает возможности технических разведок, знает способы и средства защиты информации от утечки по техническим каналам.	**Знать** технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам. **Уметь** анализировать и оценивать угрозы информационной безопасности объекта; применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем, пользоваться нормативными документами по защите информации. **Владеть** методами и средствами выявления угроз безопасности автоматизированным системам; методами технической защиты информации; методами формирования требований по защите информации; методами расчета и инструментального контроля показателей технической защиты информации.	Высокий или средний
Высокий уровень достижения компетенции - компетенция сформирована частично, рекомендованные оценки: отлично, хорошо, зачтено. **Средний уровень достижения компетенции** - компетенция сформирована частично, рекомендованные оценки: хорошо, удовлетворительно, зачтено. **Низкий уровень достижения компетенции** - компетенция не сформирована частично, оценивается неудовлетворительно или не зачтено.				

5.2. Типовые контрольные задания или иные материалы

Текущий контроль успеваемости и аттестационные испытания обучающихся могут быть организованы с использованием ресурсов ЭИОС КузГТУ. Полный перечень оценочных материалов расположен в ЭИОС КузГТУ.: https://el.kuzstu.ru/login/index.php.

Текущий контроль успеваемости и аттестационные испытания могут проводиться в письменной и (или) устной, и (или) электронной форме.

5.2.1.Оценочные средства при текущем контроле

Текущий контроль по дисциплине будет заключаться в опросе обучающихся по контрольным вопросам или тестирование по разделу дисциплины, оформлении оформлении отчетов по практическим и(или) лабораторным работам.

Опросе обучающихся по контрольным вопросам или тестирование по разделу дисциплины

Обучающийся отвечает на 2 вопроса, либо отвечает на 10 тестовых заданий.

Например:

1. Классификация информационных сигналов по физической природе.

2. Основные принципы разведки.

Критерии оценивания при ответе на вопросы:
- 100 баллов – при правильном и полном ответе на два вопроса;
- 85…99 баллов – при правильном и полном ответе на один из вопросов и правильном, но не полном ответе на другой из вопросов;
- 75…84 баллов – при правильном и неполном ответе на два вопроса;
- 65…74 баллов – правильном и полном ответе только на один из вопросов
- 25…64 – при правильном и неполном ответе только на один из вопросов;
- 0…24 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0–64	65–100
Шкала оценивания	Не зачтено	Зачтено

Критерии оценивания при тестировании:
- 100 баллов – при правильном и полном ответе на 10 вопросов;
- 85…99 баллов – при правильном ответе на 8-9 вопросов;
- 75…84 баллов – при правильном ответе на 7 вопросов;
- 65…74 баллов – правильном ответе на 5-6 вопросов
- 25…64 – при правильном ответе только на 4 вопроса;
- 0…24 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0–64	65–100
Шкала оценивания	Не зачтено	Зачтено

Примерный перечень контрольных вопросов:

1. Концепция инженерно-технической защиты информации.

1. В чем состоят основные задачи технической защиты информации?

2. Что является предметом технической защиты информации?

3. Что является задачей руководства в процессе внедрения и сопровождения систем технической защиты информации?

4. Какие цели преследует техническая защита информация?

5. Что является объектами технической защиты информации?

2. Теоретические основы инженерно-технической защиты информации.

1. Как называется совокупность условий и факторов, создающих потенциальную угрозу или реально существующую опасность нарушения безопасности информации?

2. Как называется состояние информации, при котором доступ к ней могут осуществить только субъекты, имеющие на него право?

3. Какие существуют виды информационной разведки?

4. Как называется состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право?

5. Как называется состояние информации, при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно?

3. Физические основы защиты информации

1. За счет чего возникает электромагнитный канал утечки информации?

2. Какими средствами разведки фиксируется утечка информации за счет побочных электромагнитных излучений технических средств передачи информации?

3. Какие компоненты радиоэлектронных схем наиболее опасны для возникновения утечки информации?

4. Какие физические поля наиболее сложно контролировать на предмет утечки информации?

