

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 15:58:20

Дубинкин Дмитрий Михайлович

Программа практики

Вид практики: Производственная

Тип практики: Организационно-управленческая практика

Способ проведения: стационарная и(или) выездная

Направление подготовки 10.04.01 Информационная безопасность

Направленность(профиль) подготовки 01 Организация и технология защиты информации»

Присваиваемая квалификация

"Магистр"

Формы обучения

очно-заочная

Кемерово 2025 г.



1784087278

Определения, сокращения и аббревиатуры

В данной программе практики приняты следующие сокращения:

ВКР – выпускная квалификационная работа;

ЗЕ – зачетная единица;

НЕУД – неудовлетворительно;

ОПОП – основная профессиональная образовательная программа;

ОТЛ – отлично;

ОФ – очная форма обучения;

ОЗФ – очно-заочная форма обучения;

ПК – профессиональная компетенция;

УД – удовлетворительно;

ХОР – хорошо.



1784087278

Рабочую программу составил:

ПОДПИСАНО ЭП КУЗГТУ

Подразделение: кафедра информационной безопасности

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

Дата: 17.07.2026 10:20:39

Прокопенко Евгения Викторовна

Рабочая программа обсуждена на заседании кафедры информационной безопасности

Протокол № от 15.09.2026

ПОДПИСАНО ЭП КУЗГТУ

Подразделение: кафедра информационной безопасности

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

Дата: 17.07.2026 10:20:56

Прокопенко Евгения Викторовна

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

Протокол № от 15.09.2026

ПОДПИСАНО ЭП КУЗГТУ

Подразделение: кафедра информационной безопасности

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

Дата: 17.07.2026 10:21:14

Прокопенко Евгения Викторовна



1784087278

1 Формы и способы проведения практики

Способ проведения практики: стационарная и(или) выездная.

Форма проведения практики: непрерывно - путем выделения в календарном учебном графике непрерывного периода учебного времени для проведения всех видов практик, предусмотренных ОПОП ВО.

Тип практики: Организационно-управленческая практика.

2 Перечень планируемых результатов обучения при прохождении практики,соотнесенных с планируемыми результатами освоения ОПОП

Освоение дисциплины направлено на формирование:
профессиональных компетенций:

ПК-3 - Владеет нормативно-методической базой обеспечения защиты сведений, составляющих государственную тайну

ПК-4 - Способен организовывать и сопровождать аттестацию объектов вычислительной техники и выделенных (защищаемых) помещений на соответствие требованиям по защите информации

ПК-5 - Способен организовывать и проводить приемочные испытания СЗИ, вводить в эксплуатацию СЗИ

ПК-6 - Прогнозирует риски в информационной безопасности и управляет инцидентами информационной безопасности

универсальных компетенций:

УК-2 - Способен управлять проектом на всех этапах его жизненного цикла

УК-3 - Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели

Результаты обучения по дисциплине определяются индикаторами достижения компетенций

Индикатор(ы) достижения:

Управлять проектом на создание СЗИ.

Организует работу персонала службы информационной безопасности по подготовке проекта организационно-распорядительной документации на системы защиты информации.

Владеет нормативно-методической базой обеспечения защиты сведений, составляющих государственную тайну.

Организует и сопровождает аттестацию объектов вычислительной техники и выделенных защищаемых помещений на соответствие требованиям по защите информации.

Организует и проводит приемочные испытания СЗИ, вводит в эксплуатацию СЗИ.

Прогнозирует риски в информационной безопасности и управляет инцидентами информационной безопасности.

Результаты обучения по дисциплине:

Знать нормативные акты и стандарты в области управления проектами по разработке систем информационной безопасности.

Знать основы трудового законодательства, требования ДИ работников службы информационной безопасности.

Знать нормативную базу для обеспечения защиты сведений, составляющих государственную тайну.

Знать порядок аттестации объектов информатизации на соответствие требованиям по защите информации.

Знать методы защиты информации от утечки, эксплуатационную документацию на систему защиты информации.

Знать количественный и качественный подходы к оценке рисков ИБ.

Иметь опыт построения систем управления проектами по разработке системы информационной безопасности информационных систем в условиях применения современных информационных технологий.

Иметь опыт организации обучения персонала использованию технических, программных (программно-технических) средств защиты информации.

Иметь опыт подготовки нормативно-методической базы.

Иметь опыт организации подготовки объектов вычислительной техники и выделенных (защищаемых) помещений к аттестации по требованиям безопасности информации.



1784087278

Иметь опыт организации приемочных испытаний систем защиты информации.

Иметь опыт определения риска в информационной безопасности и управления инцидентами информационной безопасности.

Уметь моделировать риски.

Уметь организовывать работу команды по подготовке проекта организационно-распорядительной документации на системы защиты информации.

Уметь использовать полученные знания в профессиональной деятельности.

Уметь подготавливать объекты вычислительной техники и выделенные (защищаемые) помещения к аттестации по требованиям безопасности информации.

Уметь организовывать приемочные испытания системы защиты информации

Уметь проводить качественную оценку рисков, определять вероятность реализации угрозы по отношению к информационному активу, определять уровень возможности успешной реализации угрозы с учетом текущего состояния ИБ, внедренных мер и средств защиты.

Владеть пониманием структуры и системы взаимосвязи процессов управления.

Владеть методами организации мер, обеспечивающих эффективность системы защиты информации.

Владеть нормативно-методической базой обеспечения защиты сведений, составляющих государственную тайну.

Владеть методами подготовки объектов вычислительной техники и выделенных (защищаемых) помещений к аттестации.

Владеть способами приемочных испытаний СЗИ, ввода в эксплуатацию СЗИ.

Владеть методами разработки мер безопасности, контрмер и действий по каждой актуальной угрозе для снижения уровня риска, управлять инцидентами

- информационной безопасности.

3 Место практики в структуре ОПОП магистратуры

Практика входит в формируемую участниками образовательного процесса часть Блока 2 «Практики» ОПОП.

Для формирования компетенций, указанных в пункте 2, в процессе прохождения практики необходимо владеть сформированными результатами обучения, полученными в результате освоения дисциплин (модулей), прохождения практики, входящих в состав обязательной и формируемой участниками образовательного процесса части образовательной программы, предшествующих прохождению практики.

4 Объем практики и ее продолжительность

Общий объем практики составляет 15 зачетных единиц.

