

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 15:58:42

Дубинкин Дмитрий Михайлович

Программа практики

Вид практики: Производственная

Тип практики: Преддипломная 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.



1784258534

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.



1784258534

Рабочую программу составил:

ПОДПИСАНО ЭП КУЗГТУ

Подразделение: кафедра информационной безопасности

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

Дата: 17.07.2026 10:22:55

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 10:23:14

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 10:23:34

Прокопенко Евгения Викторовна



1784258534

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: Преддипломная практика.

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

Освоение дисциплины направлено на формирование:
профессиональных компетенций:

ПК-1 - Владеет методикой проведения предпроектного обследования объектов информатизации и выделенных(защищаемых) помещений

ПК-2 - Способен приводить аналитическое обоснование необходимости создания систем защиты информации

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-1 - Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий

Результаты обучения по дисциплине определяются индикаторами достижения компетенций

Индикатор(ы) достижения:

Осуществляет критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий.

Владеет методикой проведения предпроектного обследования объектов информатизации и выделенных защищаемых помещений.

Приводит аналитическое обоснование необходимости создания систем 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 способы сбора и обработки данных, методологию и способы исследования в области - информационной безопасности.

Знать методологию проектирования систем, комплексов, средств и технологий обеспечения информационной безопасности, необходимые для разработки систем, комплексов, средств и технологий обеспечения информационной безопасности.

Знать российские и международные стандарты в области информационной безопасности.

Знать основные принципы организации систем, средств и технологий обеспечения информационной безопасности.

Знать понятия контура безопасности, физические и математические методы исследования защищенности объектов; порядок проведения аттестации объектов информатизации по требованиям безопасности информации, требования стандартов и иных нормативно-технических документов по безопасности информации, утвержденных Гостехкомиссией России.

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



1784258534

Знать порядок организации деятельности по управлению информационной безопасностью.
 Иметь опыт анализа проблемных ситуаций на основе системного подхода
 Иметь опыт проведения предпроектного обследования объектов информатизации и выделенных защищаемых помещений.
 Иметь опыт приведения аналитическое обоснование необходимости создания систем защиты информации.
 Иметь опыт подготовки нормативно-методической базы по защите сведений, составляющих государственную тайну.
 Иметь опыт организации и сопровождения аттестации объектов вычислительной техники и выделенных защищаемых помещений на соответствие требованиям по защите информации.
 Иметь опыт организации приемочных испытаний систем защиты информации.
 Иметь опыт анализа рисков в информационной безопасности и управлении инцидентами информационной безопасности.
 Уметь анализировать необходимую информацию в области информационной безопасности, содержащуюся в различных формах отчетности и прочих отечественных и зарубежных источника.
 Уметь выполнять проектирование и разработку систем, комплексов, средств и технологий обеспечения информационной безопасности.
 Уметь проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты.
 Уметь организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами.
 Уметь проводить экспериментальные исследования защищенности объектов, разрабатывать требования к защите от утечек по техническим каналам.
 Уметь организовывать приемочные испытания системы защиты информации.
 Уметь организовать процесс управления информационной безопасностью.
 Владеть навыками интерпретации информации, содержащейся в различных отечественных и зарубежных источниках в области информационной безопасности.
 Владеть навыками работы в среде CASE-средств анализа и проектирования систем навыками использования в практической деятельности новых знаний и умений.
 Владеть навыками обеспечения информационной безопасностью объектов защиты.
 Владеть знаниями законодательных и правовых актов в области безопасности; правилами составления локальных нормативных актов и регламентов в области информационной безопасности.
 Владеть методами инструментального контроля защищенности объекта.
 Владеть способами приемочных испытаний СЗИ, ввода в эксплуатацию СЗИ.
 Владеть навыками управления системой 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 12 зачетных единиц.
 Общий объем практики составляет 432 часа.

5 Содержание практики

/п	Этапы практики	Виды учебной работы	Часы
----	----------------	---------------------	------



1784258534

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 2.1. Проведение минилекции ведущим специалистом (наставником) предприятия 2.2. Ознакомление со структурой предприятия 2.3. Ознакомление с основными технологическими процессами 2.4. Ознакомление с механическим и энергетическим оборудованием 2.5. Ознакомление со средствами автоматизации производственных процессов 2.6. Выполнение производственной работы на выделенном участке 2.7. Сбор, обработка и систематизация информационного материала. 2.8. Формирование информационной базы.	Методы и средства управления информационной безопасности предприятия. Организация управления информационной безопасностью, проектирование систем (компонент системы) обеспечения информационной безопасности, работа с организационно-распорядительной документацией по обеспечению информационной безопасности.	396
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			432

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.

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;



1784258534

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.

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.

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.



1784258534

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:

Ф о р м а (ы) т е к у щ е г о к о н т р о л я	К о м п е т е н ц и и , ф о р м и р у е м ы е в р е з у л ь т а т е о с в о е н и я д и с ц и п л и н ы (м о д у л я)	И н д и к а т о р (ы) д о с т и ж е н и я к о м п е т е н ц и и	Р е з у л ь т а т ы о б у ч е н и я п о д и с ц и п л и н е (м о д у л ю)	У р о в е н ь