5. Как называется способ подавления опасных сигналов, основанный на создания радиопомехи в окружающее пространство?

4. Технические средства добывания и инженерно-технической защиты информации.

1. На основе какого излучения работают генераторы шумовых сигналов для подавления опасного сигнала от диктофонов?

2. При каких процессах работы средств вычислительной техники возможна утечка информации через побочные электромагнитные излучения?

3. В совокупности с какими средствами использование технических средств защиты информации дает наилучший эффект?

4. Возможна ли комбинация в применении нескольких технических средств защиты информации?

5. Какие устройства применяются для одновременного обнаружения всех присутствующих в эфире радиочастот?

5. Организационные основы инженерно-технической защиты информации

1. Какие нормативные документы описывают инженерно-техническую защиту информации?

2. На каких этапах необходимо руководствоваться нормативными документами по инженерно-технической защите информации?

3. Для кого предназначены служебные инструкции по выполнению и соблюдению правил инженерно-технической защиты информации?

4. Кто должен следить за выполнением и соблюдению правил инженерно-технической защиты информации?

5. С кем согласовывается выбор и использование средств инженерно-технической защиты информации?

6. Методическое обеспечение инженерно-технической защиты информации

1. В каких случаях к установке и настройке систем технической защиты информации допускаются только специально уполномоченные организации в соответствии с ФЗ №99?

2. Что включают в себя предварительные испытания системы защиты информации информационной системы по ГОСТ 34.603?

3. Что включает в себя опытная эксплуатация системы защиты информации информационной системы в соответствии с ГОСТ 34.603?

4. Алгоритмы проектирования (совершенствования) инженерно-технической защиты информации

5. Методы моделирования объектов защиты, угроз информации, каналов несанкционированного доступа к объектам информатизации

Примерный перечень тестовых заданий:

1. Концепция инженерно-технической защиты информации.

1. В каком случае система инженерно-технической защиты информации считается эффективной?

функционирует непрерывно
обеспечивает требуемые технические и физические характеристики
обеспечивает выполнение требований и норм по защите

2. Что входит в организационную составляющую ИТЗИ?

подбор и расстановка персонала
регламентация деятельности сотрудников и ИТЗИ
выявление технических каналов утечки информации

3. Сколько категорий нарушений определено в рамках ИТЗИ?

2
3
4
5

2. Теоретические основы инженерно-технической защиты информации.

1.Инженерно-техническая защита решает задачи по предотвращению или уменьшению угроз, вызванных …

стихийными носителями угроз
попытками злоумышленников проникнуть к местам хранения источников информации
организованной или случайной утечкой информации с использованием различных технических средств

2. Контролируемая зона – это …

территория объекта
территория объекта, на которой возможно пребывание посторонних лиц
территория объекта, на которой исключено неконтролируемое пребывание лиц

3. Средства инженерно-технической защиты подразделяются на:

физические, аппаратные, программные, криптографические, комбинированные
физические, программные, криптографические, комбинированные
физические, аппаратные, программные, комбинированные

3. Физические основы защиты информации

1. В число принципов физической защиты входят:

беспощадный отпор
непрерывность защиты в пространстве и времени
минимизация защитных средств

2. В число направлений физической защиты входят:

противопожарные меры
межсетевое экранирование
контроль защищенности

3. Как называется метод физического преграждения пути злоумышленнику к защищаемой информации (сигнализация, замки и т.д.)?

Препятствие
Управление доступом
Маскировка

4. Технические средства добывания и инженерно-технической защиты информации.

1. Как называются технические средства защиты, которые ослабляют уровень информативного сигнала?

активные
пассивные
динамические
демаскирующие

2. Выделите технические мероприятия с использованием пассивных технических средств защиты информации:

звукоизоляция
пространственное зашумление
линейное зашумление
заземление
экранирование

3. Как называется класс устройств, которые позволяют снимать информацию с поверхности оконного стекла помещения

устройства съема информации по вибро-акустическому каналу
устройства съема информации по оптическому каналу
устройства съема информации по звуковому каналу
устройства съема информации по механическому каналу

5. Организационные основы инженерно-технической защиты информации

1. К организационным мерам обеспечения безопасности относятся: выбрать все верные

Формирование политики безопасности организации
Регламентация доступа сотрудников к защищаемым ресурсам
Регламентация доступа в защищаемое помещение

2. Какие из приведенных ниже документов можно отнести к организационным?

