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

Проектирование систем защиты 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 "Проектирование систем защиты информации", соотнесенных с планируемыми результатами освоения образовательной программы

Освоение дисциплины направлено на формирование:

профессиональных компетенций:

ПК-13 - Способен разрабатывать отчетные документы и разделы технических заданий на создание систем защиты информации автоматизированных систем

ПК-14 - Способен разрабатывать системы защиты информации автоматизированных систем с учетом действующих нормативно-правовых документов

Результаты обучения по дисциплине определяются индикаторами достижения компетенций

Индикатор(ы) достижения:

Разрабатывает отчетную документацию и разделы технических заданий.

Разрабатывает системы защиты информации автоматизированных систем с учетом действующих нормативно-правовых документов

Результаты обучения по дисциплине:

Знать руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации.

Знать особенности проектирования подсистем информационной безопасности.

Уметь использовать методические документы уполномоченных федеральных органов исполнительной власти по защите информации.

Уметь разрабатывать проекты нормативных документов, регламентирующих работу по защите информации в автоматизированных системах.

Владеть документацией по защите информации.

Владеть методологиями построения систем защиты информации.

2 Место дисциплины "Проектирование систем защиты информации" в структуре ОПОП специалитета

Для освоения дисциплины необходимы знания умения, навыки и (или) опыт профессиональной деятельности, полученные в рамках изучения следующих дисциплин: Безопасность систем баз данных, Организационное и правовое обеспечение информационной безопасности, Основы информационной безопасности, Управление информационной безопасностью, Методы и средства криптографической защиты информации, Программно-аппаратные средства защиты информации, Нормативные требования по защите информации, Информационные угрозы, Классификация защищаемой информации и информационных систем, Методы и средства защиты информационных систем, Методы обнаружения угроз безопасности информационных систем, Компьютерное моделирование 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 "Проектирование систем защиты 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 "Проектирование систем защиты информации" составляет 7 зачетных единиц, 252 часа.

Форма обучения	Количество часов		
	ОФ	ЗФ	ОЗФ
Курс 5/Семестр 9			
Всего часов	252		
Контактная работа обучающихся с преподавателем (по видам учебных занятий):			
Аудиторная работа			

Форма обучения	Количество часов		
	ОФ	ЗФ	ОЗФ
Лекции	16		
Лабораторные занятия			
Практические занятия	48		
Внеаудиторная работа			
Индивидуальная работа с преподавателем:			
Курсовая работа	2		
Консультация и иные виды учебной деятельности			
Самостоятельная работа под руководством преподавателя	80		
Самостоятельная работа	106		
Форма промежуточной аттестации	зачет		

4 Содержание дисциплины "Проектирование систем защиты информации", структурированное по разделам (темам)

4.1. Лекционные занятия

Раздел дисциплины, темы лекций и их содержание	Трудоемкость в часах
	ОФ
Раздел 1. Введение в дисциплину 1.1 Цель и задачи дисциплины. Основные термины: система, проект, проектирование, средство и метод проектирования, методика и методология проектирования, принципы проектирования, техническое решение, дипломный проект и дипломная работа 1.2 Классификация систем информационной безопасностьи (СИБ) . Место СИБ в системе управления предприятием . Историческая справка 1.3 Основные задачи, решаемые в СИБ: идентификация состояния объекта, прогнозирование состояния, принятие решения	2
Раздел 2. Основы теории построения систем информационной безопасности 2.1 Классификация и характеристика обеспечивающих и функциональных подсистем СИБ 2.2 Понятие целевой функции. Критерии оценки качества СИБ (технические, экономические, социальные): производительность, надежность, достоверность, точность, экономичность, функциональная полнота. 2.3 Построение модели угроз. 2.4 Построение модели нарушителя. 2.5 Построение модели защищаемого объекта.	2