1784258534

собеседование по материалам, собранным в результате прохождения каждого этапа практики	ПК-1	Владеет методикой проведения предпроектного обследования объектов информатизации и выделенных защищаемых помещений.	Знать методологию проектирования систем, комплексов, средств и технологий обеспечения информационной безопасности, необходимые для разработки систем, комплексов, средств и технологий обеспечения информационной безопасности. Уметь выполнять проектирование и разработку систем, комплексов, средств и технологий обеспечения информационной безопасности. Владеть навыками работы в среде CASE-средств анализа и проектирования систем навыками использования в практической деятельности новых знаний и умений. Иметь опыт проведения предпроектного обследования объектов информатизации и выделенных защищаемых помещений.	Высокий или средний
собеседование по материалам, собранным в результате прохождения каждого этапа практики	ПК-2	Приводит аналитическое обоснование необходимости создания систем защиты информации.	Знать российские и международные стандарты в области информационной безопасности. Уметь проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты. Владеть навыками обеспечения информационной безопасностью объектов защиты. Иметь опыт приведения аналитического обоснования необходимости создания систем защиты информации.	Высокий или средний



1784258534

собеседование по материалам, собранным в результате прохождения каждого этапа практики	ПК-3	Владеет нормативно-методической базой обеспечения защиты сведений, составляющих государственную тайну	Знать основные принципы организации систем, средств и технологий обеспечения информационной безопасности. Уметь организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами. Владеть знаниями законодательных и правовых актов в области безопасности; правилами составления локальных нормативных актов и регламентов в области информационной безопасности. Иметь опыт подготовки нормативно-методической базы по защите сведений, составляющих государственную тайну.	Высокий или средний
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 понятия контура безопасности, физические и математические методы исследования защищенности объектов; порядок проведения аттестации объектов информатизации по требованиям безопасности информации, требования стандартов и иных нормативно-технических документов по безопасности информации, утвержденных Гостехкомиссией России. Уметь проводить экспериментальные исследования защищенности объектов, разрабатывать требования к защите от утечек по техническим каналам. Владеть методами инструментального контроля защищенности объекта. Иметь опыт организации и сопровождения аттестации объектов вычислительной техники и выделенных защищаемых помещений на соответствие требованиям по защите информации.	Высокий или средний



1784258534

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	ПК-6	Прогнозирует риски в информационной безопасности и управляет инцидентами информационной безопасности.	Знать порядок организации деятельности по управлению информационной безопасностью. Уметь организовать процесс управления информационной безопасностью. Владеть навыками управления системой информационной безопасности. Иметь опыт анализа рисков в информационной безопасности и управлении инцидентами информационной безопасности.	Высокий или средний
собеседование по материалам, собранным в результате прохождения каждого этапа практики	УК-1	Осуществляет критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий.	Знать способы сбора и обработки данных, методологию и способы исследования в области информационной безопасности. Уметь анализировать необходимую информацию в области информационной безопасности, содержащуюся в различных формах отчетности и прочих отечественных и зарубежных источника. Владеть навыками интерпретации информации, содержащейся в различных отечественных и зарубежных источниках в области информационной безопасности. Иметь опыт анализа проблемных ситуаций на основе системного подхода.	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



1784258534

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 средства 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 ЭИОС КузГТУ.

Примерные вопросы собеседования:

УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий

Содержание вопроса (задания)	Правильный ответ
«Подготовка объекта к обработке сведений, составляющих государственную тайну». В ходе преддипломной практики вам поручено подготовить к эксплуатации выделенное помещение (ВП) и автоматизированную систему (АС) для работы со сведениями под грифом «Секретно». На этапе обследования выяснили, что стена помещения является смежной с коридором общего пользования, а на компьютерах не установлены средства защиты от несанкционированного доступа (СЗИ от НСД). Какая последовательность действий является методологически верной для успешного прохождения аттестации и ввода объекта в эксплуатацию? Варианты ответа: 1. Сначала установить антивирус, затем пригласить аттестационную комиссию, а проблему со смежной стеной решить после получения аттестата. 2. Провести предпроектное обследование, обосновать установку системы виброакустической защиты и СЗИ от НСД, разработать документы согласно нормам СТР, провести приемочные испытания установленных средств и передать объект на аттестацию. 3. Написать научную статью о методах взлома защищенных стен, закупить любое зарубежное ПО для шифрования дисков и составить график дежурств сотрудников в коридоре для охраны стены	2 Выбор этого варианта демонстрирует системный подход: выявлена проблемная ситуация (уязвимость стены и отсутствие СЗИ) и выработана логическая стратегия действий от обследования до аттестации
В компании внедрена новая система безопасности, которая требует смены пароля каждые 15 дней. Это привело к тому, что сотрудники стали записывать пароли на стикерах. Какая стратегия действий будет системно верной? 1. Штрафовать сотрудников за хранение записей на рабочем столе. 2. Отменить требование регулярной смены паролей. 3. Внедрить аппаратную двухфакторную аутентификацию (токены) или биометрию, снизив частоту смены паролей. 4. Купить более яркие стикеры, чтобы пароли было проще находить.	3 Системный подход требует анализа «человеческого фактора». Стратегия должна устранять корень проблемы (неудобство), а не бороться с симптомами. Использование токенов обеспечивает безопасность без создания когнитивной нагрузки на персонал.

