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

Технические средства охраны объектов информатизации

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 "Технические средства охраны объектов информатизации", соотнесенных с планируемыми результатами освоения образовательной программы

Освоение дисциплины направлено на формирование:

общепрофессиональных компетенций:

ОПК-14 - Способен осуществлять разработку, внедрение и эксплуатацию автоматизированных систем с учетом требований по защите информации, проводить подготовку исходных данных для технико-экономического обоснования проектных решений;

Результаты обучения по дисциплине определяются индикаторами достижения компетенций

Индикатор(ы) достижения:

Эксплуатирует системы контроля и управления доступом и технические средства охраны объектов информатизации.

Результаты обучения по дисциплине:

методы и технические средства охраны объектов, СКУД и основные подходы к созданию таких средств.

разрабатывать меры защиты от выявленных угроз информационной безопасности, выбирать и устанавливать технические средства охраны объектов, СКУД и оценивать их эффективность.

навыками внедрения и эксплуатации современных технических и программных средств охраны объектов информатизации и

- СКУД.

2 Место дисциплины "Технические средства охраны объектов информатизации" в структуре ОПОП специалитета

Для освоения дисциплины необходимы знания умения, навыки и (или) опыт профессиональной деятельности, полученные в рамках изучения следующих дисциплин: Методы и средства защиты информационных систем.

В области 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 "Технические средства охраны объектов информатизации" 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 "Технические средства охраны объектов информатизации" 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			
Лекции			
Лабораторные занятия	32		
Практические занятия	16		
Внеаудиторная работа			
Индивидуальная работа с преподавателем:			
Консультация и иные виды учебной деятельности			
Самостоятельная работа под руководством преподавателя	64		
Самостоятельная работа	68		

Форма обучения	Количество часов		
	ОФ	ЗФ	ОЗФ
Форма промежуточной аттестации	экзамен /36		

4 Содержание дисциплины "Технические средства охраны объектов информатизации", структурированное по разделам (темам)

4.1. Практические (семинарские) занятия

Тема занятия	Трудоемкость в часах
	ОФ
Раздел 1. Правовое и нормативное обеспечение систем контроля и управления доступом	
Обоснование необходимости создания технических средств охраны объекта информатизации на основе нормативных и методических документов.	2
Раздел 2. Материально-вещественный технический канал утечки информации.	
Угрозы физической безопасности объекта информатизации	2
Модели нарушителей физической безопасности объекта информатизаци	4
Раздел 3. Методы и средства построения технических систем охраны объектов информатизации.	
Разработка топологии многозональной и многорубежной системы физической защиты объекта	4
Разработка структурной и функциональной схем технических средств охраны объектов информатизации	4
Раздел 4. Организационные основы создания и эксплуатации систем контроля и управления доступом	
Моделирование угроз физической безопасности объекта информатизации	4
Разработка основных организационных документов службы режима предприятия	4
Разработка инструкций по эксплуатации технических средств охраны объектов информатизации.	4
Раздел 5. Методы и средства контроля эффективности технических средств охраны объектов информатизации	
Разработка методик контроля эффективности технических средств охраны объектов информатизации. Расчётные методики контроля эффективности технических средств охраны объектов информатизации.	4
Итого	**32**

4.2 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	22
Оформление отчетов по практическим и(или) лабораторным работам	20
Подготовка к промежуточной аттестации	6
Итого	**48**
Самостоятельная работа под руководством преподавателя	64

5 Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине "Технические средства охраны объектов информатизации"

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-14	Эксплуатирует системы контроля и управления доступом и технические средства охраны объектов информатизации.	Знать методы и технические средства охраны объектов информатизации, СКУД и основные подходы к созданию таких средств. Уметь разрабатывать меры защиты от выявленных угроз информационной безопасности, выбирать и устанавливать технические средства охраны объектов информатизации, СКУД и оценивать их эффективность. Владеть навыками внедрения и эксплуатации современных технических и программных средств охраны объектов информатизации и СКУД.	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 тестирование по разделу дисциплины, оформлении оформлении отчетов по практическим и(или) лабораторным работам.

