

МИНОБРНАУКИ РОССИИ

федеральное государственное бюджетное образовательное учреждение
высшего образования

«Кузбасский государственный технический университет имени Т. Ф. Горбачева»

Институт информационных технологий, машиностроения и автотранспорта



ПОДПИСАНО ЭП КУЗГТУ

Подразделение: институт информационных
технологий, машиностроения и
автотранспорта

Должность: директор института

Дата: 15.09.2026 16:04:18

Дубинкин Дмитрий Михайлович

Рабочая программа дисциплины

Проектирование систем (компонента системы) обеспечения информационной безопасности

Направление подготовки 10.04.01 Информационная безопасность

Направленность (профиль) 01 Организация и технология защиты информации

Присваиваемая квалификация
"Магистр"

Формы обучения
очно-заочная

Кемерово 2026 г.



1784080246

Рабочую программу составил:

ПОДПИСАНО ЭП КУЗГТУ

Подразделение: кафедра информационной безопасности

Должность: заведующий кафедрой (к.н.,спд)

Дата: 17.07.2026 10:15:57

Прокопенко Евгения Викторовна

Рабочая программа обсуждена на заседании кафедры информационной безопасности

Протокол № 9 от 03.07.2026

ПОДПИСАНО ЭП КУЗГТУ

Подразделение: кафедра информационной безопасности

Должность: заведующий кафедрой (к.н.,спд)

Дата: 17.07.2026 10:16:14

Прокопенко Евгения Викторовна

Согласовано учебно-методической комиссией по направлению подготовки (специальности)
10.04.01 Информационная безопасность

Протокол № 9 от 03.07.2026

ПОДПИСАНО ЭП КУЗГТУ

Подразделение: кафедра информационной безопасности

Должность: заведующий кафедрой (к.н.,спд)

Дата: 17.07.2026 10:16:33

Прокопенко Евгения Викторовна



1784080246

1 Перечень планируемых результатов обучения по дисциплине "Проектирование систем (компонента системы) обеспечения информационной безопасности", соотнесенных с планируемыми результатами освоения образовательной программы

Освоение дисциплины направлено на формирование:

общепрофессиональных компетенций:

ОПК-2 - Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности;

Результаты обучения по дисциплине определяются индикаторами достижения компетенций

Индикатор(ы) достижения:

Разрабатывает технический проект системы обеспечения информационной безопасности, а также их компонент(подсистемы).

Результаты обучения по дисциплине:

Знать основные принципы разработки политики информационной безопасности на предприятии, принципы анализа исходных данных для проектирования подсистем и средств обеспечения информационной безопасности, современную аппаратно-программную базу компьютерной техники для решения задач защиты информации.

Уметь применять комплексный подход к обеспечению информационной безопасности объекта защиты, проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности, применять программные средства системного, прикладного и средства системного, специального назначения, инструментальные средства, языки и системы программирования для решения задач защиты информации.

Владеть основными методами обеспечения информационной безопасности объекта защиты, методами технико-экономического обоснования проектных решений, методами и средствами системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения задач защиты информации.

2 Место дисциплины "Проектирование систем (компонента системы) обеспечения информационной безопасности" в структуре ОПОП магистратуры

Для освоения дисциплины необходимы знания умения, навыки и (или) опыт профессиональной деятельности, полученные в рамках изучения следующих дисциплин: Управление информационной безопасностью, Защищенные информационные системы, Организационно-распорядительная документация по обеспечению информационной безопасности, Построение моделей угроз информационной безопасности, Технологии обеспечения информационной безопасности.

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 (компонента системы) обеспечения информационной безопасности" 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 (компонента системы) обеспечения информационной безопасности" составляет 7 зачетных единиц, 252 часа.

Форма обучения	Количество часов		
	ОФ	ЗФ	ОЗФ
Курс 2/Семестр 3			
Всего часов			252
Контактная работа обучающихся с преподавателем (по видам учебных занятий):			
Аудиторная работа			
Лекции			12
Лабораторные занятия			12



1784080246

Форма обучения	Количество часов		
	ОФ	ЗФ	ОЗФ
Практические занятия			
Внеаудиторная работа			
Индивидуальная работа с преподавателем:			
Консультация и иные виды учебной деятельности			
Самостоятельная работа под руководством преподавателя			120
Самостоятельная работа			72
Форма промежуточной аттестации			экзамен /36