Общий объем практики составляет 540 часов.

5 Содержание практики

№ п/п	Этапы практики	Виды учебной работы	Часы
3 семестр			
1	Начальный этап Организационное собрание: задачи и краткое содержание практики, требования к текущему контролю и промежуточной аттестации, инструктаж по ТБ. Проведение учебных занятий в лабораториях КузГТУ и(или) в профильных организациях на основании договора о практической подготовке.	Ознакомление с задачами, содержанием практики. Ознакомление с организационно-управленческой структурой предприятия и его подразделений. Ознакомление с реализуемыми на предприятии мероприятиями по организации и технологиям защиты информации	18



1784087278

2	Основной этап Методы и средства управления информационной безопасностью предприятия. Организация управления информационной безопасностью, проектирование систем (компонент системы) обеспечения информационной безопасности, работа с организационно-распорядительной документацией по обеспечению информационной безопасности.	Сбор и изучение материалов. Изучение и оформление проектов организационно-управленческого документооборота. Подготовка материалов к промежуточной аттестации по практике. Разработка эксплуатационной и организационно-распорядительной документации на системы защиты информации. Организация работы персонала службы информационной безопасности по подготовке проекта организационно-распорядительной документации на системы защиты информации. Прогнозирует риски в информационной безопасности и управляет инцидентами информационной безопасности Подбор нормативно-методической базой обеспечения защиты сведений, составляющих государственную тайну.	180
3	Заключительный этап Оформление и защита подготовленного итогового материала в виде презентации	Обработка и систематизация фактического и литературного материала, теоретическая подготовка к промежуточной аттестации по практике.	18
Итого			216
4 семестр			
1	Начальный этап Организационное собрание: задачи и краткое содержание практики, требования к текущему контролю и промежуточной аттестации, инструктаж по ТБ. Проведение учебных занятий в лабораториях КузГТУ и(или) в профильных организациях на основании договора о практической подготовке.	Ознакомление с задачами, содержанием практики. Ознакомление с организационно-управленческой структурой предприятия и его подразделений. Ознакомление с реализуемыми на предприятии мероприятиями по организации и технологиям защиты информации	18
2	Основной этап Методы и средства управления информационной безопасностью предприятия. Организация управления информационной безопасностью, проектирование систем (компонент системы) обеспечения информационной безопасности, работа с организационно-распорядительной документацией по обеспечению информационной безопасности.	Сбор и изучение материалов. Изучение и оформление проектов организационно-управленческого документооборота. Подготовка материалов к промежуточной аттестации по практике. Организация и сопровождение аттестации объектов вычислительной техники и выделенных защищаемых помещений на соответствие требованиям по защите информации. Организует и проведение приемочных испытаний СЗИ, ввод в эксплуатацию СЗИ. Управляет проектом на создание СЗ. Прогноз рисков в информационной безопасности и управление инцидентами информационной безопасности	288
3	Заключительный этап Оформление и защита подготовленного итогового материала в виде презентации	Обработка и систематизация фактического и литературного материала, теоретическая подготовка к промежуточной аттестации по практике.	18
Итого			324

В процессе практики каждый обучающийся выполняет индивидуальное задание, посвященное поиску, обобщению и анализу информации по заданной теме, а также выполняет разработку программы, обеспечивающей решение поставленной задачи. Организация проведения практики осуществляется на основе договоров, заключаемых Университетом с организациями, деятельность которых соответствует профессиональным компетенциям, осваиваемым в рамках образовательной программы.



1784087278

Практика может быть проведена непосредственно в Университете и его структурных подразделениях.

Для руководства практикой, проводимой в Университете и его структурных подразделениях, назначается руководитель (руководители) практики из числа лиц, относящихся к профессорско-преподавательскому составу Университета.

Для руководства практикой, проводимой в профильной организации, назначаются руководитель (руководители) практики из числа лиц, относящихся к профессорско-преподавательскому составу Университета, и руководитель (руководители) от профильной организации из числа работников профильной организации.

Руководитель практики из числа лиц, относящихся к профессорско-преподавательскому составу Университета:

1. составляет рабочий график (план) проведения практики;
2. разрабатывает индивидуальные задания для обучающихся, выполняемые в период практики;
3. участвует в распределении обучающихся по рабочим местам и видам работ в организации;
4. осуществляет контроль за соблюдением сроков проведения практики и соответствием ее содержания требованиям, установленным ОПОП;
5. оказывает методическую помощь обучающимся при выполнении ими индивидуальных заданий;- оценивает результаты прохождения практики обучающимися.

Руководитель практики от профильной организации:

1. согласовывает индивидуальные задания, содержание и планируемые результаты практики;
2. предоставляет рабочие места обучающимся;
3. обеспечивает безопасные условия прохождения практики обучающимся, отвечающие санитарным правилам и требованиям охраны труда;
4. проводит инструктаж обучающихся по ознакомлению с требованиями охраны труда, промышленной безопасности, пожарной безопасности, а также правилами внутреннего трудового распорядка.

При проведении практики в профильной организации руководителем практики от Университета и руководителем практики от профильной организации составляется совместный рабочий график (план) проведения практики. Обучающиеся в период прохождения практики:

1. выполняют индивидуальные задания;
2. соблюдают правила внутреннего трудового распорядка;
3. соблюдают требования охраны труда и пожарной безопасности.

6 Формы отчетности по практике

Формой текущего контроля по результатам прохождения практики является собеседование по материалам, собранным в результате прохождения Подготовительного и производственного этапов практики (доклад по результатам завершения каждого этапа практики (защита разделов отчета по практике)) в день, завершающий прохождение каждого этапа практик.

Формой промежуточной аттестации по итогам прохождения практики является дифференцированный зачет, который проводится после завершения прохождения Заключительного этапа практики, в последний день прохождения практики в соответствии с календарным учебным графиком. На промежуточной аттестации обучающийся представляет доклад по итогам подготовленного в процессе прохождения практики отчета по результатам практики (защита отчета).