федеральные законы
доктрины
уставы

инструкции
указы Президента
распоряжения Президента

3. Организационные требования к системе инженерно-технической защиты информации

управленческие и идентификационные
административные и аппаратурные
административные и процедурные +
аппаратурные и физические

6. Методическое обеспечение инженерно-технической защиты информации

1. Для защиты информации на основе системного подхода и анализа методическое обеспечение должно обеспечивать: выбрать все верные

моделирование объекта защиты;
выявление и моделирование угроз безопасности информации;
разработку мер инженерно-технической защиты информации.
разработку инструкций для персонала

2. Методические рекомендации по разработке мер инженерно-технической защиты информации гласят о том, что разработка мер по защите информации проводится:

эвристическим путем
практическим путем
теоретическим путем
путем проб и ошибок

3. Какая федеральная структура является автором методического документа «МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ В ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ» ?

ФСТЭК России +
ФСБ России
МВД России
Министерство обороны РФ
Департамент информационных технологий РФ («Минцифра»)
Институт инженеров по электротехнике и электронике (IEEE)

Отчеты по лабораторным и (или) практическим работам (далее вместе - работы):

По каждой работе обучающиеся самостоятельно оформляют отчеты в электронном формате (согласно перечню лабораторных и(или) практических работ п.4 рабочей программы).

Содержание отчета:

1.Тема работы.

2. Задачи работы.

3. Краткое описание хода выполнения работы.

4. Ответы на задания или полученные результаты по окончании выполнения работы (в зависимости от задач, поставленных в п. 2).

5. Выводы

Критерии оценивания:

- 75 – 100 баллов – при раскрытии всех разделов в полном объеме

- 0 – 74 баллов – при раскрытии не всех разделов, либо при оформлении разделов в неполном объеме.

Количество баллов	0–74	75–100
Шкала оценивания	Не зачтено	Зачтено

5.2.2 Оценочные средства при промежуточной аттестации

Формами промежуточной аттестации являютя экзамен, в процессе которого определяется сформированность обозначенных в рабочей программе компетенций.

Инструментом измерения сформированности компетенций являются:

ответы на вопросы во время опроса по разделам дисциплины или пройденное тестирование.
зачтенные отчеты обучающихся по лабораторным и(или) практическим работам;

На экзамене обучающийся отвечает на 2 вопроса, либо отвечает на 20 тестовых заданий

Критерии оценивания при ответе на вопросы:

- 100 баллов – при правильном и полном ответе на два вопроса;
- 85…99 баллов – при правильном и полном ответе на один из вопросов и правильном, но не полном ответе на другой из вопросов;
- 75…84 баллов – при правильном и неполном ответе на два вопроса;
- 65…74 баллов – правильном и полном ответе только на один из вопросов
- 25…64 – при правильном и неполном ответе только на один из вопросов;
- 0…24 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0–24	25-64	65-74	85-99	100
Шкала оценивания	Неуд		Хорошо	Отлично	
	не зачтено		зачтено		

Критерии оценивания при тестировании:

- 95-100 баллов – при правильном и полном ответе на 19-20 вопросов;
- 85…94 баллов – при правильном ответе на 16-18 вопросов;
- 75…84 баллов – при правильном ответе на 13-15 вопросов;
- 65…74 баллов – правильном ответе на 10-12 вопросов
- 25…64 – при правильном ответе только на 1-9 вопрос(ов);
- 0…24 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0–24	25-64	65-74	85-94	95-100
Шкала оценивания	Неуд		Хорошо	Хорошо	Отлично
	не зачтено		зачтено		

Примерный перечень вопросов на экзамен:

1. Основные задачи инженерно-технической защиты информации. Факторы, влияющие на эффективность инженерно-технической защиты информации.
2. Базовые принципы инженерно-технической защиты информации (общие, специальные, дополнительные).
3. Объект информатизации (определение). Основные технические средства и системы (ОТСС). Вспомогательные технические средства и системы (ВТСС). Технический канал утечки информации (определение). Схема технического канала утечки информации
4. Показатели эффективности инженерно-технической защиты информации.
5. Основные направления инженерно-технической защиты информации (остановиться на информационном и энергетическом скрытии).
6. Демаскирующие признаки объекта (общая классификация, классификация по характеристикам объекта – видовые, сигнальные, вещество).
7. Демаскирующие признаки объекта (общая классификация, классификация по информативности и по времени проявления).
8. Источники и носители информации. Принципы записи и съема информации.
9. Источники сигналов (общая классификация, классификация основных и вспомогательных источников информации).
10. Источники сигналов (классификация по физической природе, акустоэлектронные преобразователи).
11. Источники сигналов (классификация по физической природе, излучатели низкочастотных и высокочастотных сигналов).
12. Источники сигналов (классификация по физической природе, паразитные связи и наводки).
13. Побочные электромагнитные излучения и наводки; структура, классификация и основные характеристики технических каналов утечки информации. Схема технического канала утечки информации, возникающего за счет побочных электромагнитных излучений
14. Классификация технической разведки (по физической природе носителя), основные этапы и процедуры добывания информации технической разведкой; возможности видов технической разведки.
15. Способы и средства добывания информации без физического проникновения в контролируемую зону.

16. Способы и средства наблюдения в оптическом диапазоне.
17. Способы и средства наблюдения в радиодиапазоне.
18. Скрытие речевой информации в каналах связи; энергетическое скрытие акустических информативных сигналов; обнаружение и локализация закладных устройств, подавление их сигналов; подавление опасных сигналов акустоэлектрических преобразователей.
19. Экранирование и компенсация информативных полей; подавление информативных сигналов в цепях заземления и электропитания; подавление опасных сигналов.
20. Классификация технических каналов утечки информации.
21. Общая классификация акустического технического канала утечки информации.
22. Воздушный акустический технический канал утечки информации. Микрофоны. Регистрирующие устройства.
23. Вибрационный акустический технический канал утечки информации.
24. Электроакустический и параметрический технические каналы утечки информации.
25. Линейные и энергетические характеристики акустического поля. Основные характеристики речи и речевого сигнала. Разборчивость речи.
26. Акустический технический канал утечки информации через «посредника». Специальные закладные устройства (общие вопросы и классификация по наличию управления, по использованию источника питания, по внешнему виду).
27. Акустический технический канал утечки информации через «посредника». Специальные закладные устройства (общие вопросы и классификация по каналу передачи информации и по способу восприятия информации).
28. Электрический технический канал утечки информации.
29. Электромагнитный и индукционный технические каналы утечки информации.
30. Каналы связи как технические каналы утечки информации.
31. Визуально-оптический технический канал утечки информации.
32. Принципы защиты информации в технических каналах утечки информации.
33. Способы защиты информации в акустическом техническом канале утечки.
34. Способы и средства защиты информации от специальных закладных устройств (общие вопросы).
35. Способы и средства защиты информации от специальных закладных устройств (методы выявления, индикаторы поля).
36. Способы и средства защиты информации от специальных закладных устройств (методы выявления, специальные приемники).
37. Способы и средства защиты информации от специальных закладных устройств (методы выявления, комплексы радиоконтроля).
38. Способы и средства защиты информации от специальных закладных устройств (методы выявления, нелинейные локаторы).
39. Методы и средства защиты информации в электромагнитном техническом канале утечки информации (общие вопросы).
40. Методы и средства защиты информации в электрическом канале утечки информации (контроль линий связи).
41. Технические средства защиты информации в электрическом техническом канале утечки информации (предотвращение использования эффекта акустоэлектронного преобразования и эффекта ВЧ-навязывания).
42. Методы защиты информации в телефонных каналах связи (исключая криптографию).
43. Методы защиты информации от несанкционированной аудиозаписи.
44. Криптографические методы защиты информации в каналах связи (характеристики речевых сигналов, аналоговое и цифровое преобразование).
45. Устройства защиты от утечки информации по радиоканалам, основные методы обнаружения радиозакладок.
46. Индикаторы поля, акустическая развязка, дифференциальный индикатор поля.
47. Генераторы шума.
48. Особенности работы и основные характеристики сканирующих радиоприемников.
49. Автоматизированные комплексы обнаружения радиозакладок. Методы обнаружения и локализации в пространстве закладных устройств.
50. Обнаружители и подавители диктофонов. Назначение. Принципы работы. Основные характеристики.
51. Принципы работы локаторов нелинейностей. Основные методы обнаружения ложных и истинных соединений