Раздел 3. Основы методологии построения систем защиты информации 3.1 Основные этапы проектирования СИБ. Понятие жизненного цикла СИБ. 3.2 Основные методы проектирования СИБ: оригинальный, типовой, автоматизированный. 3.3 Основные способы проектирования СИБ: способ классификаций, морфологического анализа, групповой, аналогий, алгоритмы ТРИЗ. 3.4 Основные принципы проектирования СИБ: системный, сверху вниз, снизу вверх, встречный, равной надежности, полноты Эшби. 3.5 Классификация и характеристика инструментальных средств проектирования СИБ: по виду метода проектирования, по глобальности охвата процесса проектирования, по степени автоматизации. 3.6 Характеристика основных руководящих документов по организации проектных работ	4
Раздел 4. Особенности проектирования подсистем информационной безопасности 4.1 Проектирование подсистем защиты доступа 4.2 Проектирование подсистем учета поведения пользователя. 4.3. Проектирование подсистем сетевой защиты. 4.4.Проектирование систем видеонаблюдения 4.5 Проектирование систем защиты выделенных помещений	4
Раздел 5. Оценка технико-экономической эффективности систем информационной безопасности 5.1 Методы оценки экономической эффективности систем информационной безопасности 5.2 Основы риск-анализа при разработке систем информационной безопасности. 5.3 Основы менеджмента информационной безопасности	4
Итого	**16**

4.2 Практические (семинарские) занятия

Тема занятия	**Трудоемкость в часах**
	ОФ
Раздел 1. Введение в дисциплину	
1. Исследование целевой функции построения СИБ и выбор критерия для оценки эффективности проекта	4
Раздел 2. Основы теории построения систем информационной безопасности	
2. Моделирование системы принятия решений в СИБ	4
3. Построение диаграммы Парето	4
4. Построение модели нарушителя	4
5. Построение модели угроз	4
6. Мониторинг поведения пользователя в компьютерной системе	4
Раздел 3. Основы методологии построения систем защиты информации	

7. Настройка аутентификации пользователей с помощью электронного замка	4
8. Натурное моделирование аномалий сетевого трафика	4
9. Прогнозирование временных рядов сетевых трафиков на основе уравнений регрессии	4
10. Исследование целевой функции построения СИБ и выбор критерия для оценки эффективности проекта	4
11. Моделирование системы принятия решений в СИБ	4
12. Оптимизация маршрутов передачи конфиденциальной информации на основе сетевого планирования	4
Раздел 4. Особенности проектирования подсистем информационной безопасности	
13. Организация вычислительного процесса при решении задачи распознавания графического образа	4
14. Определение топологии размещения камер системы видеонаблюдения	4
Раздел 5. Оценка технико-экономической эффективности систем информационной безопасности	
15.Алгоритмизация задач распределения стоимостных ресурсов при проектировании сложных СИБ.	4
Итого	**48**

4.3 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	10
Оформление отчетов по практическим и(или) лабораторным работам	30
Выполнение курсовой работы/проекта	60
Подготовка к промежуточной аттестации	6
Итого	**106**
Самостоятельная работа под руководством преподавателя	80
Защита курсовой работы/проекта	2

4.5 Курсовое проектирование (курсовая работа)

Курсовая работа/проект является формой промежуточной аттестации обучающихся по дисциплине

5 Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине "Проектирование систем защиты 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	ПК-13	Разрабатывает отчетную документацию и разделы технических заданий	**Знать** руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации. **Уметь** использовать методические документы уполномоченных федеральных органов исполнительной власти по защите информации. **Владеть** документацией по защите информации.	Высокий или средний
Опрос по контрольным вопросам или тестирование, подготовка отчетов по практическим и(или) лабораторным работам	ПК-14	Разрабатывает системы защиты информации автоматизированных систем с учетом действующих нормативно-правовых документов	**Знать** особенности проектирования подсистем информационной безопасности. **Уметь** разрабатывать проекты нормативных документов, регламентирующих работу по защите информации в автоматизированных системах. **Владеть** методологиями построения систем 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. Интранет и экстранет.
2. Информационные и сетевые ресурсы открытых систем как объекты атак.

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:

Раздел 1. Введение в дисциплину

1. Цель и задачи дисциплины.
2. Основные термины: система, проект, проектирование, средство и метод проектирования, техническое решение.
3. Классификация систем информационной безопасности (СИБ).
4. Место СИБ в системе управления предприятием.
5. Основные задачи, решаемые в СИБ предприятия

Раздел 2. Основы теории построения систем информационной безопасности

1. Классификация и характеристика обеспечивающих и функциональных подсистем СИБ
2. Понятие целевой функции. Критерии оценки качества СИБ (технические, экономические, социальные)
3. Принцип построения модели угроз.
4. Принцип построения модели нарушителя.
5. Принцип построения модели защищаемого объекта.