7 Фонд оценочных средств для проведения промежуточной аттестации обучающихся по практике

7.1 Паспорт комплекта оценочных материалов

Планируемые результаты обучения по дисциплине (модулю)

Практика направлена на формирование следующих компетенций выпускника:



1784087278

Форма(ы) текущего контроля	Компетенции, формируемые в результате освоения дисциплины (модуля)	Индикатор(ы) достижения компетенции	Результаты обучения по дисциплине (модулю)	Уровень
3 семестр				
собеседование по материалам, собранным в результате прохождения каждого этапа практики	ПК-3	Владеет нормативно-методической базой обеспечения защиты сведений, составляющих государственную тайну	Знать нормативную базу для обеспечения защиты сведений, составляющих государственную тайну. Уметь использовать полученные знания в профессиональной деятельности. Владеть нормативно-методической базой обеспечения защиты сведений, составляющих государственную тайну. Иметь опыт подготовки нормативно-методической базы.	Высокий или средний
собеседование по материалам, собранным в результате прохождения каждого этапа практики	УК-3	Организует работу персонала службы информационной безопасности по подготовке проекта организационно-распорядительной документации на системы защиты информации.	Знать основы трудового законодательства, требования ДИ к работникам службы информационной безопасности. Уметь организовывать работу команды по подготовке проекта организационно-распорядительной документации на системы защиты информации. Владеть методами организации мер, обеспечивающих эффективность системы защиты информации. Иметь опыт организации обучения персонала использованию технических, программных (программно-технических) средств защиты информации.	Высокий или средний
собеседование по материалам, собранным в результате прохождения каждого этапа практики	ПК-6	Прогнозирует риски в информационной безопасности и управляет инцидентами информационной безопасности	Знать количественный и качественный подходы к оценке рисков ИБ. Уметь проводить качественную оценку рисков, определять вероятность реализации угрозы по отношению к информационному активу, определять уровень возможности успешной реализации угрозы с учетом текущего состояния ИБ, внедренных мер и средств защиты. Владеть методами разработки мер безопасности, контрмер и действий по каждой актуальной угрозе для снижения уровня риска, управлять инцидентами информационной безопасности. Иметь опыт определения риска в информационной безопасности и управления инцидентами информационной безопасности.	Высокий или средний
4 семестр				



1784087278

собеседование по материалам, собранным в результате прохождения каждого этапа практики	ПК-4	Организует и сопровождает аттестацию объектов вычислительной техники и выделенных защищаемых помещений на соответствие требованиям по защите информации	Знать порядок аттестации объектов информатизации на соответствие требованиям по защите информации. Уметь подготавливать объекты вычислительной техники и выделенные (защищаемые) помещения к аттестации по требованиям безопасности информации. Владеть методами подготовки объектов вычислительной техники и выделенных (защищаемых) помещений к аттестации. Иметь опыт организации подготовки объектов вычислительной техники и выделенных (защищаемых) помещений к аттестации по требованиям безопасности информации.	Высокий или средний
собеседование по материалам, собранным в результате прохождения каждого этапа практики	ПК-5	Организует и проводит приемочные испытания СЗИ, вводит в эксплуатацию СЗИ	Знать методы защиты информации от утечки, эксплуатационную документацию на систему защиты информации. Уметь организовывать приемочные испытания системы защиты информации Владеть способами приемочных испытаний СЗИ, ввода в эксплуатацию СЗИ. Иметь опыт организации приемочных испытаний систем защиты информации.	Высокий или средний
собеседование по материалам, собранным в результате прохождения каждого этапа практики	УК-2	Управлять проектом на создание СЗИ	Знать нормативные акты и стандарты в области управления проектами по разработке систем информационной безопасности. Уметь моделировать риски. Владеть пониманием структуры и системы взаимосвязи процессов управления. Иметь опыт построения систем управления проектами по разработке системы информационной безопасности информационных систем в условиях применения современных информационных технологий.	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.				

7.2. 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.

7.2.1. Оценочные материалы при текущем контроле

Формой текущего контроля по результатам прохождения производственной практике является собеседование по материалам, собранным в результате прохождения каждого этапа практики. Текущий контроль успеваемости обучающихся может быть организован с использованием ресурсов



1784087278

ЭИОС КузГТУ.

Примерные вопросы собеседования:

УК-2 Способен управлять проектом на всех этапах его жизненного цикла

Вопрос	Ключ ответа
На этапе завершения проекта по созданию защищенной системы Заказчик подписал все акты, но требует бесплатно добавить в систему функцию, которой не было в Техническом задании (ТЗ). Как поступить менеджеру проекта? 1. Бесплатно выполнить требование Заказчика, чтобы не портить с ним отношения. 2. Отказать Заказчику в грубой форме, сославшись на закрытие проекта. 3. Объяснить Заказчику, что проект завершен согласно ТЗ, и предложить оформить новое требование как отдельный проект (или через процедуру управления изменениями). 4. В тайне от руководства поручить программистам дописать требуемую функцию.	3 Управление жизненным циклом проекта требует жесткого соблюдения его границ. Выполнение работ вне ТЗ без оформления доп. соглашений ведет к неконтролируемым затратам ресурсов.
Во время этапа планирования проекта внедрения СЗИ выяснилось, что выделенного бюджета не хватает на закупку сертифицированного оборудования. Ваши действия? 1. Закупить более дешевое несертифицированное оборудование и скрыть это от Заказчика. 2. Инициировать совещание со стейкхолдерами для пересмотра бюджета проекта или сокращения его масштаба (границ) без потери качества защиты. 3. Начать проект и надеяться, что в процессе появятся дополнительные деньги. 4. Поручить разработчикам написать бесплатный аналог СЗИ своими силами за те же сроки.	2 На этапе планирования при обнаружении дефицита бюджета менеджер обязан вынести проблему на уровень спонсоров/заказчиков проекта для принятия стратегического решения, а не идти на нарушение требований безопасности.

УК-3 Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели

Вопрос	Ключ ответа
Команда из 5 специалистов должна за неделю провести аудит безопасности крупного филиала. Из-за сжатых сроков в коллективе началась паника. Какую стратегию руководства выбрать? 1. Сказать команде работать по 14 часов в сутки без выходных. 2. Разбить крупную цель на мелкие ежедневные задачи, распределить зоны ответственности согласно сильным сторонам сотрудников и проводить утренние 10-минутные летучки. 3. Выполнить большую часть работы самостоятельно, чтобы показать пример. 4. Отменить аудит и доложить руководству, что сроки нереальные.	2 Эффективное руководство командой в условиях стресса требует декомпозиции целей и четкого распределения ролей, что снижает неопределенность и структурирует работу коллектива.