ПК-1 Владеет методикой проведения предпроектного обследования объектов информатизации и выделенных(защищаемых) помещений

Содержание вопроса (задания)	Правильный ответ
------------------------------	------------------



1784258534

«Подготовка объекта к обработке сведений, составляющих государственную тайну». В ходе преддипломной практики вам поручено подготовить к эксплуатации выделенное помещение (ВП) и автоматизированную систему (АС) для работы со сведениями под грифом «Секретно». На этапе обследования вы выяснили, что стена помещения является смежной с коридором общего пользования, а на компьютерах не установлены средства защиты от несанкционированного доступа (СЗИ от НСД). Какая последовательность действий является методологически верной для успешного прохождения аттестации и ввода объекта в эксплуатацию? Варианты ответа: 1. Сначала установить антивирус, затем пригласить аттестационную комиссию, а проблему со смежной стеной решить после получения аттестата. 2. Провести предпроектное обследование, обосновать установку системы виброакустической защиты и СЗИ от НСД, разработать документы согласно нормам СТР, провести приемочные испытания установленных средств и передать объект на аттестацию. 3. Написать научную статью о методах взлома защищенных стен, закупить любое зарубежное ПО для шифрования дисков и составить график дежурств сотрудников в коридоре для охраны стены	2 Выполнение предпроектного обследования позволяет выявить канал утечки через смежную стену. На основе этого дается аналитическое обоснование необходимости СЗИ от НСД для выполнения требований регулятора.
При обследовании выделенного помещения (ВП) для совещаний за подвесным потолком обнаружен старый неиспользуемый громкоговоритель оповещения. Какое действие методически верно? 1. Оставить его, если он не подключен к проводам. 2. Зафиксировать как вспомогательное техническое средство и настоять на его демонтаже или защите фильтрами. 3. Использовать его для трансляции музыки, чтобы скрыть звуки переговоров. 4. Проверить, не спрятана ли в нем камера, и оставить на месте.	2. Методика обследования объектов информатизации требует выявления всех физических тел, способных создавать каналы утечки. Любое стороннее оборудование в ВП - это риск несанкционированного съема информации.

ПК-2 Способен приводить аналитическое обоснование необходимости создания систем защиты информации



1784258534

Содержание вопроса (задания)	Правильный ответ
«Подготовка объекта к обработке сведений, составляющих государственную тайну». В ходе преддипломной практики вам поручено подготовить к эксплуатации выделенное помещение (ВП) и автоматизированную систему (АС) для работы со сведениями под грифом «Секретно». На этапе обследования выяснили, что стена помещения является смежной с коридором общего пользования, а на компьютерах не установлены средства защиты от несанкционированного доступа (СЗИ от НСД). Какая последовательность действий является методологически верной для успешного прохождения аттестации и ввода объекта в эксплуатацию? Варианты ответа: 1. Сначала установить антивирус, затем пригласить аттестационную комиссию, а проблему со смежной стеной решить после получения аттестата. 2. Провести предпроектное обследование, обосновать установку системы виброакустической защиты и СЗИ от НСД, разработать документы согласно нормам СТР, провести приемочные испытания установленных средств и передать объект на аттестацию. 3. Написать научную статью о методах взлома защищенных стен, закупить любое зарубежное ПО для шифрования дисков и составить график дежурств сотрудников в коридоре для охраны стены	2 Выполнение предпроектного обследования позволяет выявить канал утечки через смежную стену. На основе этого дается аналитическое обоснование необходимости активной защиты.
Руководство считает установку системы виброакустического зашумления окон избыточной тратой средств. Какое обоснование будет наиболее убедительным? 1. Это требование моды в современных офисах. 2. Анализ угроз подтверждает наличие риска дистанционного съема речи лазерным методом через оконные стекла. 3. Система зашумления также защищает от шума машин с улицы. 4. Стоимость системы невелика по сравнению с общим бюджетом.	2. Аналитическое обоснование базируется на сопоставлении модели угроз и конкретных мер защиты. Если канал утечки существует физически, его нейтрализация становится технологической необходимостью, а не опцией.

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

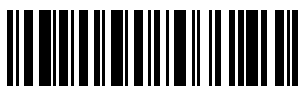


1784258534

Содержание вопроса (задания)	Правильный ответ
«Подготовка объекта к обработке сведений, составляющих государственную тайну». В ходе преддипломной практики вам поручено подготовить к эксплуатации выделенное помещение (ВП) и автоматизированную систему (АС) для работы со сведениями под грифом «Секретно». На этапе обследования вы выяснили, что стена помещения является смежной с коридором общего пользования, а на компьютерах не установлены средства защиты от несанкционированного доступа (СЗИ от НСД). Какая последовательность действий является методологически верной для успешного прохождения аттестации и ввода объекта в эксплуатацию? Варианты ответа: 1. Сначала установить антивирус, затем пригласить аттестационную комиссию, а проблему со смежной стеной решить после получения аттестата. 2. Провести предпроектное обследование, обосновать установку системы виброакустической защиты и СЗИ от НСД, разработать документы согласно нормам СТР, провести приемочные испытания установленных средств и передать объект на аттестацию. 3. Написать научную статью о методах взлома защищенных стен, закупить любое зарубежное ПО для шифрования дисков и составить график дежурств сотрудников в коридоре для охраны стены	2 Разработка документов ведется строго по нормативно-методической базе, что обязательно для объектов, связанных с государственной тайной.
Какое требование является обязательным при транспортировке жесткого диска со сведениями «секретно» между двумя зданиями организации? 1. Упаковка диска в пузырчатую пленку для защиты от ударов. 2. Помещение диска в опечатываемый спецпортфель (пенал) и передача через секретное подразделение с записью в журнале. 3. Сопровождение диска двумя охранниками с оружием. 4. Пересылка диска через обычную курьерскую службу.	2. Работа с гостайной регламентируется жесткой нормативной базой (Инструкция №3-1), которая определяет порядок учета и перемещения носителей только через уполномоченных лиц в защищенной таре.

