

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 16:02:23

Дубинкин Дмитрий Михайлович

Рабочая программа дисциплины

Технологии 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.



1784080788

Рабочую программу составил:

ПОДПИСАНО ЭП КУЗГТУ

Подразделение: кафедра информационной безопасности

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

Дата: 17.07.2026 10:03:51

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 10:04:10

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 10:04:46

Прокопенко Евгения Викторовна



1784080788

1 Перечень планируемых результатов обучения по дисциплине "Технологии обеспечения информационной безопасности", соотнесенных с планируемыми результатами освоения образовательной программы

Освоение дисциплины направлено на формирование:
обще профессиональных компетенций:

ОПК-1 - Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание;

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:

Способен обосновывать требования к системе обеспечения информационной безопасности .

Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности .

Результаты обучения по дисциплине:

Знает технологии обеспечения информационной безопасности. Знает основные виды уязвимостей систем и угрозы информационной безопасности. Знает методы и средства обеспечения информационной безопасности, а также нормативную базу регламентирующую классификацию данных средств.

Знает принципы эксплуатации средств защиты информации. Знает методы тестирования средств защиты информационной безопасности.

Умеет обосновывать выбор средств защиты информации для противодействия конкретным угрозам. Умеет осуществлять подбор средств защиты информации в соответствии с заданными критериями. Умеет обосновывать требования к мерам обеспечения информационной безопасности в соответствии с нормативной базой. Умеет составлять техническое задание по обеспечению информационной безопасности на объекте с использованием сертифицированных ФСТЭК средств защиты информации.

Умеет осуществлять настройку режимов работы средств защиты информации в соответствии с определенными моделями угроз. Умеет разрабатывать сценарии тестирования средств защиты информации. Умеет разрабатывать требования к средствам защиты информации. Умеет управлять средствами защиты информации в соответствии с требованиями к объекту защиты.

Владеет опытом настройки средства защиты информации в соответствии с требованиями к объекту защиты с целью снижения рисков информационной безопасности.

Имеет опыт разработки требования к средствам и методам контроля проектируемой системы (подсистемы либо компонента системы) обеспечения информационной безопасности.

2 Место дисциплины "Технологии 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, Построение моделей угроз 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 "Технологии 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 "Технологии обеспечения информационной безопасности" составляет 4 зачетных единицы, 144 часа.



1784080788

Форма обучения	Количество часов		
	ОФ	ЗФ	ОЗФ
Курс 1/Семестр 2			
Всего часов			144
Контактная работа обучающихся с преподавателем (по видам учебных занятий):			
Аудиторная работа			
Лекции			
Лабораторные занятия			
Практические занятия			24
Внеаудиторная работа			
Индивидуальная работа с преподавателем:			
Консультация и иные виды учебной деятельности			
Самостоятельная работа под руководством преподавателя			40
Самостоятельная работа			80
Форма промежуточной аттестации			зачет

4 Содержание дисциплины "Технологии обеспечения информационной безопасности", структурированное по разделам (темам)

4.1. Практические (семинарские) занятия

Тема занятия	Трудоемкость в часах	
	ОФ	ОЗФ
1. Обеспечение защиты информации в операционных системах: Администрирование учетных записей в ОС Windows; Дискреционный механизм разграничения доступа к файловым объектам; Разграничение доступа к запуску программного обеспечения; Аудит событий безопасности операционной системы; Анализ, настройка и контроль целостности параметров безопасности подсистемы защиты; Многофакторная аутентификация с помощью физического объекта; Разграничение доступа к устройствам; Мандатный механизм разграничения доступа к файловым объектам; Разграничение доступа к запуску программного обеспечения; Аудит событий безопасности операционной системы; Управление системными службами и процессами в ОС Windows	6	6
2 Средства криптографической защиты информации: Криптографическая защита объектов файловой системы в ОС Windows; Применение шифрования и электронной подписи в электронном документообороте; Применение криптопровайдеров на автоматизированном рабочем месте; Применение средств криптографической защиты информации на автоматизированном рабочем месте; Изучение функций удостоверяющего центра	6	6
3 Обеспечение защиты информации в компьютерных сетях: Одноранговые сети; Настройка домена на примере Active Directory; DLP-системы; Межсетевые экраны; Виртуальные защищенные сети.	6	6
4 Управление средствами защиты информации: Применение средств защиты информации для контроля целостности ОС; Централизованная защита от вирусов в локальной сети	6	6
Итого	24	24