Раздел 3. Основы методологии построения систем защиты информации

1. Основные этапы проектирования систем защиты информации (СЗИ).
2. Основные способы и методы проектирования СЗИ
3. Характеристика основных руководящих документов по организации проектных работ
4. Понятие жизненного цикла СЗИ.
5. Исходные данные для проектирования СЗИ

Раздел 4. Особенности проектирования подсистем информационной безопасности

1. Принцип проектирования подсистем защиты доступа

2. Принцип проектирования подсистем учета поведения пользователя.
3. Принцип проектирования подсистем сетевой защиты.
4. Принцип проектирования систем видеонаблюдения
5. Принцип проектирования систем защиты выделенных помещений

Раздел 5. Оценка технико-экономической эффективности систем информационной безопасности

1. Методы оценки экономической эффективности систем информационной безопасности
2. Основы риск-анализа при разработке систем информационной безопасности.
3. Основы менеджмента информационной безопасности
4. Методы оценки технической эффективности систем информационной безопасности
5. Нормативные документы для проведения технической и экономической эффективности систем информационной безопасности

Примерный перечень тестовых заданий:
Раздел 1. Введение в дисциплину

1. На какой стадии создания системы защиты информации АС определяется перечень сведений конфиденциального характера, подлежащих защите?

стадия классификации АС
предпроектная стадия
стадия проектирования
стадия ввода в действие

2. Какое средство защиты информации позволяет выявлять несанкционированный доступ (или попытки несанкционированного доступа) к ресурсам автоматизированной системы?

межсетевой экран
IDS
антивирус
СКД

3. На какие из ниже перечисленных вопросов следует ответить руководителю, прежде чем сформулировать задание на закупку или разработку системы защиты информации? выбрать все верные

каков портрет нарушителя
какие ресурсы компания готова потратить на защиту от внутренних угроз

Раздел 2. Основы теории построения систем информационной безопасности

1. Что дает использование нейронных сетей при построении системы защиты информации?

комплексность
минимизацию ошибок первого и второго рода
адаптивность
универсальность
наследование

2. заключительным этапом построения системы защиты является:

сопровождение
планирование
анализ уязвимых мест

3. Система защиты представляется в виде некоторого декартова произведения множеств, составными частями которых являются элементы системы защиты, в модели политики безопасности на основе

анализа угроз системе
конечных состояний
дискретных компонент
матрицы доступа

Раздел 3. Основы методологии построения систем защиты информации

1. Для обеспечения информационной безопасности сетевых конфигураций следует руководствоваться следующими принципами:

разделение статических и динамических данных
шифрование всей информации
формирование составных сервисов по содержательному принципу

2. Одним из первых и обязательным этапом разработки любой защищенной информационной системы является

анализ потенциально возможных угроз информации
оценка риска
изучение информационных потоков
стандартизация программного обеспечения

3. Метод управления доступом субъектов системы к объектам, основанный на идентификации и опознавании пользователя, процесса и/или группы, к которой он принадлежит, - это управление доступом

полномочное
мандатное
избирательное
привилегированное

Раздел 4. Особенности проектирования подсистем информационной безопасности

1. Подсистема регистрации и учета системы защиты информации должна выполнять следующие функции

оповещение о попытках нарушения защиты
учет носителей информации
идентификация
регистрация доступа в информационную систему
управление потоками информации

2. Подсистема обеспечения целостности системы защиты информации должна выполнять следующие функции

шифрование конфиденциальной информации
учет носителей информации
тестирование средств защиты информации
управление потоками информации
резервное копирование программного обеспечения и данных

3. Подсистема управления доступом системы защиты информации должна выполнять следующие функции

идентификация
учет носителей информации
управление потоками информации
шифрование конфиденциальной информации
аутентификация

Раздел 5. Оценка технико-экономической эффективности систем информационной безопасности

1. Как называется показатель, количественно выражающийся суммой ежегодных прямых и косвенных затрат на функционирование корпоративной системы защиты информации?

