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

Моделирование и испытание систем защиты информационных систем

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 "Моделирование и испытание систем защиты информационных систем", соотнесенных с планируемыми результатами освоения образовательной программы

Освоение дисциплины направлено на формирование:

общепрофессиональных компетенций:

ОПК-7.1. - Способен использовать программные и программно-аппаратные средства для моделирования и испытания систем защиты информационных систем;

Результаты обучения по дисциплине определяются индикаторами достижения компетенций

Индикатор(ы) достижения:

Использует программные и программно-аппаратные средства для моделирования и испытания систем защиты информационных систем

Результаты обучения по дисциплине:

Знать современные методы моделирования и испытания систем защиты информационных систем.

Уметь уметь интерпретировать полученные результаты для решения задач проектирования и прогнозирования качества работы систем защиты информационных систем

Владеть программными и программно-аппаратными средствами средствами для моделирования и испытания систем защиты информационных систем

2 Место дисциплины "Моделирование и испытание систем защиты информационных систем" в структуре ОПОП специалитета

Для освоения дисциплины необходимы знания умения, навыки и (или) опыт профессиональной деятельности, полученные в рамках изучения следующих дисциплин: Безопасность операционных систем, Безопасность систем баз данных, Организационное и правовое обеспечение информационной безопасности, Основы информационной безопасности, Сети и системы передачи информации, Техническая защита информации, 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 "Моделирование и испытание систем защиты информационных систем" 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 "Моделирование и испытание систем защиты информационных систем" составляет 5 зачетных единиц, 180 часов.

Форма обучения	**Количество часов**		
	ОФ	**ЗФ**	**ОЗФ**
Курс 5/Семестр 9			
Всего часов	180		
Контактная работа обучающихся с преподавателем (по видам учебных занятий):			
Аудиторная работа			
Лекции	32		
Лабораторные занятия	48		
Практические занятия			
Внеаудиторная работа			

Форма обучения	Количество часов		
	ОФ	ЗФ	ОЗФ
Индивидуальная работа с преподавателем:			
Консультация и иные виды учебной деятельности			
Самостоятельная работа под руководством преподавателя	20		
Самостоятельная работа	44		
Форма промежуточной аттестации	экзамен /36		

4 Содержание дисциплины "Моделирование и испытание систем защиты информационных систем", структурированное по разделам (темам)

4.1. Лекционные занятия

Раздел дисциплины, темы лекций и их содержание	Трудоемкость в часах
	ОФ
9 семестр	
Раздел 1. Моделирование систем защиты информационных систем	
Введение в дисциплину: Цели и задачи изучения, место дисциплины в структуре основной профессиональной деятельности образовательной подготовки специалиста по защите информации. Планируемые результаты обучение по дисциплине. Виды и объемы учебной работы и содержание дисциплины. Перечень основных объектов и процессов, изучаемых в дисциплине. Основные объекты, изучаемые в дисциплине, и их определения. Основные процессы, изучаемые в дисциплине, и их определения. Взаимосвязь объектов и процессов, изучаемых в дисциплине.	2
Общие положения о создании АСЗИ: Документы, применяемые при создании автоматизированных систем: нормативные правовые акты, регламентирующие порядок создания автоматизированных информационных систем; документы регуляторов в области информационных технологий, информационной безопасности и защиты информации; государственные стандарты, рекомендации, применяемые при создании автоматизированных информационных систем: государственные стандарты и рекомендации Российской Федерации, государственные военные стандарты Российской Федерации; руководящие и методические документы Минобороны России.	14
Организация и общие правила выполнения работ по созданию АСЗИ: Основные документы, на основании которых осуществляется создание АСЗИ: документы, определяющий необходимость создания АСЗИ; технические задания на создание АСЗИ и ее составных частей; техническое задание на выполнение ОКР по созданию АСЗИ; частные технические задания на выполнение составных частей ОКР; технические задания на выполнение НИР; календарный план (план-график) выполнения работ по созданию АСЗИ и ее составных частей. Участники работ по созданию АСЗИ: состав участников работ по созданию АСЗИ; обязанности участников работ по созданию АСЗИ; требования к участникам работ по созданию АСЗИ; отношения между участниками работ по созданию АСЗИ.	16
Итого	**32**