1784080788

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	30	30
Составление двуязычного глоссария к литературе по тематике научного исследования, предназначенной для внеаудиторного чтения;	44	44
Подготовка к промежуточной аттестации	6	6
Итого	80	80
Самостоятельная работа под руководством преподавателя	40	40

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 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 "Технологии обеспечения информационной безопасности"

5.1 Паспорт комплекта оценочных материалов

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



1784080788

Опрос по контрольным вопросам, подготовка отчетов по практическим и (или) лабораторным работам	ОПК-1	Способен обосновывать требования к системе обеспечения информационной безопасности	Знает технологии обеспечения информационной безопасности. Знает основные виды уязвимостей систем и угрозы информационной безопасности. Знает методы и средства обеспечения информационной безопасности, а также нормативную базу регламентирующую классификацию данных средств. Умеет обосновывать выбор средств защиты информации для противодействия конкретным угрозам. Умеет осуществлять подбор средств защиты информации в соответствии с заданными критериями. Умеет обосновывать требования к мерам обеспечения информационной безопасности в соответствии с нормативной базой. Умеет составлять техническое задание по обеспечению информационной безопасности на объекте с использованием сертифицированных ФСТЭК средств защиты информации. Владеет опытом настройки средства защиты информации в соответствии с требованиями к объекту защиты с целью снижения рисков информационной безопасности.	Высокий или средний
Опрос по контрольным вопросам, подготовка отчетов по практическим и (или) лабораторным работам	ОПК-2	Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности	Знает принципы эксплуатации средств защиты информации. Знает методы тестирования средств защиты информационной безопасности. Умеет осуществлять настройку режимов работы средств защиты информации в соответствии с определенными моделями угроз. Умеет разрабатывать сценарии тестирования средств защиты информации. Умеет разрабатывать требования к средствам защиты информации. Умеет управлять средствами защиты информации в соответствии с требованиями к объекту защиты. Имеет опыт разработки требования к средствам и методам контроля проектируемой системы (подсистемы либо компонента системы) обеспечения информационной безопасности	Высокий или средний



1784080788

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.

Например:

ОПК-1 Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание;

Содержание вопроса (задания)	Правильный ответ
Процесс выявления актуальных угроз и оценки вероятности их реализации, проводимый для обоснования состава системы защиты в проекте, называется _____.	моделированием угроз
Требования к СОИБ, описывающие конкретные защитные действия системы (например, фильтрация трафика или шифрование данных), называются _____.	функциональными требованиями

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

Содержание вопроса (задания)	Правильный ответ
Графический документ, отображающий состав подсистем защиты, их взаимную связь и распределение по узлам сети, называется _____ системы обеспечения ИБ.	структурная схема
Раздел технического проекта, содержащий перечень всех программных и аппаратных средств защиты с указанием их точных наименований, версий и количества, называется _____.	спецификация

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:



1784080788

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 зачет, в процессе которого 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 зачете 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	
Шкала оценивания	Не зачтено		Зачтено		

Примерный перечень вопросов на зачете:

ОПК-1 Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание;

Содержание вопроса (задания)	Правильный ответ
Процесс выявления актуальных угроз и оценки вероятности их реализации, проводимый для обоснования состава системы защиты в проекте, называется _____.	моделированием угроз
Требования к СОИБ, описывающие конкретные защитные действия системы (например, фильтрация трафика или шифрование данных), называются _____.	функциональными требованиями

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

Содержание вопроса (задания)	Правильный ответ
Графический документ, отображающий состав подсистем защиты, их взаимную связь и распределение по узлам сети, называется _____ системы обеспечения ИБ.	структурная схема
Раздел технического проекта, содержащий перечень всех программных и аппаратных средств защиты с указанием их точных наименований, версий и количества, называется _____.	спецификация



1784080788

Содержание вопроса (задания)	Правильный ответ
Технология создания защищенного логического канала поверх незащищенной сети (например, Интернета) для объединения офисов в единую сеть называется _____.	VPN (или виртуальная частная сеть).
Основной текстовый документ технического проекта, в котором приводится детальное описание и техническое обоснование всех принятых проектных решений, - это _____.	пояснительная записка.