Тестирование по разделу дисциплины

Обучающийся отвечает на 10 тестовых заданий.

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 тестовых заданий:

ОПК-14

1. Эксплуатационная документация на ТСФЗ должна быть оформлена в соответствии с ГОСТ: (выбрать все верные)

2.601

2.610.

2.602.

2. Укажите эксплуатационные параметры, которые важны для оборудования, работающего как внутри, так и вне помещений (выбрать все верные)

рабочий диапазон температур от -50 °С до +30 °С;

относительная влажность воздуха 98% при температуре +25 °С;

наличие атмосферных конденсируемых осадков (иней, роса);

статическая и динамическая пыль;

солнечное излучение.

световое излучение

3. Для эксплуатации инженерно-технических средств физической защиты должны разрабатываться:

план-график выполнения регламентных работ по техническому обслуживанию на очередной год;

план материально-технического обеспечения комплекса инженерно-технических средств физической защиты на очередной год;

план проверки работоспособности и технического состояния инженерно-технических средств физической защиты.

правила экстренного внепланового ремонта

4. Основными источниками информации материально-вещественного канала утечки информации являются: (выбрать все верные)

черновики документов

неисправные физические носители информации

химические отходы

бракованная продукция или отдельные ее элементы

аудиозапись, полученная нелегальным путем

видеозапись, сделанная скрытой камерой

5. Перенос информации в материально-вещественном канале за пределы контролируемой зоны

возможен: (выбрать все верные)
сотрудниками организации;
воздушными массами атмосферы;
жидкой средой;
излучениями радиоактивных веществ
магнитными и электромагнитными полями

6. Выберите все верные способы получения информации с использованием материально-вещественных каналов:
физико-химический анализ
биологический анализ
математический анализ
технический анализ
компьютерный / программный анализ

7. Что может входить в состав системы обнаружения, контроля и управления доступом (выбрать все верные)
видеосистема с датчиком движения
видеосистема без датчика движения
металлоискатели
детекторы запрещенных веществ
газоанализаторы
акустические датчики
вибрационные и сейсмо-датчики
объемные датчики
датчики освещенности
оптические датчики

8. Какие системы обнаружения могут использоваться для охраны периметра на улице (выбрать все верные)
детекторы на ИК-лучах
радиолучевые детекторы
радиоволновые (проводно-волновые)
емкостные
магнитометрические системы
сейсмические
обрывные
виброчувствительные
волоконно-оптические
лучевые
видеосистема с датчиком движения
видеосистема без датчика движения

9. Совместно с какой системой как минимум должно происходить срабатывание системы воздействия в инженерно-техническом комплексе защиты:
исполнительными механизмами СКУД (замки, решетки, запорные устройства)
системой видеонаблюдения
системой внутреннего и внешнего оповещения
системой сбора и обработки информации (ССОИ)

10. Система физической защиты (СФЗ) предприятия включает: (выбрать все верные)
организационные мероприятия;
инженерно-технические средства;
действия подразделений охраны.
действия сотрудников предприятия

11. Что включает в себя системный подход в вопросах защиты информации техническими средствами (выбрать все верные)

изучение объекта для внедряемой системы защиты;
оценку угроз безопасности объекта;
анализ средств, которые будут использоваться при построении системы защиты;
оценку экономической целесообразности внедрения системы защиты;
изучение самой системы, ее свойств, принципов работы
организационные аспекты объекта защиты и использования средств защиты
экологические аспекты объекта защиты и использования средств защиты
социальные аспекты объекта защиты и использования средств защиты