4 Содержание дисциплины "Проектирование систем (компонента системы) обеспечения информационной безопасности", структурированное по разделам (темам)

4.1. Лекционные занятия

Раздел дисциплины, темы лекций и их содержание	Трудоемкость в часах	
	ОФ	ОЗФ
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. 1.2 Классификация систем информационной безопасности (СИБ). Место СИБ в системе управления предприятием. Историческая справка. 1.3 Основные задачи, решаемые в СИБ: идентификация состояния объекта, прогнозирование состояния, принятие решения.	2	2
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	2
3. Основы методологии построения систем защиты информации 3.1 Основные этапы проектирования СИБ. Понятие жизненного цикла СИБ. 3.2 Основные методы проектирования СИБ: оригинальный, типовый, 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	2	2
4. Особенности проектирования подсистем(компонент) 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.	2	2



1784080246

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	4
Итого	12	12

4.2. Лабораторные занятия

Наименование работы	Трудоемкость в часах	
	ОФ	ОЗФ
1. Исследование целевой функции построения СИБ и выбор критерия для оценки эффективности проекта	2	2
2. Моделирование системы принятия решений в СИБ. Построение модели нарушителя. Построение модели угроз. Мониторинг поведения пользователя в компьютерной системе.	2	2
3. Настройка аутентификации пользователей с помощью электронного замка.	2	2
4. Организация вычислительного процесса при решении задачи распознавания графического образа. Определение топологии размещения камер системы видеонаблюдения.	2	2
5. Алгоритмизация задач распределения стоимостных ресурсов при проектировании сложных СИБ.	4	4
Итого	12	12

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

Вид СРС	Трудоемкость в часах	
	ОФ	ОЗФ
Ознакомление с содержанием основной и дополнительной литературы, методических материалов, конспектов для подготовки к занятиям	38	38
Оформление отчетов по практическим и(или) лабораторным работам	28	28
Подготовка к промежуточной аттестации	6	6
Итого	72	72
Экзамен	36	36
Самостоятельная работа под руководством преподавателя	120	120

Самостоятельная работа под руководством преподавателя:

Внеаудиторная самостоятельная работа выполняется обучающимся самостоятельно по индивидуальным заданиям, полученным от педагогического работника, но без его непосредственного участия.

В ходе выполнения самостоятельной работы педагогический работник осуществляет



1784080246

непосредственное руководство процессом выполнения индивидуальной самостоятельной работы в форме текущего контроля успеваемости. Текущий контроль успеваемости обеспечивает оценивание хода самостоятельного освоения дисциплины (практик). Для организации самостоятельной работы обучающегося по индивидуальным заданиям, полученным от педагогического работника, а так же показатели и критерии оценивания, описание шкал оценивания результатов самостоятельной работы, используются оценочные материалы, размещенные в фондах оценочных средств для текущего контроля успеваемости обучающихся.

5 Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине "Проектирование систем (компонента системы) обеспечения информационной безопасности"

5.1 Паспорт комплекта оценочных материалов

Планируемые результаты обучения по дисциплине (модулю)

Дисциплина направлена на формирование следующих компетенций выпускника:

Ф о р м а (ы) текущего контроля	Компетенции, формируемые в результате освоения дисциплины (модуля)	И н д и к а т о р (ы) д о с т и ж е н и я компетенции	Результаты обучения по дисциплине (модулю)	Уровень



1784080246

Опрос по контрольным вопросам, подготовка отчетов по практическим и (или) лабораторным работам	ОПК-2	Разрабатывает технический проект системы обеспечения информационной безопасности, а также их компонент(подсистемы).	Знать основные принципы разработки политики информационной безопасности на предприятии, принципы анализа исходных данных для проектирования подсистем и средств обеспечения информационной безопасности, современную аппаратно-программную базу компьютерной техники для решения задач защиты информации. Уметь применять комплексный подход к обеспечению информационной безопасности объекта защиты, проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности, применять программные средства системного, прикладного и средства специального назначения, инструментальные средства, языки и системы программирования для решения задач защиты информации. Владеть основными методами обеспечения информационной безопасности объекта защиты, методами технико-экономического обоснования проектных решений, методами и средствами системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения задач 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. 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 материалы при текущем контроле

Текущий контроль по темам дисциплины заключается в опросе обучающихся по контрольным вопросам в оформлении отчетов по лабораторным работам.

Опросе обучающихся по контрольным вопросам

Обучающийся отвечает на 2 вопроса.