1784087278

В вашей проектной команде опытный инженер-проектировщик отказывается документировать свои решения, заявляя, что «и так всё работает, а писанина – пустая трата времени». Ваши действия как лидера? 1. Уволить инженера за невыполнение требований. 2. Согласиться с ним, так как работающая система важнее бумаг. 3. Объяснить инженеру системные риски для всей команды в случае его ухода или болезни и сделать документирование обязательным критерием приемки его работы. 4. Поручить документирование за него менее опытному стажеру.	3 Лидер команды должен выработать общие правила игры. Документирование - это не бюрократия, а обеспечение непрерывности процессов и снижение зависимости команды от одного человека.
--	---

ПК-3 Владеет нормативно-методической базой обеспечения защиты сведений, составляющих государственную тайну

Вопрос	Ключ ответа
В ходе проверки архива в режимно-секретном подразделении (РСП) вы обнаружили флеш-накопитель с грифом «Секретно», лежащий на обычном рабочем столе в конце рабочего дня. Что требуют нормы СТР и Инструкции № 3-1? 1. Оставить флешку на месте, так как посторонних в помещении нет. 2. Немедленно изъять флеш-накопитель, поместить его в опечатываемый сейф и доложить руководству РСП о нарушении режима секретности. 3. Забрать флешку себе домой, чтобы она точно не пропала. 4. Положить флешку в карман и утром незаметно вернуть владельцу.	2 Нормативная база жестко регламентирует хранение носителей сведений, составляющих гостайну. В нерабочее время они обязаны находиться исключительно в опечатываемых сейфах спец. хранилищ.
Сотрудник просит скопировать файл с грифом «Секретно» на свой личный смартфон, чтобы поработать с документом дома. Каков ваш ответ на основе требований регуляторов? 1. Разрешить, если он пообещает никому не показывать этот файл. 2. Разрешить, если предварительно зашифровать файл паролем. 3. Категорически запретить, так как обработка секретных сведений на неаттестованных личных устройствах и их вынос за пределы контролируемой зоны запрещены. 4. Разрешить только в том случае, если на смартфоне установлен антивирус.	3 Защита гостайны строится на изоляции информации внутри аттестованного периметра. Вынос информации на неконтролируемые устройства образует критический канал утечки.

ПК-4 Способен организовывать и сопровождать аттестацию объектов вычислительной техники и выделенных (защищаемых) помещений на соответствие требованиям по защите информации

Вопрос	Ключ ответа
При сопровождении аттестации АС выяснилось, что на поставляемые серверы отсутствуют формуляры и сертификаты соответствия ФСТЭК России. Ваши действия? 1. Попросить аттестационную комиссию поверить вам на слово. 2. Приостановить процедуру аттестации и официально затребовать у поставщика или производителя недостающие формуляры и копии действующих сертификатов. 3. Скачать похожие сертификаты из Интернета и вставить туда названия своих серверов. 4. Сказать, что для внутренней сети сертификаты не нужны.	2 Сопровождение аттестации требует обеспечения легитимности всех СЗИ и средств обработки информации. Отсутствие обязательных документов делает аттестацию невозможной.



1784087278

Орган по аттестации в ходе испытаний выявил, что длина паролей пользователей в системе составляет всего 4 символа (вместо 8 по ТЗ). Как должен поступить сопровождающий? 1. Доказывать комиссии, что 4 символа — это очень удобно для сотрудников. 2. Изменить текст ТЗ прямо во время проверки, снизив планку до 4 символов. 3. Признать несоответствие, оперативно перенастроить парольную политику на сервере до требуемых 8 символов и продемонстрировать исправление комиссии. 4. Предложить комиссии взятку за игнорирование этого пункта.	3 Задача сопровождающего — содействовать успешному прохождению аттестации путем оперативного устранения выявленных недочетов, если они носят конфигурационный характер.
---	---

ПК-5 Способен организовывать и проводить приемочные испытания СЗИ, вводить в эксплуатацию СЗИ

Вопрос	Ключ ответа
При приемочных испытаниях системы контроля доступа (СКУД) выяснилось, что при отключении электропитания все замки на дверях остаются заблокированными, препятствуя эвакуации. Какое решение принять? 1. Принять систему, так как это обеспечивает максимальный уровень защиты от злоумышленников. 2. Отклонить приемку СЗИ и выставить требование подрядчику настроить автоматическую разблокировку замков при пропадании питания или срабатывании пожарной тревоги. 3. Принять систему и выдать всем сотрудникам по топору на случай пожара. 4. Изменить ТЗ, указав, что эвакуация из здания не предусмотрена.	2 Приемочные испытания систем физической и информационной безопасности не должны противоречить нормам охраны труда и пожарной безопасности.
Вы успешно завершили все тесты межсетевого экрана по Программе и методике испытаний (ПМИ). Что является финальным шагом для его ввода в промышленную эксплуатацию? 1. Устное поздравление команды инженеров. 2. Отправка электронного письма всем сотрудникам о том, что теперь всё защищено. 3. Подписание Акта завершения приемочных испытаний членами комиссии и издание руководителем Приказа о вводе СЗИ в эксплуатацию. 4. Перезагрузка межсетевого экрана.	3 Официальный ввод СЗИ в эксплуатацию на предприятии — это юридически значимое действие, требующее документальной фиксации ответственности в виде актов и приказов.

ПК-6 Прогнозирует риски в информационной безопасности и управляет инцидентами информационной безопасности

Вопрос	Ключ ответа
Антивирусная система на сервере внезапно начала фиксировать массовое и быстрое изменение расширений сотен файлов на ".locked". Спрогнозируйте риск и выберите действие. 1. Это плановое архивирование данных системой; ничего делать не нужно. 2. Риск поломки жесткого диска; нужно немедленно перезагрузить сервер. 3. Риск атаки вируса-шифровальщика; необходимо немедленно изолировать сервер от сети и остановить подозрительные процессы. 4. Риск сбоя в базе данных; нужно запустить проверку диска.	3 Прогнозирование рисков позволяет вовремя распознать паттерн поведения шифровальщика. Первым шагом локализации инцидента является отключение от сети для спасения остальных узлов инфраструктуры.