экономическая эффективность бизнеса
общая величина затрат на внедрение системы ИБ
совокупная стоимость владения системой ИБ
коэффициент возврата инвестиций

2. Какой показатель отражает общую величину затрат на внедрение системы защиты

информации?

BCP
NPV
ROI
TCO

3. Какая из приведенных методик является самой важной при выборе или проектировании систем защиты информации

анализ рисков
результаты ожидаемых убытков в годовом исчислении (ALE)
анализ затрат / выгоды

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 зачет, курсовая работа/проект, в процессе которых 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;

Курсовая работа/проект является формой промежуточной аттестации обучающихся по дисциплине.

Курсовая работа/проект выполняется обучающимися с целью:

формирования навыков применения теоретических знаний, полученных в ходе освоения дисциплины;
формирования практических навыков в части сбора, анализа и интерпретации результатов, необходимых для последующего выполнения научных научно-исследовательской работы;
формирования навыков логически и последовательно иллюстрировать подготовленную в процессе выполнения курсовой работы/проекта информацию;
формирования способностей устанавливать закономерности и тенденции развития явлений и процессов , анализировать , обобщать и формулировать выводы;
формировать умение использовать результаты, полученные в ход е выполнения курсовой работы/проекта в профессиональной деятельности.

Тема курсовой работы/проекта выбирается обучающимся самостоятельно.

Критерии оценивания курсовой работы/проекта:

85-100 баллов – исчерпывающее или достаточное изложение содержания тематики курсовой работы/проекта в пояснительной записке, соответствие структуры постельной записки курсовой работы/проекта установленным требованиям, уверенное изложение тематики курсовой работы/проекта в ходе процедуры защиты, верные ответы на заданные педагогическим работником вопросы.

70-84 баллов – исчерпывающее но не достаточное изложение содержания тематики курсовой работы/проекта в пояснительной записке, незначительное не соответствие структуры постельной записки курсовой работы/проекта установленным требованиям, неуверенное изложение тематики

курсовой работы/проекта в ходе процедуры защиты, верные ответы на заданные педагогическим работником вопросы.

34–69 баллов – недостаточное изложение содержания тематики курсовой работы/проекта в пояснительной записке, нарушение структуры пояснительной записки курсовой работы/проекта установленным требованиям, неуверенное изложение тематики курсовой работы/проекта в ходе процедуры защиты, верный ответ на один или отсутствие верных ответов на оба вопроса, или курсовая работа/проект не представлена к проверке и защите.

0-34 баллов – курсовая работа/проект не выполнена.

Количество баллов	0–34	34-69	70-84	85-100
Шкала оценивания	Неуд	Удовл	Хорошо	Отлично

Примерные темы курсовых работ/проектов:

1. Проектирование системы разграничения доступа в сети
2. Разработка автоматизированной системы поддержки принятия решений при выборе средств физической защиты
3. Разработка метода синтеза вейвлетов для выявления аномалий в системах обнаружения вторжений.
4. Разработка метода автоматизированной оценки рисков
5. Проектирование АРМ специалиста по информационной безопасности коммерческого банка
6. Модернизация подсистемы защиты персональных данных
7. Разработка метода автоматизированного обнаружения атак на основе анализа событий информационной безопасности ЛВС
8. Разработка метода автоматизированного мониторинга соответствия грифов конфиденциальности документов в мандатной системе контроля доступа
9. Модернизация системы защиты конфиденциального документооборота
10. Разработка концепции защиты информации в автоматизированной системе мониторинга технического состояния системы
11. Проектирование системы видеонаблюдения офиса
12. Модернизация системы защиты электронного документооборота на основе ЭЦП
13. Модернизация системы защиты электронного документооборота
14. Проектирование подсистемы управления доступом сетевым оборудованием региональной сети передачи данных
15. Разработка метода мониторинга перемещения мобильных объектов информатизации на основе средств спутниковой навигации
16. Разработка метода автоматизированного выбора стратегии таможенного досмотра по электронным данным декларативных документов на основе семантического анализа и теории игр.