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-1 Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание;

Содержание вопроса (задания)	Правильный ответ
Какой этап является определяющим при обосновании требований к системе обеспечения информационной безопасности (СОИБ) в техническом задании? 1. Закупка серверного оборудования. 2. Анализ рисков и моделирование угроз безопасности информации. 3. Назначение системного администратора. 4. Выбор цвета интерфейса программного обеспечения.	2
Каким государственным стандартом (ГОСТ) следует руководствоваться в первую очередь при разработке структуры и содержания технического задания на создание автоматизированной системы? 1. ГОСТ 2.105 (Общие требования к текстовым документам). 2. ГОСТ 34.602 (Техническое задание на создание автоматизированной системы). 3. ГОСТ Р 7.0.97 (Организационно-распорядительная документация). 4. ГОСТ 19.101 (Виды программных документов).	2
Установите соответствие технологий защиты и решаемых ими задач при обосновании проекта	А - 3, Б - 1, В - 2.
Технология защиты	
Основная задача обеспечения ИБ	
А VPN (Virtual Private Network)	
Б) IDS/IPS системы	
В) Межсетевой экран (Firewall)	



1784080788

Содержание вопроса (задания)		Правильный ответ
Установите соответствие видов угроз и технологий их нейтрализации для обоснования ТЗ		А - 2, Б - 3, В - 1.
Вид угрозы	Технология нейтрализации	
А) Несанкционированный доступ	1) Резервное копирование избыточное хранение (RAID)	
Б) Модификация данных	2) Многофакторная аутентификация и управление доступом	
В) Нарушение доступности	3) Использование электронной подписи (ЭП) и хэширования	
Установите правильную последовательность этапов разработки технического задания на создание системы обеспечения информационной безопасности (СОИБ) согласно ГОСТ 34.602: 1. Согласование и утверждение проекта ТЗ заказчиком и разработчиком. 2. Сбор и анализ исходных данных об объекте информатизации. 3. Формирование технических требований к подсистемам защиты. 4. Определение целей создания и назначения будущей системы.		2, 4, 3, 1.
Расположите действия инженера по обоснованию состава средств защиты в логической последовательности: 1. Выбор конкретных технологий защиты (шифрование, МЭ, антивирус). 2. Определение перечня актуальных угроз безопасности информации. 3. Сопоставление выбранных технологий с требованиями регуляторов (ФСТЭК/ФСБ). 4. Идентификация защищаемых активов и информационных потоков.		4, 2, 1, 3.

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

Содержание вопроса (задания)		Правильный ответ
Какой этап является первоочередным при обосновании состава требований к системе обеспечения информационной безопасности в проекте ТЗ? 1. Закупка лицензий на программное обеспечение. 2. Идентификация активов и моделирование угроз безопасности. 3. Назначение системного администратора организации. 4. Обучение пользователей работе с офисными программами.		2
В какой раздел технического задания (согласно ГОСТ 34.602) включаются требования по обеспечению конфиденциальности, целостности и доступности информации? 1. Общие сведения о проекте. 2. Порядок контроля и приемки системы. 3. Требования к системе (или подсистемам защиты). 4. Требования к документированию.		3
Установите соответствие классов средств защиты информации (СЗИ) и их проектных задач		А - 2, Б - 1, В - 3.
Класс СЗИ	Основная задача в техническом проекте	
А) СЗИ от несанкционированного доступа (НД)	1) Обнаружение и блокировка сетевых угроз на периметре	
Б) Межсетевой экран (МЭ)	2) Контроль доступа к файлам и устройствам внутри ОС	
В) Система обнаружения вторжений (СОВ)	3) Анализ сетевого трафика и обнаружение атак (сигнатурных и аномальных)	



1784080788

Содержание вопроса (задания)		Правильный ответ
Установите соответствие уровней архитектуры системы и применяемых технологий защиты		А - 3, Б - 1, В - 2.
Уровень системы	Технология защиты в проекте	
А) Сетевой уровень	1) Разграничение прав доступа к таблицам БД	
Б) Прикладной уровень	2) Проверка подлинности пользователя по биометрии	
В) Уровень идентификации	3) Организация защищённого туннеля (VPN)	
Расположите действия проектировщика по созданию подсистемы управления доступом в логическом порядке: 1. 1. Выбор метода аутентификации (пароль, токен, биометрия). 2. 2. Определение перечня защищаемых ресурсов и категорий пользователей. 3. 3. Описание правил разграничения доступа (матрица доступа). 4. 4. Проектирование механизмов регистрации (логирования) действий пользователей.		2, 3, 1, 4.
Установите последовательность этапов проектирования защищенного канала связи (VPN) между офисами: 1. 1. Выбор криптографических алгоритмов и протоколов (например, IPsec или TLS). 2. 2. Определение точек входа/выхода трафика (места установки шлюзов). 3. 3. Расчет необходимой пропускной способности канала с учетом шифрования. 4. 4. Описание порядка генерации и распределения ключей шифрования.		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 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.