1784087278

При прогнозировании рисков вы понимаете, что единственный системный администратор компании знает все пароли наизусть и нигде их не фиксирует. Какое управленческое решение снизит этот риск? 1. Заставить администратора сдать экзамен на память. 2. Уволить администратора, пока он ничего не забыл. 3. Внедрить систему управления паролями (менеджер паролей) с разделением прав и регламентировать обязательное документирование учетных записей. 4. Ничего не делать, так как администратор работает в компании уже 10 лет.	3 Снижение риска потери критических знаний и монополизации доступа достигается за счет внедрения специализированных инструментов хранения паролей и регламентации процессов документирования.
--	--

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

Тематика индивидуальных заданий на практику:

3 семестр

1. Разработка эксплуатационной и организационно-распорядительной документации на системы защиты информации.
2. Подбор нормативно-методической базой обеспечения защиты сведений, составляющих государственную тайну.

4 семестр

1. Организация и сопровождение аттестации объектов вычислительной техники и выделенных защищаемых помещений на соответствие требованиям по защите информации.
2. Организация и проведение приемочных испытаний СЗИ, ввод в эксплуатацию СЗИ.
3. Организация работы персонала службы информационной безопасности по подготовке проекта организационно-распорядительной документации на системы защиты информации.
4. Прогноз рисков в информационной безопасности и управление инцидентами информационной безопасности

7.2.2. Оценочные материалы при промежуточной аттестации

Формой промежуточной аттестации является дифференцированный зачет, который проводится после завершения прохождения Заключительного этапа практики, в последний день прохождения практики в соответствии с календарным учебным графиком.

На промежуточной аттестации обучающийся проходит опрос по контрольным вопросам и (или) проходит тестирование.

Аттестационное испытание может быть организовано с использованием ресурсов ЭИОС КузГТУ.

В процессе промежуточной аттестации устанавливается сформированность запланированных результатов прохождения практики, сформированность компетенций, указанных в п. 1 настоящей программы практики

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



1784087278

- 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		

Примерные вопросы собеседования:

УК-2 Способен управлять проектом на всех этапах его жизненного цикла

Вопрос	Ключ ответа
На этапе завершения проекта по созданию защищенной системы Заказчик подписал все акты, но требует бесплатно добавить в систему функцию, которой не было в Техническом задании (ТЗ). Как поступить менеджеру проекта? 1. Бесплатно выполнить требование Заказчика, чтобы не портить с ним отношения. 2. Отказать Заказчику в грубой форме, сославшись на закрытие проекта. 3. Объяснить Заказчику, что проект завершен согласно ТЗ, и предложить оформить новое требование как отдельный проект (или через процедуру управления изменениями). 4. В тайне от руководства поручить программистам дописать требуемую функцию.	3 Управление жизненным циклом проекта требует жесткого соблюдения его границ. Выполнение работ вне ТЗ без оформления доп. соглашений ведет к неконтролируемым затратам ресурсов.
Во время этапа планирования проекта внедрения СЗИ выяснилось, что выделенного бюджета не хватает на закупку сертифицированного оборудования. Ваши действия? 1. Закупить более дешевое несертифицированное оборудование и скрыть это от Заказчика. 2. Инициировать совещание со стейкхолдерами для пересмотра бюджета проекта или сокращения его масштаба (границ) без потери качества защиты. 3. Начать проект и надеяться, что в процессе появятся дополнительные деньги. 4. Поручить разработчикам написать бесплатный аналог СЗИ своими силами за те же сроки.	2 На этапе планирования при обнаружении дефицита бюджета менеджер обязан вынести проблему на уровень спонсоров/заказчиков проекта для принятия стратегического решения, а не идти на нарушение требований безопасности.

УК-3 Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели

Вопрос	Ключ ответа
Команда из 5 специалистов должна за неделю провести аудит безопасности крупного филиала. Из-за сжатых сроков в коллективе началась паника. Какую стратегию руководства выбрать? 1. Сказать команде работать по 14 часов в сутки без выходных. 2. Разбить крупную цель на мелкие ежедневные задачи, распределить зоны ответственности согласно сильным сторонам сотрудников и проводить утренние 10-минутные летучки. 3. Выполнить большую часть работы самостоятельно, чтобы показать пример. 4. Отменить аудит и доложить руководству, что сроки нереальные.	2 Эффективное руководство командой в условиях стресса требует декомпозиции целей и четкого распределения ролей, что снижает неопределенность и структурирует работу коллектива.



1784087278

В вашей проектной команде опытный инженер-проектировщик отказывается документировать свои решения, заявляя, что «и так всё работает, а писанина – пустая трата времени». Ваши действия как лидера? 1. Уволить инженера за невыполнение требований. 2. Согласиться с ним, так как работающая система важнее бумаг. 3. Объяснить инженеру системные риски для всей команды в случае его ухода или болезни и сделать документирование обязательным критерием приемки его работы. 4. Поручить документирование за него менее опытному стажеру.	3 Лидер команды должен выработать общие правила игры. Документирование - это не бюрократия, а обеспечение непрерывности процессов и снижение зависимости команды от одного человека.
--	---

ПК-3 Владеет нормативно-методической базой обеспечения защиты сведений, составляющих государственную тайну

Вопрос	Ключ ответа
В ходе проверки архива в режимно-секретном подразделении (РСП) вы обнаружили флеш-накопитель с грифом «Секретно», лежащий на обычном рабочем столе в конце рабочего дня. Что требуют нормы СТР и Инструкции № 3-1? 1. Оставить флешку на месте, так как посторонних в помещении нет. 2. Немедленно изъять флеш-накопитель, поместить его в опечатываемый сейф и доложить руководству РСП о нарушении режима секретности. 3. Забрать флешку себе домой, чтобы она точно не пропала. 4. Положить флешку в карман и утром незаметно вернуть владельцу.	2 Нормативная база жестко регламентирует хранение носителей сведений, составляющих гостайну. В нерабочее время они обязаны находиться исключительно в опечатываемых сейфах спец. хранилищ.
Сотрудник просит скопировать файл с грифом «Секретно» на свой личный смартфон, чтобы поработать с документом дома. Каков ваш ответ на основе требований регуляторов? 1. Разрешить, если он пообещает никому не показывать этот файл. 2. Разрешить, если предварительно зашифровать файл паролем. 3. Категорически запретить, так как обработка секретных сведений на неаттестованных личных устройствах и их вынос за пределы контролируемой зоны запрещены. 4. Разрешить только в том случае, если на смартфоне установлен антивирус.	3 Защита гостайны строится на изоляции информации внутри аттестованного периметра. Вынос информации на неконтролируемые устройства образует критический канал утечки.