52. Схема технического канала утечки информации, возникающего за счет побочных электромагнитных наводок.
53. Схема перехвата речевой информации по акустовибрационному каналу утечки речевой информации. Основные характеристики и возможности электронных стетоскопов и радиостетоскопов.
54. Классификация пассивных и активных способов и средств защиты информации, обрабатываемой техническими средствами.
55. Основные требования к заземлению технических средств. Схемы заземлителей. Схемы заземления технических средств. Схемы измерения сопротивления заземления технических средств.
56. Основные требования к системе пространственного электромагнитного зашумления. Схема установки системы пространственного зашумления на объекте информатизации. Основные требования по установке системы пространственного зашумления на объекте информатизации. Основные характеристики генераторов шума.
57. Основные требования к системе электропитания технических средств. Способы защиты цепей электропитания технических средств от утечки информации, возникающей за счет побочных электромагнитных излучений.
58. Основные требования к помехоподавляющим фильтрам, используемым для защиты цепей электропитания технических средств. Основные характеристики фильтров нижних частот (ФНЧ). Схемы установки помехоподавляющих фильтров на объекте информатизации.
59. Классификация пассивных и активных способов и средств защиты выделенных помещений от утечки речевой информации по техническим каналам.
60. Средства звуко– и виброизоляции выделенных помещений. Экранирующие материалы, их основные характеристики. Экранированные помещения и экранированные камеры (классификация, состав, основные характеристики).
61. Порядок проведения контроля эффективности защиты СВТ от утечки информации, возникающей за счет ПЭМИН.
62. Методы обнаружения, идентификации РЗ и определения их местоположения.
63. Порядок организации защиты информации на объектах информатизации.
64. Предварительное специальное обследование объекта информатизации.
65. Лицензирование деятельности по технической защите информации. Сертификация технических средств защиты информации.
66. Порядок организации защиты информации от утечек по техническим каналам на объектах информатизации и в выделенных помещениях на различных этапах жизненного цикла объекта защиты.
67. Порядок ввода объекта информатизации и системы технической защиты информации в эксплуатацию.
68. Порядок организации и проведения аттестации объекта информатизации по требованиям безопасности информации.
69. Организация аттестации объекта информатизации по требованиям безопасности информации. Перечень документов, представляемых Заявителем для проведения аттестации объекта информатизации.
70. Порядок проведения аттестации объекта информатизации по требованиям безопасности информации.

Примерный перечень тестовых заданий на экзамен:

Согласно «Оранжевой книге» дискреционную защиту имеет группа критериев

D
A
B
C

При качественном подходе риск измеряется в терминах

денежных потерь
заданных с помощью шкалы или ранжирования
оценок экспертов
объема информации

При полномочной политике безопасности совокупность меток с одинаковыми

значениями образует

область равной критичности
область равного доступа
уровень безопасности
уровень доступности

Согласно «Европейским критериям» формальное описание функций безопасности требуется на уровне

E5
E7
E4
E6

Степень защищенности информации от негативного воздействия на неё с точки зрения нарушения её физической и логической целостности или несанкционированного использования — это

уязвимость информации
надежность информации
защищенность информации
базопасность информации

Проверка подлинности субъекта по предъявленному им идентификатору для принятия решения о предоставлении ему доступа к ресурсам системы — это

аудит
аутентификация
авторизация
идентификация

5.2.3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций

1. Текущий контроль успеваемости обучающихся, осуществляется в следующем порядке: в конце завершения освоения соответствующей темы обучающиеся, по распоряжению педагогического работника, убирают все личные вещи, электронные средства связи и печатные источники информации.