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

Содержание вопроса (задания)	Правильный ответ
«Подготовка объекта к обработке сведений, составляющих государственную тайну». В ходе преддипломной практики вам поручено подготовить к эксплуатации выделенное помещение (ВП) и автоматизированную систему (АС) для работы со сведениями под грифом «Секретно». На этапе обследования вы выяснили, что стена помещения является смежной с коридором общего пользования, а на компьютерах не установлены средства защиты от несанкционированного доступа (СЗИ от НСД). Какая последовательность действий является методологически верной для успешного прохождения аттестации и ввода объекта в эксплуатацию? Варианты ответа: 1. Сначала установить антивирус, затем пригласить аттестационную комиссию, а проблему со смежной стеной решить после получения аттестата. 2. Провести предпроектное обследование, обосновать установку системы виброакустической защиты и СЗИ от НСД, разработать документы согласно нормам СТР, провести приемочные испытания установленных средств и передать объект на аттестацию. 3. Написать научную статью о методах взлома защищенных стен, закупить любое зарубежное ПО для шифрования дисков и составить график дежурств сотрудников в коридоре для охраны стены	2 Только после выполнения всех технических и организационных мер объект готов к аттестации.



1784258534

Содержание вопроса (задания)	Правильный ответ
В ходе аттестационных испытаний выяснилось, что на сервере не обновлены антивирусные базы. Ваши действия в роли сопровождающего? 1. Сообщить комиссии, что интернет временно не работает. 2. Признать несоответствие, немедленно обновить базы и предоставить отчет комиссии для фиксации в протоколе. 3. Предложить комиссии прийти на следующей неделе. 4. Удалить антивирус, чтобы он не мешал проверке.	2. Сопровождение аттестации подразумевает оперативное взаимодействие с экспертами и устранение мелких недостатков в ходе испытаний для получения «Аттестата соответствия» в срок.

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

Содержание вопроса (задания)	Правильный ответ
«Подготовка объекта к обработке сведений, составляющих государственную тайну». В ходе преддипломной практики вам поручено подготовить к эксплуатации выделенное помещение (ВП) и автоматизированную систему (АС) для работы со сведениями под грифом «Секретно». На этапе обследования выяснили, что стена помещения является смежной с коридором общего пользования, а на компьютерах не установлены средства защиты от несанкционированного доступа (СЗИ от НСД). Какая последовательность действий является методологически верной для успешного прохождения аттестации и ввода объекта в эксплуатацию? Варианты ответа: 1. Сначала установить антивирус, затем пригласить аттестационную комиссию, а проблему со смежной стеной решить после получения аттестата. 2. Провести предпроектное обследование, обосновать установку системы виброакустической защиты и СЗИ от НСД, разработать документы согласно нормам СТР, провести приемочные испытания установленных средств и передать объект на аттестацию. 3. Написать научную статью о методах взлома защищенных стен, закупить любое зарубежное ПО для шифрования дисков и составить график дежурств сотрудников в коридоре для охраны стены	2 Перед аттестацией обязательно проводятся приемочные испытания и ввод СЗИ в эксплуатацию, чтобы убедиться, что средства защиты настроены корректно и выполняют свои функции.
При приемочных испытаниях системы защиты от НСД обнаружено, что она блокирует доступ пользователям, имеющим законные права. О чем это говорит? 1. О слишком высокой надежности системы. 2. О некорректной настройке правил разграничения доступа, требующей доработки системы перед вводом. 3. О том, что пользователи пытаются взломать систему. 4. О неисправности клавиатуры.	2. Приемочные испытания проверяют соответствие системы техническому заданию (ТЗ). Ошибочная блокировка легитимных пользователей мешает бизнес-процессам и свидетельствует о неготовности СЗИ к эксплуатации.

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



1784258534

Содержание вопроса (задания)	Правильный ответ
«Подготовка объекта к обработке сведений, составляющих государственную тайну». В ходе преддипломной практики вам поручено подготовить к эксплуатации выделенное помещение (ВП) и автоматизированную систему (АС) для работы со сведениями под грифом «Секретно». На этапе обследования вы выяснили, что стена помещения является смежной с коридором общего пользования, а на компьютерах не установлены средства защиты от несанкционированного доступа (СЗИ от НСД). Какая последовательность действий является методологически верной для успешного прохождения аттестации и ввода объекта в эксплуатацию? Варианты ответа: 1. Сначала установить антивирус, затем пригласить аттестационную комиссию, а проблему со смежной стеной решить после получения аттестата. 2. Провести предпроектное обследование, обосновать установку системы виброакустической защиты и СЗИ от НСД, разработать документы согласно нормам СТР, провести приемочные испытания установленных средств и передать объект на аттестацию. 3. Написать научную статью о методах взлома защищенных стен, закупить любое зарубежное ПО для шифрования дисков и составить график дежурств сотрудников в коридоре для охраны стены	2 Устранение уязвимости стены на этапе проектирования - это предотвращение перехвата информации по виброакустическому каналу.
Система мониторинга зафиксировала 500 попыток входа под именем "admin" с внешнего IP-адреса за одну минуту. К какому типу инцидентов это относится? 1. Плановое обновление системы. 2. Инцидент типа «Brute-force» (подбор пароля), требующий немедленной блокировки IP-адреса. 3. Пользователь просто забыл пароль и часто нажимает Enter. 4. Технический сбой в работе сетевой карты.	2. Умение прогнозировать риски позволяет отличить штатную активность от аномальной. Массовые попытки авторизации - классический инцидент ИБ, требующий стандартного алгоритма реагирования для предотвращения взлома.