12. Принципы построения эффективной системы контроля и управления доступом (выбрать все верные)
обнаружение нарушителя на максимальном удалении от цели
оценка попытки проникновения со стороны нарушителя до завершения его обнаружения
устойчивая связь между обнаружением нарушителя и реагированием на него
задержка на максимально приемлемом удалении от цели
непрерывное наблюдение за нарушителем, проникнувшего в периметр охраняемого объекта

13. Система сбора, обработки, отображения и документирования информации от систем контроля и управления доступом может выполнять: (выбрать все верные)
управление телевизионными передающими камерами и микрофонами
контроль работоспособности средств обнаружения
выдачу сведений о характере неисправности нерабочего оборудования
автоматический вызов технического персонала для ремонта неисправного оборудования
размер ущерба, причиненного ложным срабатыванием охранного оборудования
размер ущерба, причиненного совершенного злоумышленниками

14. Какие каналы связи могут использоваться для передачи и сбора информации от систем контроля и управления доступом? : (выбрать все верные)
совмещение с компьютерной сетью на основе витой пары
выделенная сеть на основе витой пары или телефонного кабеля
сеть wi-fi
совмещение с телефонной сетью
совмещение с питающей электросетью
спутниковая связь
ИК, Bluetooth - связь

15. Средства сбора и обработки информации от средств обнаружения, средств связи и тревожно-вызывной сигнализации (ССОИ) предназначены для обработки поступающей информации с целью: (выбрать все верные)
последующего ее преобразования в вид, удобный для восприятия и анализа оператором
выдачи управляющих сигналов различного назначения
выдачи автоматически формируемого заключения о пробелах существующей системы безопасности и рекомендаций по их устранению
формирования управленческих решений для руководителя службы безопасности

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:

о пройденное тестирование.
зачтенные отчеты обучающихся по лабораторным и(или) практическим работам;

На экзамене обучающийся отвечает 20 тестовых заданий

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 тестовых заданий на экзамен:

ОПК-14

1. Эксплуатационная документация на ТСФЗ должна быть оформлена в соответствии с ГОСТ: (выбрать все верные)

2.601
2.610.
2.602.

2. Укажите эксплуатационные параметры, которые важны для оборудования, работающего как внутри, так и вне помещений (выбрать все верные)

рабочий диапазон температур от -50 °С до +30 °С;
относительная влажность воздуха 98% при температуре +25 °С;
наличие атмосферных конденсируемых осадков (иней, роса);
статическая и динамическая пыль;
солнечное излучение.
световое излучение

3. Для эксплуатации инженерно-технических средств физической защиты должны разрабатываться:

план-график выполнения регламентных работ по техническому обслуживанию на очередной год;
план материально-технического обеспечения комплекса инженерно-технических средств физической защиты на очередной год;
план проверки работоспособности и технического состояния инженерно-технических средств физической защиты.
правила экстренного внепланового ремонта

4. Основными источниками информации материально-вещественного канала утечки информации являются: (выбрать все верные)

черновики документов
неисправные физические носители информации
химические отходы
бракованная продукция или отдельные ее элементы

аудиозапись, полученная нелегальным путем
видеозапись, сделанная скрытой камерой

5. Перенос информации в материально-вещественном канале за пределы контролируемой зоны возможен: (выбрать все верные)
сотрудниками организации;
воздушными массами атмосферы;
жидкой средой;
излучениями радиоактивных веществ
магнитными и электромагнитными полями

6. Выберите все верные способы получения информации с использованием материально-вещественных каналов:
физико-химический анализ
биологический анализ
математический анализ
технический анализ
компьютерный / программный анализ

7. Что может входить в состав системы обнаружения, контроля и управления доступом (выбрать все верные)
видеосистема с датчиком движения
видеосистема без датчика движения
металлоискатели
детекторы запрещенных веществ
газоанализаторы
акустические датчики
вибрационные и сейсмо-датчики
объемные датчики
датчики освещенности
оптические датчики