На зачете 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		

9 семестр:

Примерный перечень вопросов на зачет:

1. Разработка частного технического задания на СЗИ
2. Разработка организационно-технических мероприятий по защите информации в соответствии с предъявляемыми требованиями
3. Средства выявления несанкционированного доступа (или попытки несанкционированного доступа) к ресурсам автоматизированной системы
4. Компоненты защиты информации от несанкционированного доступа
5. Основные этапы проектирования СЗИ.
6. Методы оценки стоимости информационных ресурсов.
7. Методы оценки информационных рисков.
8. Политика безопасности и ее влияние на проектируемую СЗИ.
9. Системы авторизации, преимущества, недостатки и особенности применения.
10. Полная стоимость СЗИ, состав и принципы минимизации.
11. Централизованная система управления безопасностью, принципы реализации, основные задачи и требования к режиму безопасности.
12. Методы управления рисками в системе информационной безопасности при проектировании СЗИ
13. Проектирование ПО администратора информационной безопасности.
14. Формирование технического задания на проектирование СЗИ
15. Функциональная декомпозиция с использованием методологии IDEF0 при проектировании СЗИ.
16. Объектная декомпозиция с использованием методологии UML.
17. Методологии тестирования разработанной СЗИ
18. Определение перечня информации, подлежащей защите с помощью СЗИ
19. Определение актуальных угроз при проектировании СЗИ.
20. Разработка моделей угроз при проектировании СЗИ
21. Определение класса защиты разрабатываемой СЗИ.
22. Обоснование архитектуры и выбор компонентов для СЗИ.
23. Определение набора объектов и субъектов доступа.
24. Определение модели доступа в зависимости от класса защищенности.
25. Выбор средств защиты от НСД для локального и удаленного доступа.
26. Определение набора событий аудита для проектируемой СЗИ
27. Определение средств и методов аудита проектируемой СЗИ.
28. Разработка форматов журналов аудита.
29. Разработка и виды документации на проектируемую СЗИ.
30. Основные подсистемы СЗИ

Примерный перечень тестовых заданий на зачет:

1. На какой стадии создания системы защиты информации АС определяется перечень сведений конфиденциального характера, подлежащих защите?

стадия классификации АС
предпроектная стадия
стадия проектирования
стадия ввода в действие

2. Какое средство защиты информации позволяет выявлять несанкционированный доступ (или попытки несанкционированного доступа) к ресурсам автоматизированной системы?

межсетевой экран
IDS
антивирус
СКД

3. На какие из ниже перечисленных вопросов следует ответить руководителю, прежде чем

сформулировать задание на закупку или разработку системы защиты информации? выбрать все верные

каков портрет нарушителя
какие ресурсы компания готова потратить на защиту от внутренних угроз

4. Что дает использование нейронных сетей при построении системы защиты информации?

комплексность
минимизацию ошибок первого и второго рода
адаптивность
универсальность
наследование

5. заключительным этапом построения системы защиты является:

сопровождение
планирование
анализ уязвимых мест

6. Система защиты представляется в виде некоторого декартова произведения множеств, составными частями которых являются элементы системы защиты, в модели политики безопасности на основе

анализа угроз системе
конечных состояний
дискретных компонент
матрицы доступа

7. Для обеспечения информационной безопасности сетевых конфигураций следует руководствоваться следующими принципами:

разделение статических и динамических данных
шифрование всей информации
формирование составных сервисов по содержательному принципу

8. Одним из первых и обязательным этапом разработки любой защищенной информационной системы является

анализ потенциально возможных угроз информации
оценка риска
изучение информационных потоков
стандартизация программного обеспечения

9. Метод управления доступом субъектов системы к объектам, основанный на идентификации и опознавании пользователя, процесса и/или группы, к которой он принадлежит, - это управление доступом

полномочное
мандатное
избирательное
привилегированное

10. Подсистема регистрации и учета системы защиты информации должна выполнять следующие функции

оповещение о попытках нарушения защиты
учет носителей информации
идентификация
регистрация доступа в информационную систему
управление потоками информации

11. Подсистема обеспечения целостности системы защиты информации должна выполнять следующие функции

шифрование конфиденциальной информации
учет носителей информации
тестирование средств защиты информации
управление потоками информации
резервное копирование программного обеспечения и данных

12. Подсистема управления доступом системы защиты информации должна выполнять следующие функции

идентификация
учет носителей информации
управление потоками информации
шифрование конфиденциальной информации
аутентификация

13. Как называется показатель, количественно выражающийся суммой ежегодных прямых и косвенных затрат на функционирование корпоративной системы защиты информации?