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:

1. Системный анализ прикладной области, выявление угроз и оценка уязвимости информационных систем СЭД, разработка требований и критериев оценки информационной безопасности;
2. Обоснование выбора состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты СЭД на основе российских и международных стандартов;
3. Разработка систем, комплексов, средств и технологий обеспечения информационной безопасности информационного пространства СЭД;
4. Разработка программ и методик, испытаний средств и систем обеспечения информационной безопасности СЭД;
5. Анализ фундаментальных и прикладных проблем информационной безопасности СЭД в условиях становления современного информационного общества;
6. Разработка планов и программ проведения научных исследований и технических разработок в области информационной безопасности, подготовка отдельных заданий для исполнителей;



1784258534

7. Аудит информационной безопасности информационных систем и объектов информатизации СЭД;
8. Аттестация объектов информатизации СЭД по требованиям безопасности информации.
9. Изучение объекта информатизации на предмет качества защиты информации и выявление уязвимостей на примере информационной среды учебного учреждения
10. Изучение объекта информатизации на предмет качества защиты информации и выявление уязвимостей на примере производственного предприятия
11. Изучение объекта информатизации на предмет качества защиты информации и выявление уязвимостей на примере государственного учреждения
12. Изучение объекта информатизации на предмет качества защиты информации и выявление уязвимостей на примере торгового предприятия
13. Изучение объекта информатизации на предмет качества защиты информации и выявление уязвимостей на примере системы управления объектом (АСУТО, Умный дом...)

7.2.2. Оценочные средства 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 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 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

Примерные вопросы собеседования:

УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий

Содержание вопроса (задания)	Правильный ответ
«Подготовка объекта к обработке сведений, составляющих государственную тайну». В ходе преддипломной практики вам поручено подготовить к эксплуатации выделенное помещение (ВП) и автоматизированную систему (АС) для работы со сведениями под грифом «Секретно». На этапе обследования выяснили, что стена помещения является смежной с коридором общего пользования, а на компьютерах не установлены средства защиты от несанкционированного доступа (СЗИ от НСД). Какая последовательность действий является методологически верной для успешного прохождения аттестации и ввода объекта в эксплуатацию? Варианты ответа: 1. Сначала установить антивирус, затем пригласить аттестационную комиссию, а проблему со смежной стеной решить после получения аттестата. 2. Провести предпроектное обследование, обосновать установку системы виброакустической защиты и СЗИ от НСД, разработать документы согласно нормам СТР, провести приемочные испытания установленных средств и передать объект на аттестацию. 3. Написать научную статью о методах взлома защищенных стен, закупить любое зарубежное ПО для шифрования дисков и составить график дежурств сотрудников в коридоре для охраны стены	2 Выбор этого варианта демонстрирует системный подход: выявлена проблемная ситуация (уязвимость стены и отсутствие СЗИ) и выработана логическая стратегия действий от обследования до аттестации



1784258534

В компании внедрена новая система безопасности, которая требует смены пароля каждые 15 дней. Это привело к тому, что сотрудники стали записывать пароли на стикерах. Какая стратегия действий будет системно верной? 1. Штрафовать сотрудников за хранение записей на рабочем столе. 2. Отменить требование регулярной смены паролей. 3. Внедрить аппаратную двухфакторную аутентификацию (токены) или биометрию, снизив частоту смены паролей. 4. Купить более яркие стикеры, чтобы пароли было проще находить.	3 Системный подход требует анализа «человеческого фактора». Стратегия должна устранять корень проблемы (неудобство), а не бороться с симптомами. Использование токенов обеспечивает безопасность без создания когнитивной нагрузки на персонал.
--	--

ПК-1 Владеет методикой проведения предпроектного обследования объектов информатизации и выделенных(защищаемых) помещений

Содержание вопроса (задания)	Правильный ответ
«Подготовка объекта к обработке сведений, составляющих государственную тайну». В ходе преддипломной практики вам поручено подготовить к эксплуатации выделенное помещение (ВП) и автоматизированную систему (АС) для работы со сведениями под грифом «Секретно». На этапе обследования вы выяснили, что стена помещения является смежной с коридором общего пользования, а на компьютерах не установлены средства защиты от несанкционированного доступа (СЗИ от НСД). Какая последовательность действий является методологически верной для успешного прохождения аттестации и ввода объекта в эксплуатацию? Варианты ответа: 1. Сначала установить антивирус, затем пригласить аттестационную комиссию, а проблему со смежной стеной решить после получения аттестата. 2. Провести предпроектное обследование, обосновать установку системы виброакустической защиты и СЗИ от НСД, разработать документы согласно нормам СТР, провести приемочные испытания установленных средств и передать объект на аттестацию. 3. Написать научную статью о методах взлома защищенных стен, закупить любое зарубежное ПО для шифрования дисков и составить график дежурств сотрудников в коридоре для охраны стены	2 Выполнение предпроектного обследования позволяет выявить канал утечки через смежную стену. На основе этого дается аналитическое обоснование необходимости СЗИ от НСД для выполнения требований регулятора.
При обследовании выделенного помещения (ВП) для совещаний за подвесным потолком обнаружен старый неиспользуемый громкоговоритель оповещения. Какое действие методически верно? 1. Оставить его, если он не подключен к проводам. 2. Зафиксировать как вспомогательное техническое средство и настоять на его демонтаже или защите фильтрами. 3. Использовать его для трансляции музыки, чтобы скрыть звуки переговоров. 4. Проверить, не спрятана ли в нем камера, и оставить на месте.	2. Методика обследования объектов информатизации требует выявления всех физических тел, способных создавать каналы утечки. Любое стороннее оборудование в ВП - это риск несанкционированного съема информации.