8. Какие системы обнаружения могут использоваться для охраны периметра на улице (выбрать все верные)
детекторы на ИК-лучах
радиолучевые детекторы
радиоволновые (проводно-волновые)
емкостные
магнитометрические системы
сейсмические
обрывные
виброчувствительные
волоконно-оптические
лучевые
видеосистема с датчиком движения
видеосистема без датчика движения

9. Совместно с какой системой как минимум должно происходить срабатывание системы воздействия в инженерно-техническом комплексе защиты:
исполнительными механизмами СКУД (замки, решетки, запорные устройства)
системой видеонаблюдения
системой внутреннего и внешнего оповещения
системой сбора и обработки информации (ССОИ)

10. Система физической защиты (СФЗ) предприятия включает: (выбрать все верные)
организационные мероприятия;
инженерно-технические средства;
действия подразделений охраны.


1776294274

действия сотрудников предприятия

11. Что включает в себя системный подход в вопросах защиты информации техническими средствами (выбрать все верные)
изучение объекта для внедряемой системы защиты;
оценку угроз безопасности объекта;
анализ средств, которые будут использоваться при построении системы защиты;
оценку экономической целесообразности внедрения системы защиты;
изучение самой системы, ее свойств, принципов работы
организационные аспекты объекта защиты и использования средств защиты
экологические аспекты объекта защиты и использования средств защиты
социальные аспекты объекта защиты и использования средств защиты

12. Принципы построения эффективной контроля и управления доступом (выбрать все верные)
обнаружение нарушителя на максимальном удалении от цели
оценка попытки проникновения со стороны нарушителя до завершения его обнаружения
устойчивая связь между обнаружением нарушителя и реагированием на него
задержка на максимально приемлемом удалении от цели
непрерывное наблюдение за нарушителем, проникнувшего в периметр охраняемого объекта

13. Система сбора, обработки, отображения и документирования информации от систем контроля и управления доступом может выполнять: (выбрать все верные)
управление телевизионными передающими камерами и микрофонами
контроль работоспособности средств обнаружения
выдачу сведений о характере неисправности нерабочего оборудования
автоматический вызов технического персонала для ремонта неисправного оборудования
размер ущерба, причиненного ложным срабатыванием охранного оборудования
размер ущерба, причиненного совершенного злоумышленниками

14. Какие каналы связи могут использоваться для передачи и сбора информации от систем контроля и управления доступом? : (выбрать все верные)
совмещение с компьютерной сетью на основе витой пары
выделенная сеть на основе витой пары или телефонного кабеля
сеть wi-fi
совмещение с телефонной сетью
совмещение с питающей электросетью
спутниковая связь
ИК, Bluetooth - связь

15. Средства сбора и обработки информации от средств обнаружения, средств связи и тревожно-вызывной сигнализации (ССОИ) предназначены для обработки поступающей информации с целью: (выбрать все верные)
последующего ее преобразования в вид, удобный для восприятия и анализа оператором
выдачи управляющих сигналов различного назначения
выдачи автоматически формируемого заключения о пробелах существующей системы безопасности и рекомендаций по их устранению
формирования управленческих решений для руководителя службы безопасности

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. Полшков, А. В. Технические средства охраны : учебное пособие / А. В. Полшков, А. С. Шабуров. — Пермь : ПНИПУ, 2013. — 249 с. — ISBN 978-5-398-01067-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/160595 (дата обращения: 23.03.2026). — Режим доступа: для авториз. пользователей.

2. Поликанин, А. Н. Технические средства охраны и видеонаблюдения. Системы видеонаблюдения и тепловизионного контроля : учебное пособие / А. Н. Поликанин. — Новосибирск : СГУГиТ, 2021. — 46 с. — ISBN 978-5-907320-92-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/222380 (дата обращения: 23.03.2026). — Режим доступа: для авториз. пользователей.