1784080246

Например:

Содержание вопроса (задания)	Правильный ответ
Как называется основной документ, разрабатываемый на начальном этапе проектирования, который содержит совокупность требований к системе и является юридическим основанием для выполнения работ исполнителем?	Техническое задание (или ТЗ).
Процесс описания потенциального нарушителя, его возможностей, целей и вероятных способов реализации атак в рамках разработки проекта системы защиты называется _____ угроз.	Моделирование

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

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 материалы при промежуточной аттестации

Формами промежуточной аттестации являются экзамен, в процессе которых определяется сформированность обозначенных в рабочей программе компетенций.

Инструментом измерения сформированности компетенций являются:

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

На экзамене обучающийся отвечает на 2 вопроса или проходит тестирование.

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	



1784080246

Шкала оценивания	Не зачтено	Зачтено
------------------	------------	---------

Примерный перечень вопросов на экзамен:

Содержание вопроса (задания)	Правильный ответ
Как называется основной документ, разрабатываемый на начальном этапе проектирования, который содержит совокупность требований к системе и является юридическим основанием для выполнения работ исполнителем?	Техническое задание (или ТЗ).
Процесс описания потенциального нарушителя, его возможностей, целей и вероятных способов реализации атак в рамках разработки проекта системы защиты называется _____ угроз.	Моделирование

Примерный перечень вопросов на зачет:

1. Методы оценки экономической эффективности систем информационной безопасности.
2. Основы риск-анализа при разработке систем информационной безопасности.
3. Основы менеджмента информационной безопасности.

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 - при 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	Удовлетворительно	Хорошо	Отлично	
	не зачтено	зачтено			

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

ОПК-2 Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности;

Содержание вопроса (задания)	Правильный ответ								
На каком этапе проектирования системы обеспечения ИБ осуществляется построение модели угроз и определение актуальных векторов атак? 1. Ввод системы в эксплуатацию. 2. Гарантийное обслуживание. 3. Предпроектное обследование и формирование требований. 4. Утилизация компонентов системы.	3								
Какое проектное решение направлено на минимизацию ущерба при компрометации одного из сегментов корпоративной сети? 1. Использование антивируса на сервере. 2. Резервное копирование баз данных. 3. Сегментация сети с использованием межсетевых экранов. 4. Назначение одного администратора для всех подсистем.	3								
Установите соответствие между стадией создания автоматизированной системы в защищенном исполнении (согласно ГОСТ 34.601-90) и основным содержанием работ на этой стадии:	A - 2, Б - 3, В - 1.								
<table border="1"> <tr> <th>Стадия проектирования</th><th>Содержание работ</th></tr> <tr> <td>А) Формирование требований</td><td>1) Разработка деталей, схем и программных кодов</td></tr> <tr> <td>Б) Технический проект</td><td>2) Обследование объекта и создание обоснования необходимости системы</td></tr> <tr> <td>В) Рабочая документация</td><td>3) Разработка окончательных проектных решений по системе и её частям</td></tr> </table>	Стадия проектирования	Содержание работ	А) Формирование требований	1) Разработка деталей, схем и программных кодов	Б) Технический проект	2) Обследование объекта и создание обоснования необходимости системы	В) Рабочая документация	3) Разработка окончательных проектных решений по системе и её частям	
Стадия проектирования	Содержание работ								
А) Формирование требований	1) Разработка деталей, схем и программных кодов								
Б) Технический проект	2) Обследование объекта и создание обоснования необходимости системы								
В) Рабочая документация	3) Разработка окончательных проектных решений по системе и её частям								



1784080246

Содержание вопроса (задания)		Правильный ответ
При разработке технического проекта системы защиты информации соотнесите вид обеспечения (левая колонка) с его компонентами (правая колонка):		А - 2, Б - 3, В - 1.
Вид обеспечения СЗИ	Компоненты в проекте	
А) Программное обеспечение	1) Инструкции и интерфейсы администратора и регламенты управления доступом	
Б) Техническое обеспечение	2) Средства антивирусной защиты и операционные системы	
В) Организационное обеспечение	3) Межсетевые экраны, серверы и средства криптозащиты	
Текст задания: Расположите этапы проектирования подсистемы управления доступом в логическом порядке (от анализа к реализации): 1. 1. Определение перечня защищаемых информационных ресурсов. 2. 2. Выбор программно-аппаратных средств идентификации и аутентификации. 3. 3. Формирование матрицы доступа (назначение прав пользователям). 4. 4. Разработка регламентов и инструкций по управлению учетными записями.		1, 3, 2, 4.
Установите правильную последовательность действий при разработке раздела «Моделирование угроз» в составе технического проекта: 1. 1. Определение актуальных угроз безопасности информации. 2. 2. Описание характеристик объекта информатизации и его границ. 3. 3. Анализ потенциальных нарушителей (внутренних и внешних). 4. 4. Оценка возможных негативных последствий (ущерба).		2, 3, 1, 4.