Для подготовки ответов на вопросы обучающиеся используют чистый лист бумаги любого размера и ручку. На листе бумаги обучающиеся указывают свои фамилию, имя, отчество (при наличии), номер учебной группы и дату проведения текущего контроля успеваемости.

Научно-педагогический работник устно задает два вопроса, которые обучающийся может записать на подготовленный для ответа лист бумаги.

В течение установленного научно-педагогическим работником времени обучающиеся письменно формулируют ответы на заданные вопросы. По истечении указанного времени листы бумаги с подготовленными ответами обучающиеся передают научно-педагогическому работнику для последующего оценивания результатов текущего контроля успеваемости.

При подготовке ответов на вопросы обучающимся запрещается использование любых электронных и печатных источников информации. В случае обнаружения научно-педагогическим работником факта использования обучающимся при подготовке ответов на вопросы указанные источники информации – оценка результатов текущего контроля соответствует 0 баллов и назначается дата повторного прохождения текущего контроля успеваемости.

Текущий контроль успеваемости обучающихся по результатам выполнения лабораторных и (или) практических работ осуществляется в форме отчета, который предоставляется научно-педагогическому работнику на бумажном и (или) электронном носителе. Научно-педагогический работник, после проведения оценочных процедур, имеет право вернуть обучающемуся отчет для последующей корректировки с указанием перечня несоответствий. Обучающийся обязан устранить все указанные несоответствия и направить отчет научно-педагогическому работнику в срок, не

превышающий трех учебных дней, следующих за днем проведения текущего контроля успеваемости.

Результаты текущего контроля доводятся до сведения обучающихся в течение трех учебных дней, следующих за днем проведения текущего контроля успеваемости.

Обучающиеся, которые не прошли текущий контроль успеваемости в установленные сроки, обязаны пройти его в срок до начала процедуры промежуточной аттестации по дисциплине в соответствии с расписанием промежуточной аттестации.

Результаты прохождения процедур текущего контроля успеваемости обучающихся учитываются при оценивании результатов промежуточной аттестации обучающихся.

1. Промежуточная аттестация обучающихся проводится после завершения обучения по дисциплине в семестре в соответствии с календарным учебным графиком и расписанием промежуточной аттестации.

Для успешного прохождения процедуры промежуточной аттестации по дисциплине обучающиеся должны:

1. получить положительные результаты по всем предусмотренным рабочей программой формам текущего контроля успеваемости;
2. получить положительные результаты аттестационного испытания.

Для успешного прохождения аттестационного испытания обучающийся в течение времени, установленного научно-педагогическим работником, осуществляет подготовку ответов на два вопроса, выбранных в случайном порядке.

Для подготовки ответов используется чистый лист бумаги и ручка.

На листе бумаги обучающиеся указывают свои фамилию, имя, отчество (при наличии), номер учебной группы и дату проведения аттестационного испытания.

При подготовке ответов на вопросы обучающимся запрещается использование любых электронных и печатных источников информации.

По истечении указанного времени, листы с подготовленными ответам на вопросы обучающиеся передают научно-педагогическому работнику для последующего оценивания результатов промежуточной аттестации.

В случае обнаружения научно-педагогическим работником факта использования обучающимся при подготовке ответов на вопросы указанные источники информации – оценка результатов промежуточной аттестации соответствует 0 баллов и назначается дата повторного прохождения аттестационного испытания.

Результаты промежуточной аттестации обучающихся размещаются в ЭИОС КузГТУ.