6.2 Дополнительная литература

1. Гриненко, В. А. Физическая защита радиационно-опасных объектов. Инженерно-технические средства охраны : монография / В. А. Гриненко, А. И. Коростелев. — Москва : НИЯУ МИФИ, 2014. — 252 с. — ISBN 978-5-7262-2040-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/103216 (дата обращения: 23.03.2026). — Режим доступа: для авториз. пользователей.

2. Кожомбердиева, Г. И. Криптографическая защита информации и управление доступом на платформе Java : учебно-методическое пособие / Г. И. Кожомбердиева, М. Л. Глухарев. — Санкт-Петербург : ПГУПС, 2016. — 87 с. — ISBN 978-5-7641-0856-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/91082 (дата обращения: 23.03.2026). — Режим доступа: для авториз. пользователей.

3. Девянин, П. Н. Модели безопасности компьютерных систем : управление доступом и информационными потоками : учебное пособие / П. Н. Девянин. – Москва : Горячая линия – Телеком, 2012. – 320 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=253178 (дата обращения: 11.04.2026). – ISBN 978-5-9912-0147-6. – Текст : электронный.

4. Девянин, П. Н. Модели безопасности компьютерных систем : управление доступом и информационными потоками : учебное пособие / П. Н. Девянин. – 2-е изд., испр. и доп. – Москва : Горячая линия – Телеком, 2013. – 338 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=275208 (дата обращения: 11.04.2026). – Библиогр. в кн. – ISBN 978-5-9912-0328-9. – Текст : электронный.

6.3 Методическая литература

1. Методические рекомендации по организации учебной деятельности обучающихся КузГТУ / ФГБОУ ВО «Кузбас. гос. техн. ун-т им. Т. Ф. Горбачева», Каф. приклад. информ. технологий ; сост. Л. И. Михалева. – Кемерово : КузГТУ, 2017. – 32 с. – URL: http://library.kuzstu.ru/meto.php?n=553 (дата обращения: 23.03.2026). – Текст : электронный.

6.4 Профессиональные базы данных и информационные справочные системы

1. Электронная библиотечная система «Университетская библиотека онлайн» http://biblioclub.ru/
2. Электронная библиотечная система «Лань» http://e.lanbook.com
3. Электронная библиотека КузГТУ https://library.kuzstu.ru/index.php/punkt-2/podrazdel-21
4. Образовательная платформа «Юрайт» https://urait.ru/
5. Справочная правовая система «КонсультантПлюс» http://www.consultant.ru/
6. Электронная библиотека "Эксперт" Системы Технорматив https://gost.online/index.htm
7. Национальная электронная библиотека https://rusneb.ru/
8. Базы данных Springer Journals, Springer eBooks https://link.springer.com/

6.5 Периодические издания

1. Безопасность информационных технологий: научный журнал

https://eivis.ru/browse/publication/379646

2. Защита информации. Инсайд: информационно-методический журнал https://eivis.ru/browse/publication/122426

3. Информационные ресурсы России : научно-практический журнал https://eivis.ru/browse/publication/114926

4. Информационные системы и технологии : научно-технический журнал https://eivis.ru/browse/publication/542286

5. Информационные технологии (с приложением) : теоретический и прикладной научно-технический журнал

6. Информационные технологии и вычислительные системы : журнал https://elibrary.ru/contents.asp?titleid=8746

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.

8 Методические указания для обучающихся по освоению дисциплины "Технические средства охраны объектов информатизации"

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 "Технические средства охраны объектов информатизации", 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

10 Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине "Технические средства охраны объектов информатизации"

Для реализации программы учебной дисциплины предусмотрены специальные помещения:

1. Специальное помещение № 1406 представляет собой учебную аудиторию для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Перечень основного оборудования:

Комплект мебели (столы и стулья). Проектор. Персональный компьютер.

Перечень программного обеспечения: Libre Office. Mozilla Firefox. Google Chrome. 7-zip .Microsoft Windows. ESET NOD32 Smart Security Business Edition. Kaspersky Endpoint Security. Браузер Спутник.