ПК-2 Способен приводить аналитическое обоснование необходимости создания систем защиты информации



1784258534

Содержание вопроса (задания)	Правильный ответ
«Подготовка объекта к обработке сведений, составляющих государственную тайну». В ходе преддипломной практики вам поручено подготовить к эксплуатации выделенное помещение (ВП) и автоматизированную систему (АС) для работы со сведениями под грифом «Секретно». На этапе обследования выяснили, что стена помещения является смежной с коридором общего пользования, а на компьютерах не установлены средства защиты от несанкционированного доступа (СЗИ от НСД). Какая последовательность действий является методологически верной для успешного прохождения аттестации и ввода объекта в эксплуатацию? Варианты ответа: 1. Сначала установить антивирус, затем пригласить аттестационную комиссию, а проблему со смежной стеной решить после получения аттестата. 2. Провести предпроектное обследование, обосновать установку системы виброакустической защиты и СЗИ от НСД, разработать документы согласно нормам СТР, провести приемочные испытания установленных средств и передать объект на аттестацию. 3. Написать научную статью о методах взлома защищенных стен, закупить любое зарубежное ПО для шифрования дисков и составить график дежурств сотрудников в коридоре для охраны стены	2 Выполнение предпроектного обследования позволяет выявить канал утечки через смежную стену. На основе этого дается аналитическое обоснование необходимости активной защиты.
Руководство считает установку системы виброакустического зашумления окон избыточной тратой средств. Какое обоснование будет наиболее убедительным? 1. Это требование моды в современных офисах. 2. Анализ угроз подтверждает наличие риска дистанционного съема речи лазерным методом через оконные стекла. 3. Система зашумления также защищает от шума машин с улицы. 4. Стоимость системы невелика по сравнению с общим бюджетом.	2. Аналитическое обоснование базируется на сопоставлении модели угроз и конкретных мер защиты. Если канал утечки существует физически, его нейтрализация становится технологической необходимостью, а не опцией.

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

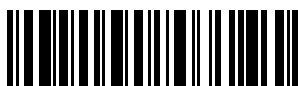


1784258534

Содержание вопроса (задания)	Правильный ответ
«Подготовка объекта к обработке сведений, составляющих государственную тайну». В ходе преддипломной практики вам поручено подготовить к эксплуатации выделенное помещение (ВП) и автоматизированную систему (АС) для работы со сведениями под грифом «Секретно». На этапе обследования вы выяснили, что стена помещения является смежной с коридором общего пользования, а на компьютерах не установлены средства защиты от несанкционированного доступа (СЗИ от НСД). Какая последовательность действий является методологически верной для успешного прохождения аттестации и ввода объекта в эксплуатацию? Варианты ответа: 1. Сначала установить антивирус, затем пригласить аттестационную комиссию, а проблему со смежной стеной решить после получения аттестата. 2. Провести предпроектное обследование, обосновать установку системы виброакустической защиты и СЗИ от НСД, разработать документы согласно нормам СТР, провести приемочные испытания установленных средств и передать объект на аттестацию. 3. Написать научную статью о методах взлома защищенных стен, закупить любое зарубежное ПО для шифрования дисков и составить график дежурств сотрудников в коридоре для охраны стены	2 Разработка документов ведется строго по нормативно-методической базе, что обязательно для объектов, связанных с государственной тайной.
Какое требование является обязательным при транспортировке жесткого диска со сведениями «секретно» между двумя зданиями организации? 1. Упаковка диска в пузырчатую пленку для защиты от ударов. 2. Помещение диска в опечатываемый спецпортфель (пенал) и передача через секретное подразделение с записью в журнале. 3. Сопровождение диска двумя охранниками с оружием. 4. Пересылка диска через обычную курьерскую службу.	2. Работа с гостайной регламентируется жесткой нормативной базой (Инструкция №3-1), которая определяет порядок учета и перемещения носителей только через уполномоченных лиц в защищенной таре.

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

Содержание вопроса (задания)	Правильный ответ
«Подготовка объекта к обработке сведений, составляющих государственную тайну». В ходе преддипломной практики вам поручено подготовить к эксплуатации выделенное помещение (ВП) и автоматизированную систему (АС) для работы со сведениями под грифом «Секретно». На этапе обследования вы выяснили, что стена помещения является смежной с коридором общего пользования, а на компьютерах не установлены средства защиты от несанкционированного доступа (СЗИ от НСД). Какая последовательность действий является методологически верной для успешного прохождения аттестации и ввода объекта в эксплуатацию? Варианты ответа: 1. Сначала установить антивирус, затем пригласить аттестационную комиссию, а проблему со смежной стеной решить после получения аттестата. 2. Провести предпроектное обследование, обосновать установку системы виброакустической защиты и СЗИ от НСД, разработать документы согласно нормам СТР, провести приемочные испытания установленных средств и передать объект на аттестацию. 3. Написать научную статью о методах взлома защищенных стен, закупить любое зарубежное ПО для шифрования дисков и составить график дежурств сотрудников в коридоре для охраны стены	2 Только после выполнения всех технических и организационных мер объект готов к аттестации.



1784258534

Содержание вопроса (задания)	Правильный ответ
В ходе аттестационных испытаний выяснилось, что на сервере не обновлены антивирусные базы. Ваши действия в роли сопровождающего? 1. Сообщить комиссии, что интернет временно не работает. 2. Признать несоответствие, немедленно обновить базы и предоставить отчет комиссии для фиксации в протоколе. 3. Предложить комиссии прийти на следующей неделе. 4. Удалить антивирус, чтобы он не мешал проверке.	2. Сопровождение аттестации подразумевает оперативное взаимодействие с экспертами и устранение мелких недостатков в ходе испытаний для получения «Аттестата соответствия» в срок.