Текущий контроль успеваемости и промежуточная аттестация обучающихся могут быть организованы с использованием ЭИОС КузГТУ, порядок и формы проведения текущего контроля успеваемости и промежуточной аттестации обучающихся при этом не меняется.

6 Учебно-методическое обеспечение

6.1 Основная литература

1. Исаева, М. Ф. Техническая защита информации : учебное пособие / М. Ф. Исаева. — Санкт-Петербург : ПГУПС, 2017. — 49 с. — ISBN 978-5-7641-1008-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/101600 (дата обращения: 23.03.2026). — Режим доступа: для авториз. пользователей.

2. Скрипник, Д. А. Общие вопросы технической защиты информации : учебное пособие / Д. А. Скрипник. – 2-е изд., испр. – Москва : Национальный Открытый Университет «ИНТУИТ», 2016. – 425 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=429070 (дата обращения: 16.04.2026). – Библиогр. в кн. – Текст : электронный.

3. Прокопенко, Е. В. Техническая защита информации : учебное пособие для студентов специальности 10.05.03 "Информационная безопасность автоматизированных систем" / Е. В. Прокопенко, В. О. Коротин ; Кузбасский государственный технический университет им. Т. Ф. Горбачева. – Кемерово : КузГТУ, 2024. – 1 файл (1,67 Мб). – URL: http://library.kuzstu.ru/meto.php?n=91990&type=utchposob:common (дата обращения: 23.03.2026). – Текст : электронный.

6.2 Дополнительная литература

1. Титов, А. А. Инженерно-техническая защита информации : учебное пособие / А. А. Титов. — Москва : ТУСУР, 2010. — 197 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/4959 (дата обращения: 23.03.2026). — Режим доступа: для авториз. пользователей.

2. Данилов, А. Н. Инженерно-техническая защита информации : учебное пособие / А. Н. Данилов, А. Л. Лобков. — Пермь : ПНИПУ, 2007. — 340 с. — ISBN 978-5-88151-821-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/160366 (дата обращения: 23.03.2026). — Режим доступа: для авториз. пользователей.

3. Рагозин, Ю. Н. Инженерно-техническая защита информации : учебное пособие : [16+] / Ю. Н. Рагозин. – Санкт-Петербург : Интермедия, 2018. – 168 с. : схем., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=481159 (дата обращения: 12.04.2026). – Библиогр. в кн. – ISBN 978-5-4383-0161-5. – Текст : электронный.

6.3 Методическая литература

1. Техническая защита информации : методические материалы для обучающихся специальности 10.05.03 "Информационная безопасность автоматизированных систем" очной формы обучения / ФГБОУ ВО "Кузбас. гос. техн. ун-т им. Т. Ф. Горбачева", Каф. информ. безопасности ; сост.: Е. В. Прокопенко, И. В. Чичерин. – Кемерово : КузГТУ, 2018. – 36 с. – URL: http://library.kuzstu.ru/meto.php?n=4639 (дата обращения: 23.03.2026). – Текст : электронный.

6.4 Профессиональные базы данных и информационные справочные системы

1. Универсальная полнотекстовая база данных электронных периодических изданий «ИВИС» https://eivis.ru/
2. Электронная библиотечная система «Университетская библиотека онлайн» http://biblioclub.ru/
3. Электронная библиотечная система «Лань» http://e.lanbook.com
4. Электронная библиотека КузГТУ https://library.kuzstu.ru/index.php/punkt-2/podrazdel-21
5. Электронная библиотека Новосибирского государственного технического университета https://clck.ru/UoXpv
6. Образовательная платформа «Юрайт» https://urait.ru/
7. Электронная библиотечная система «Znanium» https://new.znanium.com/my/documents
8. Справочная правовая система «КонсультантПлюс» http://www.consultant.ru/
9. Электронная библиотека "Эксперт" Системы Технорматив https://gost.online/index.htm
10. Национальная электронная библиотека https://rusneb.ru/