10 семестр	
Раздел 2. Испытание систем защиты информационных систем	
Содержание основных работ по созданию АСЗИ, проводимых на стадиях проектирования АСЗИ: Содержание основных работ, проводимых на стадии «Технический проект»: содержание основных работ, проводимых на этапе «Разработка проектных решений по системе и её частям»; содержание основных работ, проводимых на этапе «Разработка документации на АС и её части»: определение перечня документации, подлежащей разработке; разработка технического проекта АСЗИ; разработка необходимых схем; разработка необходимых заданий; разработка необходимых описаний компонентов АСЗИ; оценка надёжности создаваемой АСЗИ; защита технического проекта АСЗИ; доработка и утверждение технического проекта АСЗИ и других документов АСЗИ; содержание основных работ, проводимых на этапе «Разработка и оформление документации на поставку изделий для комплектования АС и (или) технических требований (технических заданий) на их разработку: разработка документации на поставку изделий для комплектования АСЗИ; подготовка технических заданий на разработку изделий для комплектования АСЗИ, не изготавливаемых серийно; содержание основных работ, проводимых на этапе «Разработка заданий на проектирование в смежных частях проекта объекта авто-матизации».	34
Испытание систем защиты информационных систем	14
Итого	**48**

4.2 Практические (семинарские) занятия

Тема занятия	**Трудоемкость в часах**
	ОФ
10 семестр	
Испытание систем защиты информационных систем	16
Комплекс показателей защищенности систем	16
Методика оценки защищенности системы	16
Методика применения инструментальных средств для анализа системы защиты информации	16
Итого	**64**

4.3 Лабораторные занятия

Тема занятия	**Трудоемкость в часах**
	ОФ
9 семестр	
Моделирование систем защиты информационных систем	20
Системный подход	6

Динамичный характер поля угроз	6
Иерархия уровней в модели	8
Модель системы защиты информационных систем	8
Итого	**48**

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

Вид СРС	**Трудоемкость в часах**
	ОФ
9 семестр	
Ознакомление с содержанием основной и дополнительной литературы, методических материалов, конспектов лекций для подготовки к занятиям	24
Оформление отчетов по практическим и(или) лабораторным работам	14
Подготовка к промежуточной аттестации	6
Итого	**44**
Самостоятельная работа под руководством преподавателя	20
Экзамен	36
10 семестр	
Ознакомление с содержанием основной и дополнительной литературы, методических материалов, конспектов лекций для подготовки к занятиям	10
Оформление отчетов по практическим и(или) лабораторным работам	10
Выполнение курсовой работы/проекта	14
Подготовка к промежуточной аттестации	6
Итого	**40**
Самостоятельная работа под руководством преподавателя	26
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 "Моделирование и испытание систем защиты информационных систем"

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-7.1. - Способен использовать программные и программноаппаратные средства для моделирования и испытания систем защиты информационных систем	Использует программные и программно-аппаратные средства для моделирования и испытания систем защиты информационных систем	**Знать** современные методы моделирования и испытания систем защиты информационных систем. **Уметь** уметь интерпретировать полученные результаты для решения задач проектирования и прогнозирования качества работы систем защиты информационных систем **Владеть** программными и программно-аппаратными средствами средствами для моделирования и испытания систем защиты информационных систем	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. Моделирование систем защиты информационных систем

1. Какие методы моделирования наиболее эффективны при построении системы защиты объекта информатизации?
2. Приведите пример модели многозвенной защиты объекта информа-тизации. Как в этом случае рассчитывается прочность защиты?
3. Биосистемная аналогия при моделировании систем защиты информационных систем
4. специальное ПО для моделирования систем ИБ, основные принципы его функционирования
5. Какой вид диаграмм используется для описания модели системы поддержки принятия парето-оптимальных решений в процессе моделирования систем защиты ИС?