ПК-4 Способен организовывать и сопровождать аттестацию объектов вычислительной техники и выделенных (защищаемых) помещений на соответствие требованиям по защите информации

Вопрос	Ключ ответа
При сопровождении аттестации АС выяснилось, что на поставляемые серверы отсутствуют формуляры и сертификаты соответствия ФСТЭК России. Ваши действия? 1. Попросить аттестационную комиссию поверить вам на слово. 2. Приостановить процедуру аттестации и официально затребовать у поставщика или производителя недостающие формуляры и копии действующих сертификатов. 3. Скачать похожие сертификаты из Интернета и вставить туда названия своих серверов. 4. Сказать, что для внутренней сети сертификаты не нужны.	2 Сопровождение аттестации требует обеспечения легитимности всех СЗИ и средств обработки информации. Отсутствие обязательных документов делает аттестацию невозможной.



1784087278

Орган по аттестации в ходе испытаний выявил, что длина паролей пользователей в системе составляет всего 4 символа (вместо 8 по ТЗ). Как должен поступить сопровождающий? 1. Доказывать комиссии, что 4 символа — это очень удобно для сотрудников. 2. Изменить текст ТЗ прямо во время проверки, снизив планку до 4 символов. 3. Признать несоответствие, оперативно перенастроить парольную политику на сервере до требуемых 8 символов и продемонстрировать исправление комиссии. 4. Предложить комиссии взятку за игнорирование этого пункта.	3 Задача сопровождающего — содействовать успешному прохождению аттестации путем оперативного устранения выявленных недочетов, если они носят конфигурационный характер.
---	---

ПК-5 Способен организовывать и проводить приемочные испытания СЗИ, вводить в эксплуатацию СЗИ

Вопрос	Ключ ответа
При приемочных испытаниях системы контроля доступа (СКУД) выяснилось, что при отключении электропитания все замки на дверях остаются заблокированными, препятствуя эвакуации. Какое решение принять? 1. Принять систему, так как это обеспечивает максимальный уровень защиты от злоумышленников. 2. Отклонить приемку СЗИ и выставить требование подрядчику настроить автоматическую разблокировку замков при пропадании питания или срабатывании пожарной тревоги. 3. Принять систему и выдать всем сотрудникам по топору на случай пожара. 4. Изменить ТЗ, указав, что эвакуация из здания не предусмотрена.	2 Приемочные испытания систем физической и информационной безопасности не должны противоречить нормам охраны труда и пожарной безопасности.
Вы успешно завершили все тесты межсетевого экрана по Программе и методике испытаний (ПМИ). Что является финальным шагом для его ввода в промышленную эксплуатацию? 1. Устное поздравление команды инженеров. 2. Отправка электронного письма всем сотрудникам о том, что теперь всё защищено. 3. Подписание Акта завершения приемочных испытаний членами комиссии и издание руководителем Приказа о вводе СЗИ в эксплуатацию. 4. Перезагрузка межсетевого экрана.	3 Официальный ввод СЗИ в эксплуатацию на предприятии — это юридически значимое действие, требующее документальной фиксации ответственности в виде актов и приказов.

ПК-6 Прогнозирует риски в информационной безопасности и управляет инцидентами информационной безопасности

Вопрос	Ключ ответа
Антивирусная система на сервере внезапно начала фиксировать массовое и быстрое изменение расширений сотен файлов на ".locked". Спрогнозируйте риск и выберите действие. 1. Это плановое архивирование данных системой; ничего делать не нужно. 2. Риск поломки жесткого диска; нужно немедленно перезагрузить сервер. 3. Риск атаки вируса-шифровальщика; необходимо немедленно изолировать сервер от сети и остановить подозрительные процессы. 4. Риск сбоя в базе данных; нужно запустить проверку диска.	3 Прогнозирование рисков позволяет вовремя распознать паттерн поведения шифровальщика. Первым шагом локализации инцидента является отключение от сети для спасения остальных узлов инфраструктуры.



1784087278

При прогнозировании рисков вы понимаете, что единственный системный администратор компании знает все пароли наизусть и нигде их не фиксирует. Какое управленческое решение снизит этот риск? 1. Заставить администратора сдать экзамен на память. 2. Уволить администратора, пока он ничего не забыл. 3. Внедрить систему управления паролями (менеджер паролей) с разделением прав и регламентировать обязательное документирование учетных записей. 4. Ничего не делать, так как администратор работает в компании уже 10 лет.	3 Снижение риска потери критических знаний и монополизации доступа достигается за счет внедрения специализированных инструментов хранения паролей и регламентации процессов документирования
--	---

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			

УК-2 Способен управлять проектом на всех этапах его жизненного цикла

Вопрос	Ключ ответа
Организация инициирует проект по модернизации системы защиты персональных данных в связи с изменениями в законодательстве. Опишите ваши действия как менеджера проекта на этапе инициации.	Разработка и утверждение Устава проекта. Необходимо определить: глобальную цель, ключевые заинтересованные стороны, предварительный бюджет и сроки.
Организация инициирует проект по модернизации системы защиты персональных данных в связи с изменениями в законодательстве. Опишите ваши действия как менеджера проекта на этапе завершения этого проекта.	Проведение приемо-сдаточных испытаний и подписание актов. Формирование итогового отчета, расформирование проектной команды, передача системы в эксплуатацию.

УК-3 Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели

Вопрос	Ключ ответа
Вы назначены руководителем временной рабочей группы из 4 человек (аналитик, два инженера и специалист по режимам). Ваша цель – за 2 недели подготовить филиал к аттестации. Из-за сжатых сроков в команде возникло напряжение и споры о приоритетах. Сформулируйте командную стратегию.	параллельное выполнение задач с ежедневными 10-минутными совещаниями для контроля статуса и снятия блокирующих проблем.
Вы назначены руководителем временной рабочей группы из 4 человек (аналитик, два инженера и специалист по режимам). Ваша цель – за 2 недели подготовить филиал к аттестации. Из-за сжатых сроков в команде возникло напряжение и споры о приоритетах. Распределите задачи.	Аналитик: Актуализирует и собирает разрешительную и техническую документацию на автоматизированную систему. Инженеры: установка, настройка и проверка корректности работы СЗИ от НСД и антивирусов. Специалист по режимам: Проверяет физическую безопасность помещений, опечатывание техники и ведение журналов учета.