1784080788

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. Импортзамещающие технологии обеспечения информационной безопасности и защиты данных : учебное пособие / Д. А. Короченцев, Л. В. Черкесова, Е. А. Ревякина [и др.]. — Ростов-на-Дону : Донской ГТУ, 2021. — 335 с. — ISBN 978-5-7890-1893-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/237782> (дата обращения: 31.03.2025). — Режим доступа: для авториз. пользователей.

2. Документальное обеспечение информационной безопасности : учебное пособие / составители Е. Е. Смычков [и др.]. — Севастополь : СевГУ, 2022. — 142 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/261899> (дата обращения: 31.03.2025). — Режим доступа: для авториз. пользователей.

3. Максуров, А. А. Обеспечение информационной безопасности в сети Интернет : монография / А.А. Максуров. — Москва : ИНФРА-М, 2025. — 226 с. — (Научная мысль). — DOI 10.12737/1942595. - ISBN 978-5-16-018251-3. - Текст : электронный. - URL: <https://znanium.ru/catalog/product/2171257> (дата обращения: 07.09.2026). - Режим доступа: по подписке.

4. Донгак, Ш. М. Организационное и правовое обеспечение информационной безопасности : учебное пособие / Ш. М. Донгак, Н. М. Хади. — Москва : РТУ МИРЭА, 2024. — 74 с. — ISBN 978-5-7339-2307-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/448901> (дата обращения: 31.03.2025). — Режим доступа: для авториз. пользователей.



1784080788

6.2 Дополнительная литература

1. Дронов, В. Ю. Бизнес-процесс «Обеспечение информационной безопасности организации» : учебное пособие / В. Ю. Дронов, Г. А. Дронова. — Новосибирск : НГТУ, 2021. — 76 с. — ISBN 978-5-7782-4537-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/306350> (дата обращения: 31.03.2025). — Режим доступа: для авториз. пользователей.

2. Медведев, Н. В. Дипломное проектирование по специальности «Комплексное обеспечение информационной безопасности автоматизированных систем» : методические указания : методическое пособие : [16+] / Н. В. Медведев, П. М. Квасов ; под ред. В. А. Матвеева ; Московский государственный технический университет им. Н.Э. Баумана. — Москва : МГТУ им. Н.Э. Баумана, 2011. — 80 с. : табл. — Режим доступа: по подписке. — URL: <https://biblioclub.ru/index.php?page=book&id=256990> (дата обращения: 12.09.2026). — Текст : электронный.

3. Полякова, Т. А. Организационное и правовое обеспечение информационной безопасности: учебник для вузов / Полякова Т. А., Стрельцов А. А., Чубукова С. Г., Ниесов В. А. ; Под ред. Поляковой Т. А., Стрельцова А. А.. — 2-е изд., пер. и доп. — Москва : Юрайт, 2025. — 357 с. — ISBN 978-5-534-19108-0. — URL: <https://urait.ru/book/organizacionnoe-i-pravovoe-obespechenie-informacionnoy-bezopasnosti-560516> (дата обращения: 31.03.2025). — Текст : электронный.

4. Ищейнов, В. Я. Организационное и техническое обеспечение информационной безопасности. Защита конфиденциальной информации : учебное пособие / В.Я. Ищейнов, М.В. Мецатунян. — Москва : ИНФРА-М, 2024. — 256 с. — (Высшее образование: Специалист). — ISBN 978-5-16-016535-6. — Текст : электронный. — URL: <https://znanium.ru/catalog/product/2139841> (дата обращения: 07.09.2026). — Режим доступа: по подписке.

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: 31.03.2025). — 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. Электронная библиотечная система «Znanium» <https://new.znanium.com/my/documents>
7. Справочная правовая система «КонсультантПлюс» <http://www.consultant.ru/>
8. 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.



1784080788

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.

8 Методические указания для обучающихся по освоению дисциплины "Технологии 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, 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 "Технологии 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. Kaspersky Endpoint Security
6. Браузер Спутник

10 Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине "Технологии обеспечения информационной безопасности"

Специальное помещение № 3217 представляет собой учебную аудиторию для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации

Перечень основного оборудования:

специализированная мебель (столы и стулья);

технические средства обучения, служащие для представления учебной информации большой аудитории (ноутбук, переносной проектор, переносной экран);

наборы демонстрационного оборудования и учебно-наглядных пособий, обеспечивающие тематические иллюстрации;

сетевая рабочая станция;

кафедра напольная 760*600*1250мм.;



1784080788

проектор Acer X1260;
проекционный экран Projecta;
доска классная;
вешалка (доска для одежды).
Специальное помещение для самостоятельной работы № 1211
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.



1784080788