экономическая эффективность бизнеса
общая величина затрат на внедрение системы ИБ
совокупная стоимость владения системой ИБ
коэффициент возврата инвестиций

14. Какой показатель отражает общую величину затрат на внедрение системы защиты информации?

BCP
NPV
ROI
TCO

15. Какая из приведенных методик является самой важной при выборе или проектировании систем защиты информации

анализ рисков
результаты ожидаемых убытков в годовом исчислении (ALE)
анализ затрат / выгоды

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.

Выполненная курсовая работа/проект в форме пояснительной записки направляется педагогическому работнику, являющемуся руководителем курсовой работы/проекта, в срок за 10 дней до дня процедуры защиты курсовой работы/проекта, установленном в соответствии с расписанием.

Защита курсовой работы/проекта осуществляется в форме доклада, время доклада устанавливается не более 15 минут и ответов на 2 вопроса по теме курсовой работы/проекта.

Защита курсовой работы/проекта организуется до промежуточной аттестации по дисциплине в форме зачета (экзамена). Обучающиеся, не получившие удовлетворительную оценку за курсовую работу/проект дорабатывают её и проходят повторную аттестация согласно установленному расписанию. В процессе защиты курсовой работы/проекта педагогический работник устанавливает форсированность планируемых результатов обучения по дисциплине.

Результаты, полученные по итогам выполнения курсовой работы/проекта, учитываются при прохождении промежуточной аттестации по дисциплине, проводимой в форме зачета (экзамена).

Требования к структуре пояснительной записки курсовой работы /проекта

Курсовая работа/проект выполняется с помощью компьютерной техники, шрифтом Times New

Roman размером 14 пунктов и межстрочным интервалом 1,5 .

Объем пояснительной записки курсовой работы/проекта 20-25 листов без учета приложений. Количество приложений не ограничено. В качестве приложений могут быть размещены фотографии, таблицы, диаграммы и т.п.

Курсовая работа/проект, после согласования с педагогическим работником – руководителем курсовой работы/проекта (далее – руководитель), распечатывается. На титульном листе указывается тема курсовой работы/проекта, ФИО обучающегося, курс обучения, учебная группа, ФИО руководителя, его ученое звание и ученая степень.

Распечатанная пояснительная записка курсовой работы/проекта оформляется в папку-скоросшиватель и передается обучающимся самостоятельно на кафедру, работником которой является руководитель, для оценивания руководителем содержания пояснительной записки выполненной курсовой работы/проекта.

Требования к структуре пояснительной записки курсовой работы /проекта

1. титульный лист;
2. содержание;
3. введение;
4. основная часть;
5. заключение;
6. список использованных литературных источников, в том числе размещенных в сети Интернет и в ЭБС;
7. приложения.

6 Учебно-методическое обеспечение

6.1 Основная литература

1. Болодурина, И. П. Проектирование компонентов распределенных информационных систем : учебное пособие / И. П. Болодурина, Т. Волкова ; Оренбургский государственный университет. – Оренбург : Оренбургский государственный университет, 2012. – 215 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=259156 (дата обращения: 15.04.2026). – ISBN 978-5-4417-0077-1. – Текст : электронный.

2. Завьялов, А. В. Анализ и проектирование информационных систем : методические указания / А. В. Завьялов. — Москва : РТУ МИРЭА, 2020. — 22 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/163813 (дата обращения: 23.03.2026). — Режим доступа: для авториз. пользователей.

3. Гвоздева, Т. В. Проектирование информационных систем. Стандартизация : учебное пособие / Т. В. Гвоздева, Б. А. Баллод. — Санкт-Петербург : Лань, 2019. — 252 с. — ISBN 978-5-8114-3517-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/115515 (дата обращения: 23.03.2026). — Режим доступа: для авториз. пользователей.

4. Основы управления информационной безопасностью : учебное пособие для студентов, обучающихся по направлениям подготовки (специальностям) укрупненной группы специальностей 090000 "Информационная безопасность" / А. П. Курило, Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. – 2-е изд. – Москва : Горячая линия-Телеком, 2022. – 244 с. – (Вопросы управления информационной безопасностью). – Текст : непосредственный.