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

Содержание вопроса (задания)	Правильный ответ
«Подготовка объекта к обработке сведений, составляющих государственную тайну». В ходе преддипломной практики вам поручено подготовить к эксплуатации выделенное помещение (ВП) и автоматизированную систему (АС) для работы со сведениями под грифом «Секретно». На этапе обследования выяснили, что стена помещения является смежной с коридором общего пользования, а на компьютерах не установлены средства защиты от несанкционированного доступа (СЗИ от НСД). Какая последовательность действий является методологически верной для успешного прохождения аттестации и ввода объекта в эксплуатацию? Варианты ответа: 1. Сначала установить антивирус, затем пригласить аттестационную комиссию, а проблему со смежной стеной решить после получения аттестата. 2. Провести предпроектное обследование, обосновать установку системы виброакустической защиты и СЗИ от НСД, разработать документы согласно нормам СТР, провести приемочные испытания установленных средств и передать объект на аттестацию. 3. Написать научную статью о методах взлома защищенных стен, закупить любое зарубежное ПО для шифрования дисков и составить график дежурств сотрудников в коридоре для охраны стены	2 Перед аттестацией обязательно проводятся приемочные испытания и ввод СЗИ в эксплуатацию, чтобы убедиться, что средства защиты настроены корректно и выполняют свои функции.
При приемочных испытаниях системы защиты от НСД обнаружено, что она блокирует доступ пользователям, имеющим законные права. О чем это говорит? 1. О слишком высокой надежности системы. 2. О некорректной настройке правил разграничения доступа, требующей доработки системы перед вводом. 3. О том, что пользователи пытаются взломать систему. 4. О неисправности клавиатуры.	2. Приемочные испытания проверяют соответствие системы техническому заданию (ТЗ). Ошибочная блокировка легитимных пользователей мешает бизнес-процессам и свидетельствует о неготовности СЗИ к эксплуатации.

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



1784258534

Содержание вопроса (задания)	Правильный ответ
«Подготовка объекта к обработке сведений, составляющих государственную тайну». В ходе преддипломной практики вам поручено подготовить к эксплуатации выделенное помещение (ВП) и автоматизированную систему (АС) для работы со сведениями под грифом «Секретно». На этапе обследования вы выяснили, что стена помещения является смежной с коридором общего пользования, а на компьютерах не установлены средства защиты от несанкционированного доступа (СЗИ от НСД). Какая последовательность действий является методологически верной для успешного прохождения аттестации и ввода объекта в эксплуатацию? Варианты ответа: 1. Сначала установить антивирус, затем пригласить аттестационную комиссию, а проблему со смежной стеной решить после получения аттестата. 2. Провести предпроектное обследование, обосновать установку системы виброакустической защиты и СЗИ от НСД, разработать документы согласно нормам СТР, провести приемочные испытания установленных средств и передать объект на аттестацию. 3. Написать научную статью о методах взлома защищенных стен, закупить любое зарубежное ПО для шифрования дисков и составить график дежурств сотрудников в коридоре для охраны стены	2. Устранение уязвимости стены на этапе проектирования - это предотвращение перехвата информации по виброакустическому каналу.
Система мониторинга зафиксировала 500 попыток входа под именем "admin" с внешнего IP-адреса за одну минуту. К какому типу инцидентов это относится? 1. Плановое обновление системы. 2. Инцидент типа «Brute-force» (подбор пароля), требующий немедленной блокировки IP-адреса. 3. Пользователь просто забыл пароль и часто нажимает Enter. 4. Технический сбой в работе сетевой карты.	2. Умение прогнозировать риски позволяет отличить штатную активность от аномальной. Массовые попытки авторизации - классический инцидент ИБ, требующий стандартного алгоритма реагирования для предотвращения взлома.

Критерии оценивания при ответе на вопросы:

- 100 баллов - при правильном и полном ответе на два вопроса;
- 85...99 баллов - при правильном и полном ответе на один из вопросов и правильном, но не полном ответе на другой из вопросов;
- 75...84 баллов - при правильном и неполном ответе на два вопроса;
- 65...74 баллов - правильном и полном ответе только на один из вопросов
- 25...64 - при правильном и неполном ответе только на один из вопросов;
- 0...24 баллов - при отсутствии правильных ответов на вопросы.

Количество баллов	0-64	65-100
Шкала оценивания	Не зачтено	Зачтено

Критерии оценивания при тестировании:

- 95-100 баллов - при правильном и полном ответе на 19-20 вопросов;
- 85...94 баллов - при правильном ответе на 16-18 вопросов;
- 75...84 баллов - при правильном ответе на 13-15 вопросов;
- 65...74 баллов - правильном ответе на 10-12 вопросов
- 25...64 - при правильном ответе только на 1-9 вопрос(ов);
- 0...24 баллов - при отсутствии правильных ответов на вопросы.

Количество баллов	0-24	25-64	65-74	85-94	95-100
Шкала оценивания	Неуд	Удовлетворительно		Хорошо	Отлично
	не зачтено	зачтено			

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ



1784258534

УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий

Содержание вопроса (задания)	Правильный ответ
Сотрудники компании начали массово использовать незащищенные мессенджеры для передачи рабочих файлов, так как корпоративная почта имеет жесткий лимит на объем вложений.	Провести системный анализ (бизнес-потребности и риски ИБ). Стратегия: внедрение корпоративного облачного хранилища с разграничением прав доступа вместо блокировок, мешающих работе.
Выявлено дублирование функций между отделом ИТ и службой ИБ при управлении учетными записями, что приводит к задержкам.	Разработка стратегии централизации управления через внедрение IdM-системы и четкое разделение зон ответственности в регламенте

ПК-1 Владеет методикой проведения предпроектного обследования объектов информатизации и выделенных(защищаемых) помещений

Содержание вопроса (задания)	Правильный ответ
Составьте перечень объектов обследования в выделенном помещении перед его аттестацией.	Определение границ контролируемой зоны, фиксация всех ОТСС и ВТСС(основные технические средства и системы вспомогательные технические средства и системы), проверка наличия инженерных коммуникаций, выходящих за пределы выделенного помещения.
Проведите обследование ЛВС филиала для выявления неучтенных точек доступа.	Использование сетевых сканеров и визуальный осмотр коммутационных узлов. Итогом является актуализированная топология сети.