ПК-3 Владеет нормативно-методической базой обеспечения защиты сведений, составляющих



1784087278

государственную тайну

Вопрос	Ключ ответа
В ходе аудита архива защищенного подразделения вы обнаружили неучтенный жесткий диск, на котором, по словам сотрудника, хранятся старые копии секретных документов. На диске нет никаких маркировок. Опишите ваши действия.	Немедленно изъять носитель и изолировать его от любых вычислительных сетей. Доложить руководству подразделения по защите государственной тайны. Провести служебное расследование. Принять решение о его уничтожении или официальном вводе в эксплуатацию.
В ходе аудита архива защищенного подразделения вы обнаружили неучтенный ноутбук, на котором, по словам сотрудника, хранятся старые файлы секретных документов. На ноутбуке нет никаких маркировок. Опишите ваши действия.	Немедленная локализация и физическая защита Документирование и информирование Служебное расследование Принятие итогового решения

ПК-4 Способен организовывать и сопровождать аттестацию объектов вычислительной техники и выделенных (защищаемых) помещений на соответствие требованиям по защите информации

Вопрос	Ключ ответа
В ходе организационного этапа подготовки к аттестации выделенного помещения (для обсуждения сведений, составляющих государственную тайну) вы обнаружили, что в техническом паспорте на помещение отсутствует схема расположения основных и вспомогательных технических средств (ОТСС и ВТСС), а также не указаны границы контролируемой зоны. Опишите ваши действия как организатора и сопровождающего лица для устранения этой проблемы до приезда аттестационной комиссии.	Провести физический осмотр помещения и нанести на масштабную схему все установленные технические средства. Определить и измерить расстояние от технических средств до границ контролируемой зоны. Оформить полученные данные в виде графического приложения к техническому паспорту и утвердить обновленный техпаспорт у руководства предприятия.
В ходе организационного этапа подготовки к аттестации выделенного помещения (для обсуждения сведений, составляющих государственную тайну) вы обнаружили, что в техническом паспорте на помещение отсутствует схема расположения основных и вспомогательных технических средств (ОТСС и ВТСС), а также не указаны границы контролируемой зоны. Проведите анализ ситуации.	Эксплуатация и аттестация объекта без актуального и полного технического паспорта невозможна согласно требованиям нормативно-методических документов ФСТЭК России.

ПК-5 Способен организовывать и проводить приемочные испытания СЗИ, вводить в эксплуатацию СЗИ

Вопрос	Ключ ответа
Вам поручено организовать и провести приемочные испытания системы защиты от несанкционированного доступа (СЗИ от НСД), установленной на автоматизированное рабочее место. Сформулируйте один простой сценарий проверки для приемочных испытаний.	Цель: Убедиться, что СЗИ блокирует загрузку операционной системы при изменении контролируемого файла. Действие: Администратор безопасности намеренно вносит изменения в один из системных файлов, поставленных на контроль целостности в СЗИ, и перезагружает компьютер. Ожидаемый результат: СЗИ от НСД при загрузке выявляет модификацию файла, блокирует дальнейший старт операционной системы и выводит сообщение о нарушении целостности среды. Данный факт заносится в протокол испытаний.



1784087278

Вам поручено организовать и провести приемочные испытания системы защиты от несанкционированного доступа (СЗИ от НСД), установленной на автоматизированное рабочее место. Опишите итоговое действие для официального ввода данной СЗИ в эксплуатацию.	После успешного завершения всех проверок по программе и методике испытаний оформляется «Акт завершения приемочных испытаний». На основании акта разрабатывается и подписывается руководством предприятия «Приказ о вводе СЗИ от НСД в промышленную эксплуатацию».
---	---

ПК-6 Прогнозирует риски в информационной безопасности и управляет инцидентами информационной безопасности

Вопрос	Ключ ответа
В журнале событий межсетевого экрана зафиксирована аномалия: в нерабочее время (в 02:00 ночи) произошла выгрузка 50 Гб данных с корпоративного файлового сервера на неизвестный внешний IP-адрес. Спрогнозируйте риски.	Критический риск утечки конфиденциальной информации, нарушение требований законодательства и регуляторов, финансовые и репутационные потери.
В журнале событий межсетевого экрана зафиксирована аномалия: в нерабочее время (в 02:00 ночи) произошла выгрузка 50 Гб данных с корпоративного файлового сервера на неизвестный внешний IP-адрес. Опишите порядок управления этим инцидентом	Локализация. Анализ. Устранение и восстановление. Документирование.

7.2.3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций

7.2.3.1. Текущий контроль по результатам прохождения практики проводится по месту прохождения практики обучающегося в присутствии руководителя практики от КузГТУ и руководителя практики от профильной организации.

Текущий контроль проводится по завершении каждого этапа практики, кроме заключительного.

7.2.3.2. Промежуточная аттестация проводится по завершению заключительного этапа практики, по месту прохождения практики обучающегося в присутствии руководителя практики от КузГТУ и руководителя практики от профильной организации.

На промежуточную аттестацию представляется устный отчет по результатам практики (возможно в форме презентации), согласованный с руководителями практики от КузГТУ и профильной организации.

Формой промежуточной аттестации является дифференцированный зачет, который проводится после завершения прохождения Заключительного этапа практики, в последний день прохождения практики в соответствии с календарным учебным графиком. На промежуточной аттестации обучающийся представляет доклад по итогам подготовленного в процессе прохождения практики отчета по результатам практики (защита отчета) и отчет, оформленный в соответствии с установленными требованиями к содержанию и индивидуальным планом графиком прохождения практики.

8 Перечень учебной литературы и ресурсов сети «Интернет», необходимых для проведения практики

8.1 Основная литература

1. Раченко, Т. А. Информационная безопасность : учебно-методическое пособие / Т. А. Раченко. — Тольятти : ТГУ, 2024. — 135 с. — ISBN 978-5-8259-1612-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/427130> (дата обращения: 30.03.2026). — Режим доступа: для авториз. пользователей.