6.2 Дополнительная литература

1. Беляков, С. Л. Основы разработки программ на языке C++ для систем информационной безопасности : учебное пособие : [16+] / С. Л. Беляков, А. В. Боженюк, М. В. Петряева ; Южный федеральный университет. – Ростов-на-Дону ; Таганрог : Южный федеральный университет, 2020. – 152 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=612164 (дата обращения: 10.04.2026). – Библиогр. в кн. – ISBN 978-5-9275-3521-7. – Текст : электронный.

2. Рочев, К. В. Информационные технологии. Анализ и проектирование информационных систем : учебное пособие / К. В. Рочев. — 2-е изд., испр. — Санкт-Петербург : Лань, 2019. — 128 с. — ISBN 978-5-8114-3801-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/122181 (дата обращения: 23.03.2026). — Режим доступа: для авториз. пользователей.

3. Проектирование информационных систем : курс лекций : учебное пособие : [16+] / авт.-сост. Т. В. Киселева. – Ставрополь : Северо-Кавказский Федеральный университет (СКФУ), 2018. – Часть 1. – 150 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=563326 (дата обращения: 09.04.2026). – Библиогр.в кн. – Текст : электронный.

4. Грекул, В. И. Проектирование информационных систем : учебник и практикум для академического бакалавриата : [для студентов вузов, обучающихся по инженерно-техническим и экономическим направлениям] / В. И. Грекул, Н. Л. Коровкина, Г. А. Левочкина ; Нац. исслед. ун-т Высш. школа экономики. – Москва : Юрайт, 2017. – 385 с. – (Бакалавр. Академический курс). – Текст : непосредственный.

5. Гвоздева, Т. В. Проектирование информационных систем. Планирование проекта. Лабораторный практикум : учебное пособие / Т. В. Гвоздева. — Санкт-Петербург : Лань, 2019. — 116 с. — ISBN 978-5-8114-3836-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/122173 (дата обращения: 23.03.2026). — Режим доступа: для авториз. пользователей.

6. Гвоздева, Т. В. Проектирование информационных систем: технология автоматизированного проектирования. Лабораторный практикум : учебное пособие / Т. В. Гвоздева, Б. А. Баллод. — 2-е изд., стер. — Санкт-Петербург : Лань, 2020. — 156 с. — ISBN 978-5-8114-5147-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/133477 (дата обращения: 23.03.2026). — Режим доступа: для авториз. пользователей.

7. Вейцман, В. М. Проектирование информационных систем : учебное пособие / В. М. Вейцман. — Санкт-Петербург : Лань, 2019. — 316 с. — ISBN 978-5-8114-3713-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/122172 (дата обращения: 23.03.2026). — Режим доступа: для авториз. пользователей.

6.3 Методическая литература

1. Моделирование процессов и систем защиты 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. – Ч. 1: Системный подход к управлению защитой информации. – Кемерово : КузГТУ, 2018. – 27 с. – URL: http://library.kuzstu.ru/meto.php?n=9124 (дата обращения: 23.03.2026). – Текст : электронный.

6.4 Профессиональные базы данных и информационные справочные системы

1. База данных Springer Materials http://materials.springer.com/
2. Цифровая библиотека IPRsmart https://ipr-smart.ru/
3. Электронная библиотечная система «Университетская библиотека онлайн» http://biblioclub.ru/
4. Электронная библиотечная система «Лань» http://e.lanbook.com
5. Электронная библиотека КузГТУ https://library.kuzstu.ru/index.php/punkt-2/podrazdel-21
6. Электронная библиотека Новосибирского государственного технического университета https://clck.ru/UoXpv
7. Образовательная платформа «Юрайт» https://urait.ru/
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/
11. 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. Информация и безопасность : научный журнал

7 Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

ЭИОС КузГТУ:

а) 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 "Проектирование систем защиты 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 "Проектирование систем защиты информации", включая перечень программного обеспечения и информационных справочных систем

Для изучения дисциплины может использоваться следующее программное обеспечение:

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

10 Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине "Проектирование систем защиты 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.