2. Специальное помещение № 1435 представляет собой учебную аудиторию для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Перечень основного оборудования:

Комплект мебели (столы и стулья). Проектор. Персональные компьютеры.

Перечень программного обеспечения: Libre Office. Mozilla Firefox. Google Chrome. 7-zip .Microsoft Windows. ESET NOD32 Smart Security Business Edition. Kaspersky Endpoint Security. Браузер Спутник.

3. Помещение для самостоятельной работы обучающихся:

Специальное помещение № 1237 представляет собой помещения для самостоятельной работы, оснащенные компьютерной техникой с возможностью подключения к информационно-телекоммуникационной сети Интернет и обеспечением доступа в электронную информационно-образовательную среду образовательной организации:

Перечень основного оборудования:

Комплект мебели (столы и стулья). Персональные компьютеры. Коммутатор AlliedTelesynLayer 2 SmartSwitch,

Перечень программного обеспечения: LibreOffice. MozillaFirefox. Google Chrome. 7-zip .Microsoft Windows. ESET NOD32 Smart Security Business Edition. Kaspersky Endpoint Security. БраузерСпутник.

4. Помещение для самостоятельной работы обучающихся:

Специальное помещение № 1211 представляет собой помещения для самостоятельной работы, оснащенные компьютерной техникой с возможностью подключения к информационно-телекоммуникационной сети Интернет и обеспечением доступа в электронную информационно-образовательную среду образовательной организации:

Перечень основного оборудования:

Специализированная мебель (столы и стулья); компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду КузГТУ, в том числе:

проектор, экран настенный моторизованный.

Перечень программного обеспечения: LibreOffice. Mozilla Firefox. Google Chrome. 7-zip .Microsoft Windows. ESET NOD32 Smart Security Business Edition. Kaspersky Endpoint Security. БраузерСпутник.

5. Лаборатория №1251 представляет собой лабораторию в области программно-аппаратных средств защиты информации, оснащенную антивирусными программными комплексами, аппаратными средствами аутентификации пользователя, средствами анализа защищенности компьютерных сетей, устройствами чтения смарт-карт и радиометок, программно-аппаратными комплексами защиты информации, включающими в том числе средства криптографической защиты информации;

Перечень основного оборудования:

Комплект мебели (столы и стулья). Проектор. Персональные компьютеры.

Перечень программного обеспечения: Libre Office. Mozilla Firefox. Google Chrome. 7-zip .Microsoft Windows. ESET NOD32 Smart Security Business Edition. Kaspersky Endpoint Security. Браузер Спутник.

6. Специально оборудованный кабинет №1147 представляет собой компьютерный класс для научно-исследовательской работы обучающихся, курсового и дипломного проектирования, оснащенный рабочими местами на базе вычислительной техники с набором необходимых для проведения и

оформления результатов исследований дополнительных аппаратных и (или) программных средств, а также комплектом оборудования для печати

Перечень основного оборудования:

Специализированная мебель (столы и стулья); Коммутаторы, Металлические рольставни с пружинным механизмом, белые 1650мм*2270мм; Сейф металлический; Системные блоки ITS (i3-10100/H410M/8 Gb/SSD 240Gb/БП AA500W); Точка доступа D-link; Мониторы 23.6" AOC 24B1H VA 1920x1080 (16:9), 250кд/м2, 5мс, VGA, HDMI, черные; Системные блокиMasteroMiddleMC05, IntelCorei510400 2.9GHz, 8GbRAM, 240GbSSD, DOS, программно-аппаратный комплекс для обнаружения компьютерных атак VipNet, средство доверенной загрузки (СДЗ) Соболь.

7. Специально оборудованный кабинет № 1019 представляет собой аудиторию – специальную библиотеку (библиотеку литературы ограниченного доступа), предназначенную для хранения и обеспечения использования в образовательном процессе нормативных и методических документов ограниченного доступа.

Перечень основного оборудования:

Специализированная мебель (столы и стулья).

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.