Раздел 2. Испытание систем защиты информационных систем

1. Показатели эффективности систем защиты ИС
2. Типовые алгоритмы испытаний систем защиты ИС
3. Цели и задачи испытания систем защиты ИС
4. Принцип проведения инструментальных (инструментально-расчетных) измерений
5. Подсистемы систем защиты ИС, подлежащие испытанию

Примерный перечень тестовых заданий:

Раздел 1. Моделирование систем защиты информационных систем

1. При моделировании активных действий противника, представляющего угрозу ИС, его обычно ставят:

в наименее благоприятные условия
в условия, приближенные к реальным
в случайно выбранные условия
в наиболее благоприятные условия

2. Моделирование процедуры дешифрования в системе защиты ИС предусматривает:

обязательнее знание ключа шифрования
обязательнее отсутствие знаний о ключе
частичное знание ключа шифрования
необязательное знание ключа шифрования

3. Для моделирования процессов в системе защиты информации используются следующие методы моделирования: выбрать все верные

аналитическое
имитационное
оптимизационное

Раздел 2. Испытание систем защиты информационных систем

1. Какие подсистемы систем защиты информации подлежат испытанию в обязательном порядке: выбрать все верные

средства вычислительной техники
межсетевые экраны
механизм управления доступом

механизм контроля целостности

2. В каком нормативном документе изложены основные правила испытаний систем защиты ИС? выбрать все верные

руководящий документ Гостехкомиссии РФ
руководящий документ ФСБ РФ
руководящий документ МВД РФ
руководящий документ ФСТЭК РФ
ГОСТ 19.301-79,
ГОСТ 51719-2001

3. Какие существуют виды испытаний для автоматизированных систем согласно ГОСТ 34.603 п.1.3: выбрать все верные

Предварительные
Опытная эксплуатация;
Приемочные.
Периодические
стресс-тестирование

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, экзамен, 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:

,
,
,
,
,

На зачете/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		

9 семестр:

Примерный перечень вопросов на экзамен:

1. Моделирование как инструмент анализа комплексных систем защиты информации.
2. Виды моделей систем защиты ИС
3. Требования к построению модели систем защиты ИС
4. Составные компоненты информационной модели систем защиты ИС

5. Функции организационной модели систем защиты ИС
6. Функции структурной модели систем защиты ИС
7. Исходные данные, необходимые для моделирования систем защиты ИС
8. Математические модели квазигармонических процессов как модели реальных процессов в системах защиты от несанкционированного прослушивания.
9. Модели шумов в системах защиты информации.
10. Формирование однокомпонентной системы перехвата сигналов в системе защиты ИС.
11. Способ перехода от математической модели процесса к цифровой модели: нормировка параметров модели, задание шага дискретизации и энергетических характеристик.
12. Определение динамических диапазонов модулируемых процессов в системах защиты ИС.
13. Метод наращивания сложности модели путем присоединения к базовой дополнительных функций.
14. Метод композиции элементарных операции для создания сложных систем защиты информации.
15. Этапы создания общей структуры модели процессов и систем защиты информации в среде компьютерного моделирования.
16. Декомпозиция, согласование параметров входных процессов с параметрами системы защиты информации, компоновка модели в виде значимых узлов.
17. Основы системного подхода в теории и практике моделирования процессов и систем.
18. Итоговая документация процесса моделирования системы защиты ИС
19. Итоговая документация процесса испытания системы защиты ИС
20. Виды необходимой документации для начала процесса моделирования системы защиты ИС

Примерный перечень тестовых заданий на экзамен:

1. При моделировании активных действий противника, представляющего угрозу ИС, его обычно ставят:

в наименее благоприятные условия
в условия, приближенные к реальным
в случайно выбранные условия
в наиболее благоприятные условия

2. Моделирование процедуры дешифрования в системе защиты ИС предусматривает:

обязательнее знание ключа шифрования
обязательнее отсутствие знаний о ключе
частичное знание ключа шифрования
необязательное знание ключа шифрования

3. Для моделирования процессов в системе защиты информации используются следующие методы моделирования: выбрать все верные

аналитическое
имитационное
оптимизационное

10 семестр:

Примерный перечень вопросов на зачет:

1. Виды необходимой документации для начала процесса испытания системы защиты ИС
2. Отличия моделирования от макетирования систем защиты информации
3. К какой нормативной процедуре относится испытание системы защиты ИС?
4. Критерии успешности проведения испытаний систем защиты ИС
5. Моделирование сценариев действий нарушителя ИБ с использованием сети Петри
6. Анализ рисков ИБ при моделировании систем защиты ИС с использованием методики COBIT
7. Модели безопасности с полным перекрытием множества угроз
8. Составные компоненты информационной модели
9. Математические теории. используемые в процессе моделирования систем защиты ИС
10. Виды и способы испытаний систем защиты информации ИС
11. Какие методы моделирования наиболее эффективны при построении системы защиты объекта