6.5 Периодические издания

1. Безопасность информационных технологий: научный журнал https://eivis.ru/browse/publication/379646
2. Вестник Кузбасского государственного технического университета : научно-технический журнал https://vestnik.kuzstu.ru/
3. Защита информации. Инсайд: информационно-методический журнал https://eivis.ru/browse/publication/122426
4. Информация и безопасность : научный журнал

7 Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

ЭИОС КузГТУ:

a) Электронная библиотека КузГТУ. – Текст: электронный // Научно-техническая библиотека Кузбасского государственного технического университета им. Т. Ф. Горбачева : сайт. – Кемерово, 2001 – . – URL: https://elib.kuzstu.ru/. – Текст: электронный.

b) Портал.КузГТУ : Автоматизированная Информационная Система (АИС) : [сайт] / Кузбасский государственный технический университет им. Т. Ф. Горбачева. – Кемерово : КузГТУ, [б. г.]. – URL: https://portal.kuzstu.ru/. – Режим доступа: для авториз. пользователей. – Текст: электронный.

c) Электронное обучение : [сайт] / Кузбасский государственный технический университет им. Т. Ф. Горбачева. – Кемерово : КузГТУ, [б. г.]. – URL: https://el.kuzstu.ru/. – Режим доступа: для авториз. пользователей КузГТУ. – Текст: электронный.


1774206182

8 Методические указания для обучающихся по освоению дисциплины "Техническая защита информации"

Самостоятельная работа обучающегося является частью его учебной деятельности, объемы самостоятельной работы по каждой дисциплине (модулю) практике, государственной итоговой аттестации, устанавливаются в учебном плане.

Самостоятельная работа по дисциплине (модулю), практике организуется следующим образом:

1. До начала освоения дисциплины обучающемуся необходимо ознакомиться с содержанием рабочей программы дисциплины (модуля), программы практики в следующем порядке:

1.1 содержание знаний, умений, навыков и (или) опыта профессиональной деятельности, которые будут сформированы в процессе освоения дисциплины (модуля), практики;

1.2 содержание конспектов лекций, размещенных в электронной информационной среде КузГТУ в порядке освоения дисциплины, указанном в рабочей программе дисциплины (модуля), практики;

1.3 содержание основной и дополнительной литературы.

2. В период освоения дисциплины обучающийся осуществляет самостоятельную работу в следующем порядке:

2.1 выполнение практических и (или) лабораторных работы и (или) отчетов в порядке, установленном в рабочей программе дисциплины (модуля), практики;

2.2 подготовка к опросам и (или) тестированию в соответствии с порядком, установленном в рабочей программе дисциплины (модуля), практики;

2.3 подготовка к промежуточной аттестации в соответствии с порядком, установленном в рабочей программе дисциплины (модуля), практики.

В случае затруднений, возникших при выполнении самостоятельной работы, обучающемуся необходимо обратиться за консультацией к педагогическому работнику. Периоды проведения консультаций устанавливаются в расписании консультаций.

9 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине "Техническая защита информации", включая перечень программного обеспечения и информационных справочных систем

Для изучения дисциплины может использоваться следующее программное обеспечение:

1. Mozilla Firefox
2. Google Chrome
3. 7-zip
4. Microsoft Windows
5. ESET NOD32 Smart Security Business Edition
6. Kaspersky Endpoint Security
7. Браузер Спутник

10 Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине "Техническая защита информации"

Для реализации программы учебной дисциплины предусмотрены специальные помещения:

1. Помещения для самостоятельной работы обучающихся должны оснащенные компьютерной техникой с возможностью подключения к сети Интернет и обеспечением доступа к электронной информационно-образовательной среде Организации.

2. Учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

11 Иные сведения и (или) материалы

1. Образовательный процесс осуществляется с использованием как традиционных так и современных интерактивных технологий.

В рамках аудиторных занятий применяются следующие интерактивные методы:

- разбор конкретных примеров;
- мультимедийная презентация.

2. Проведение групповых и индивидуальных консультаций осуществляется в соответствии с

расписанием консультаций по темам, заявленным в рабочей программе дисциплины, в период освоения дисциплины и перед промежуточной аттестацией с учетом результатов текущего контроля.