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



1784080246

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 ответами 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. Мошак, Н. Н. Защищенные информационные системы : учебное пособие / Н. Н. Мошак, Л. К. Птицына. — Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2020. — 216 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/180099> (дата обращения: 01.04.2025). — Режим доступа: для авториз. пользователей.

2. Ксендзов, А. В. Защищенные системы передачи информации : учебное пособие / А. В. Ксендзов. — Рязань : РГРТУ, 2021 — Часть 1 — 2021. — 96 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/310535> (дата обращения: 01.04.2025). — Режим доступа: для авториз. пользователей.

3. Васин, Н. Н. Сети и системы передачи информации. Раздел 4. Безопасность сетей и систем передачи информации : учебное пособие / Н. Н. Васин. — Самара : ПГУТИ, 2023. — 180 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/411527> (дата обращения: 01.04.2025). — Режим доступа: для авториз. пользователей.

4. Васин, Н. Н. Сети и системы передачи информации. Раздел 1. Основы технологий сетей и систем передачи информации : учебное пособие / Н. Н. Васин. — Самара : ПГУТИ, 2021. — 113 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/411524> (дата обращения: 01.04.2025). — Режим доступа: для авториз.



1784080246

пользователей.

6.2 Дополнительная литература

1. Сети и системы передачи информации : учебное пособие (курс лекций) : направление подготовки 10.03.01 Информационная безопасность : [16+] / А. П. Жук, Д. В. Орёл, Е. П. Жук, Г. И. Линец ; Северо-Кавказский федеральный университет. – Ставрополь : Северо-Кавказский Федеральный университет (СКФУ), 2021. – 158 с. : ил., табл. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=712322> (дата обращения: 11.09.2026). – Библиогр. в кн. – Текст : электронный.

2. Костров, Б. В. Сети и системы передачи информации : учебник для студентов, обучающихся по профессиям и специальностям среднего профессионального образования / Б. В. Костров, В. Н. Ручкин ; Б. В. Костров, В. Н. Ручкин. – 5-е изд., стер. – Москва : Академия, 2025. – 288 с. с. – (Профессиональное образование). – URL: <https://academia-moscow.ru/reader/?id=997106> (дата обращения: 01.04.2025). – Текст : электронный.

3. Чернышев, Н. Н. Сети и системы передачи информации : методические указания / Н. Н. Чернышев, Т. В. Ниженец. — Москва : РТУ МИРЭА, 2023. — 24 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/331634> (дата обращения: 01.04.2025). — Режим доступа: для авториз. пользователей.

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: 01.04.2025). – 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. Справочная правовая система «КонсультантПлюс» <http://www.consultant.ru/>
7. Национальная электронная библиотека <https://rusneb.ru/>

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.

б) 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.

с) 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.



1784080246

8 Методические указания для обучающихся по освоению дисциплины "Проектирование систем (компонента системы) обеспечения информационной безопасности"

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, установленным в рабочей программе дисциплины (модуля), практики;

2.3 подготовка к промежуточной аттестации в соответствии с порядком, установленным 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 (компонента системы) обеспечения информационной безопасности", включая перечень программного обеспечения и информационных справочных систем

Для изучения дисциплины может использоваться следующее программное обеспечение:

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

10 Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине "Проектирование систем (компонента системы) обеспечения информационной безопасности"

Специально оборудованный кабинет №1147 представляет собой компьютерный класс обеспечивающий практическую подготовку в соответствии с направленностью (профилем) программы магистратуры 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 блоки MasteroMiddleMC05, IntelCorei510400 2.9GHz, 8GbRAM, 240GbSSD, DOS, программно-аппаратный комплекс для обнаружения компьютерных атак VipNet, средство доверенной загрузки (СДЗ) Соболев.

Специальное помещение для самостоятельной работы № 1211



1784080246

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;
проектор, экран настенный моторизованный.
Специальное помещение для самостоятельной работы № 3210
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.

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.



1784080246