информатизации?
12. Пример модели многозвенной защиты объекта информатизации.
13. Методика расчёта прочности защиты
14. Биосистемная аналогия при моделировании систем защиты информационных систем
15. Специальное ПО для моделирования систем ИБ, основные принципы его функционирования
16. Виды диаграмм, используемых для описания модели системы поддержки принятия Парето-оптимальных решений в процессе моделирования систем защиты ИС
17. Типовые алгоритмы испытаний систем защиты ИС
18. Цели и задачи испытания систем защиты ИС
19. Принцип проведения инструментальных (инструментально-расчетных) измерений
20. Подсистемы систем защиты ИС, подлежащие испытанию
21. Какие подсистемы систем защиты информации подлежат испытанию в обязательном порядке?
22. Нормативные документы, описывающие правила проведения испытаний систем защиты ИС

Примерный перечень тестовых заданий на зачет:

1. Какие подсистемы систем защиты информации подлежат испытанию в обязательном порядке: выбрать все верные

средства вычислительной техники
межсетевые экраны
механизм управления доступом
механизм контроля целостности

2. В каком нормативном документе изложены основные правила испытаний систем защиты ИС? выбрать все верные

руководящий документ Гостехкомиссии РФ
руководящий документ ФСБ РФ
руководящий документ МВД РФ
руководящий документ ФСТЭК РФ
ГОСТ 19.301-79,
ГОСТ 51719-2001

3. Какие существуют виды испытаний для автоматизированных систем согласно ГОСТ 34.603 п.1.3: выбрать все верные

Предварительные
Опытная эксплуатация;
Приемочные.
Периодические
стресс-тестирование

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. Голиков, А. М. Защита информации в инфокоммуникационных системах и сетях : учебное пособие / А. М. Голиков. — Москва : ТУСУР, 2012. — 374 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/11381 (дата обращения: 23.03.2026). — Режим доступа: для авториз. пользователей.

2. Флегонтов, А. В. Моделирование информационных систем. Unified Modeling Language : учебное пособие / А. В. Флегонтов, И. Ю. Матюшичев. — 2-е изд., стер. — Санкт-Петербург : Лань, 2019. — 112 с. — ISBN 978-5-8114-2907-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/112065 (дата обращения: 23.03.2026). — Режим доступа: для авториз. пользователей.

6.2 Дополнительная литература

1. Котенко, В. В. Технологии информационного анализа пользовательского уровня телекоммуникационных систем : учебное пособие : [16+] / В. В. Котенко ; Южный федеральный университет. – Ростов-на-Дону ; Таганрог : Южный федеральный университет, 2019. – 195 с. : ил., табл., схем. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=577870 (дата обращения: 10.04.2026). – Библиогр.: с. 186 - 189. – ISBN 978-5-9275-3176-9. – Текст : электронный.

2. Креопалов, В. В. Технические средства и методы защиты информации : учебно-практическое пособие / В. В. Креопалов. – Москва : Евразийский открытый институт, 2011. – 278 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=90753 (дата обращения: 13.04.2026). – ISBN 978-5-374-00507-3. – Текст : электронный.

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. 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. Электронная библиотека Новосибирского государственного технического университета https://clck.ru/UoXpv
5. Образовательная платформа «Юрайт» https://urait.ru/
6. Научная электронная библиотека eLIBRARY.RU https://elibrary.ru/projects/subscription/rus_titles_open.asp?
7. Национальная электронная библиотека https://rusneb.ru/

6.5 Периодические издания

1. Информационные системы и технологии : научно-технический журнал https://eivis.ru/browse/publication/542286
2. Информационные технологии и вычислительные системы : журнал https://elibrary.ru/contents.asp?titleid=8746
3. Информация и безопасность : научный журнал
4. Открытые системы. СУБД : журнал https://eivis.ru/browse/publication/64072
5. Программные продукты и системы : международный научно-практический журнал
6. САПР и графика : 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.

8 Методические указания для обучающихся по освоению дисциплины "Моделирование и испытание систем защиты информационных систем"

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 "Моделирование и испытание систем защиты информационных систем", 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. Microsoft Project
8. Kaspersky Endpoint Security
9. Браузер Спутник

10 Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине "Моделирование и испытание систем защиты информационных систем"

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.