2. Зенков, А. В. Информационная безопасность и защита информации: учебник для вузов / Зенков А. В.. - 2-е изд., пер. и доп. - Москва : Юрайт, 2025. - 107 с. - ISBN 978-5-534-16388-9. - URL: <https://urait.ru/book/informacionnaya-bezopasnost-i-zaschita-informacii-567915> (дата обращения: 30.03.2026). - Текст : электронный.

3. Чернова, Е. В. Информационная безопасность человека: учебник для вузов / Чернова Е. В.. - 3-е изд., пер. и доп. - Москва : Юрайт, 2025. - 327 с. - ISBN 978-5-534-16772-6. - URL:



1784087278

<https://urait.ru/book/informacionnaya-bezopasnost-cheloveka-566457> (дата обращения: 30.03.2026). – Текст : электронный.

4. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах : учебное пособие / В.Ф. Шаньгин. — Москва : ФОРУМ : ИНФРА-М, 2022. — 592 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-8199-0730-6. - Текст : электронный. - URL: <https://znanium.ru/catalog/product/1843022> (дата обращения: 07.09.2026). – Режим доступа: по подписке.

8.2 Дополнительная литература

1. Кочетков, Н. М. Учебная практика (Организационно-управленческая практика) : методическое пособие / Н. М. Кочетков, А. С. Красникова, О. В. Шишкина. – Москва : Креативная экономика, 2017. – 24 с. : ил. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=599515> (дата обращения: 10.09.2026). – Библиогр.: с. 17 - 18. – ISBN 978-5-91292-215-2. – DOI 10.18334/9785912922152. – Текст : электронный.

2. Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2024. — 336 с. — (Высшее образование). — DOI: <https://doi.org/10.29039/1761-6>. - ISBN 978-5-369-01761-6. - Текст : электронный. - URL: <https://znanium.ru/catalog/product/2082642> (дата обращения: 07.09.2026). – Режим доступа: по подписке.

3. Клименко, И. С. Информационная безопасность и защита информации: модели и методы управления : монография / И.С. Клименко. — Москва : ИНФРА-М, 2024. — 180 с. — (Научная мысль). — DOI 10.12737/monography_5d412ff13c0b88.75804464. - ISBN 978-5-16-015149-6. - Текст : электронный. - URL: <https://znanium.ru/catalog/product/2052391> (дата обращения: 07.09.2026). – Режим доступа: по подписке.

8.3 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: 30.03.2026). – Текст : электронный.

8.4 Профессиональные базы данных и информационные справочные системы

1. Универсальная полнотекстовая база данных электронных периодических изданий «ИВИС» <https://eivis.ru/>

2. Электронная библиотечная система «Университетская библиотека онлайн» <http://biblioclub.ru/>

3. Электронная библиотечная система «Лань» <http://e.lanbook.com>

4. Электронная библиотека КузГТУ <https://library.kuzstu.ru/index.php/punkt-2/podrazdel-21>

5. Электронная библиотека Новосибирского государственного технического университета <https://clck.ru/UoXpv>

6. Образовательная платформа «Юрайт» <https://urait.ru/>

7. Электронная библиотечная система «Znanium» <https://new.znanium.com/my/documents>

8. Справочная правовая система «КонсультантПлюс» <http://www.consultant.ru/>

9. Национальная электронная библиотека <https://rusneb.ru/>

8.5 Периодические издания

1. Безопасность информационных технологий: научный журнал <https://eivis.ru/browse/publication/379646>

2. Информация и безопасность : научный журнал

8.6 Ресурсы 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.



1784087278

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.

9 Перечень информационных технологий, используемых при проведении практики, включая перечень программного обеспечения и информационных справочных систем

При проведении практики может использоваться следующее программное обеспечение:

1. 7-zip
2. Open Office
3. Microsoft Windows
4. ESET NOD32 Smart Security Business Edition
5. Kaspersky Endpoint Security
6. Браузер Спутник

10 Описание материально-технической базы, необходимой для проведения практики

Лаборатория № 1149 представляет собой лабораторию в области технологий обеспечения информационной безопасности и защищенных информационных систем, оснащенную средствами вычислительной техники, сетевым оборудованием, техническими, программными и программно-аппаратными средствами защиты информации и средствами контроля защищенности информации.

Перечень основного оборудования:

Комплект мебели (столы и стулья). Персональные компьютеры. Сетевое оборудование, технические, программные и программно-аппаратные средства защиты информации и средства контроля защищенности информации.

Моноблок (Intel Core i5-10400 / 8 Gb RAM); горизонт кабельный организатор (25B-1U-02BL); коммутац панель кат.5 (27B-U5-24BL 24 ports); коммутац панель кат.6 (27B-U6-24BL 24 ports); шкаф коммутац Eurolan (S3000-22U 600x600 мм, перед - стекло, зад - металл, 60F-22-66-31BL); коммутатор управляемый (D-Link DGS-3130-54TS 48 ports); программно-аппаратный комплекс (Infotecs IDS-1000); модуль доверенной загрузки (&amp;amp;amp;amp;amp;quot;Соболь-4&amp;amp;amp;amp;amp;amp;quot;); средство активной защиты информации от утечки за счет наводок информ сигнала на цепи заземления и электропитания (&amp;amp;amp;amp;amp;amp;amp;quot;Соната-PC3&amp;amp;amp;amp;amp;quot;); точка доступа Wi-fi двухдиапазонная (D-Link DWL-8620AP); патч-корды кат 5 (Eurolan); патч-корды кат 6 (Eurolan);

кабельный тестер (CableMaster-800); коммутатор управляемый (D-Link DES-1210-28 28 ports); коммутатор неуправляемый (D-Link DSS-100E-9P 8+1 ports); маршрутизатор проводной (D-Link DSR-150 8 ports); Wi-Fi маршрутизатор двухдиапазонный (D-Link DWR-980 4 Lan-ports).

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

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&amp;amp;amp;amp;amp;quot; AOC 24B1H VA 1920x1080 (16:9), 250кд/м2, 5мс, VGA, HDMI, черные; Системные блокиMasteroMiddleMC05, IntelCorei510400 2.9GHz, 8GbRAM, 240GbSSD, DOS, программно-аппаратный комплекс для обнаружения компьютерных атак VipNet, средство доверенной загрузки (СДЗ) Соболь.

Специальное помещение для самостоятельной работы № 1211

Перечень основного оборудования:



1784087278

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.



1784087278



1784087278