ПК-2 Способен приводить аналитическое обоснование необходимости создания систем защиты информации

Содержание вопроса (задания)	Правильный ответ
Обоснуйте выбор между программным и аппаратно-программным модулем доверенной загрузки.	Сравнение по уровню контроля целостности: АПМДЗ блокирует доступ до загрузки ОС, что критично для защиты от подмены загрузчика.
Приведите обоснование установки межсетевого экрана нового поколения.	Анализ статистики атак прикладного уровня, которые не видит обычный L3-firewall.

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

Содержание вопроса (задания)	Правильный ответ
Укажите требования к хранению секретных носителей информации в нерабочее время.	Согласно нормам СТР, носители должны храниться в опечатываемых сейфах в специально оборудованных помещениях.
Опишите порядок маркировки системного блока, предназначенного для обработки секретных сведений.	Нанесение бирки с инвентарным номером, грифом секретности и подписью ответственного за эксплуатацию.

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

Содержание вопроса (задания)	Правильный ответ
Подготовьте проект программы и методики испытаний (ПМИ) автоматизированной системы.	Определение перечня проверок (парольная политика, антивирус, контроль целостности) и критериев успешности.
Какие действия необходимо предпринять при обнаружении несоответствия настройки СЗИ требованиям аттестата в ходе проверки?	Приостановка работ, корректировка настроек согласно ТЗ и повторное сканирование уязвимостей.

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

Содержание вопроса (задания)	Правильный ответ
Опишите процедуру тестирования системы обнаружения вторжений (СОВ).	Имитация типовых атак и фиксация срабатывания оповещений в журнале событий.



1784258534

Содержание вопроса (задания)	Правильный ответ
Составьте акт ввода в эксплуатацию подсистемы антивирусной защиты.	Подтверждение корректности установки на все узлы и настройки централизованного обновления баз.

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

Содержание вопроса (задания)	Правильный ответ
Спрогнозируйте риски при использовании администраторами общих учетных записей.	Невозможность персонализации ответственности при инциденте; риск несанкционированного изменения настроек без следа.
Разработайте алгоритм действий при обнаружении массовой рассылки фишинговых писем.	Блокировка адреса отправителя, удаление писем из почтовых ящиков, принудительный сброс паролей скомпрометированных пользователей.

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. 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.

2. Системы контроля и управления доступом к объекту информатизации : учебное пособие / составители А. Г. Киренберг [и др.]. — Кемерово : КузГТУ имени Т.Ф. Горбачева, 2023. — 128 с. — ISBN 978-5-00137-426-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/399767> (дата обращения: 07.09.2026). — Режим доступа: для авториз. пользователей.

3. Прокопенко, Е. В. Категорирование объектов критической информационной инфраструктуры : учебное пособие / Е. В. Прокопенко, В. О. Коротин. — Кемерово : КузГТУ имени Т.Ф. Горбачева, 2025. — 112 с. — ISBN 978-5-00137-535-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/516391> (дата обращения: 07.09.2026). — Режим доступа: для авториз. пользователей.

8.2 Дополнительная литература



1784258534

1. 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: <https://urait.ru/book/informacionnaya-bezopasnost-cheloveka-566457> (дата обращения: 07.09.2026). – Текст : электронный.

2. Щербак, А. В. Информационная безопасность : учебник для вузов / А. В. Щербак. — 2-е изд. — Москва : Издательство Юрайт, 2026. — 252 с. — (Высшее образование). — ISBN 978-5-9916-4299-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/589902> (дата обращения: 15.07.2026).

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: 07.09.2026). – 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. Справочная правовая система «КонсультантПлюс» <http://www.consultant.ru/>
8. 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.

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. Libre Office
2. Mozilla Firefox
3. Google Chrome
4. Opera
5. Yandex
6. Open Office



1784258534

7. Microsoft Windows
8. ESET NOD32 Smart Security Business Edition
9. Kaspersky Endpoint Security
10. 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 ("Соболь-4"); средство активной защиты информации от утечки за счет наводок информ сигнала на цепи заземления и электропитания ("Соната-PC3"); 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" 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:

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.

Специально оборудованный кабинет № 1019 представляет собой аудиторию – специальную библиотеку (библиотеку литературы ограниченного доступа), предназначенную для хранения и обеспечения использования в образовательном процессе нормативных и методических документов



1784258534

ограниченного доступа.

Перечень основного оборудования:

Специализированная мебель (столы и стулья).

Специальное помещение № 6308 представляет собой аудиторию (защищаемое помещение) для проведения учебных занятий, в ходе которых до обучающихся доводится информация ограниченного доступа, не содержащая сведений, составляющих государственную тайну. Аттестат соответствия №2601.49.22 от 09.09.2022.

Перечень основного оборудования:

Специализированная мебель (столы и стулья); АРМ, Аттестат соответствия №2601.48.22 от 09.09.2022

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:

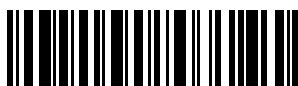
- разбор конкретных примеров;

- 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.



1784258534



1784258534