

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 15:57:42

Дубинкин Дмитрий Михайлович

Программа практики

Вид практики: Производственная

Тип практики: Проектно-технологическая 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.



1784087261

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.



1784087261

Рабочую программу составил:

ПОДПИСАНО ЭП КУЗГТУ

Подразделение: кафедра информационной безопасности

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

Дата: 17.07.2026 10:18:52

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 10:19:07

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 10:19:28

Прокопенко Евгения Викторовна



1784087261

1 Формы и способы проведения практики

Способ проведения практики: стационарная и(или) выездная.

Форма проведения практики: дискретно - путем чередования в календарном учебном графике периодов учебного времени для проведения практик с периодами учебного времени для проведения теоретических занятий.

Тип практики: Проектно-технологическая практика.

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

Освоение дисциплины направлено на формирование:

общепрофессиональных компетенций:

ОПК-3 - Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности;

ОПК-4 - Способен осуществлять сбор, обработку и анализ научно-технической информации по теме исследования, разрабатывать планы и программы проведения научных исследований и технических разработок;

ОПК-5 - Способен проводить научные исследования, включая экспериментальные, обрабатывать результаты исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи.

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

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

Результаты обучения по дисциплине определяются индикаторами достижения компетенций

Индикатор(ы) достижения:

Обосновывает требования к системе обеспечения информационной безопасности и способен разработать проект технического задания на ее создание.

Способен разработать технические проекты систем (подсистем) либо компонента системы обеспечения информационной безопасности.

Способен разработать проекты организационно-распорядительных документов по обеспечению информационной безопасности.

Осуществляет сбор, обработку и анализ научно-технической информации по теме исследования, разрабатывать планы и программы проведения научных исследований и технических разработок.

Проводит научные исследования, включая экспериментальные, обрабатывать результаты исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи.

Результаты обучения по дисциплине:

Знать уязвимости информационных ресурсов, возможные угрозы безопасности информации, информационные процессы объектов.

Знать основы организации защиты государственной тайны и конфиденциальной информации; методы анализа информационной безопасности объектов и систем; стандарты в области информационной безопасности.

Знать требования основных действующих государственных стандартов (ГОСТ) регламентирующие построение, проектирование и эксплуатацию информационных и аналитических систем.

Знать методы проектирования автоматизированных систем; основные принципы проектного управления.

Знать основные принципы экспериментальных исследований, соотношение теоретического и экспериментального знания, методику проведения экспериментов.

Иметь опыт формальной постановки и решения задачи обеспечения информационной безопасности компьютерных систем.

Иметь опыт разработки технических проектов систем (подсистем) либо компонента системы обеспечения информационной безопасности.

Иметь опыт разработки проектов организационно-распорядительных документов по обеспечению информационной безопасности.



1784087261

Иметь опыт сбора, обработки и анализа научно-технической информации по теме исследования, разрабатывать планы и программы проведения научных исследований и технических разработок.

Иметь опыт оформления научно-технических отчетов, обзоров, результатов выполненных исследований, научных докладов и статей.

Уметь определять информационные ресурсы, подлежащие защите информации, угрозы безопасности информации.

Уметь отечественные и зарубежные стандарты в области компьютерной безопасности и информационной безопасности объектов для проектирования, разработки и оценки защищенности компьютерных систем.

Уметь осуществлять подготовку технических заданий на построение и проектирование информационных и аналитических систем; осуществлять подготовку организационно-распорядительной документации (инструкции, приказы, распоряжения) регламентирующей эксплуатацию информационных систем.

Уметь проектировать и сопровождать типовые специализированные автоматизированные информационные системы, локальные сети; осуществлять подготовку технико-экономических обоснований соответствующих проектных решений.

Уметь разбираться в лабораторном оборудовании по профилю своей деятельности и работать с оборудованием для проведения экспериментов, применять методики, обрабатывать результаты, проводить оценку погрешности, проводить экспериментально-исследовательские работы системы защиты информации.

Владеть профессиональной терминологией в области обеспечения безопасности персональных данных; методами мониторинга и аудита, выявления угроз и управления информационной безопасностью.

Владеть методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов.

Владеть навыками оформления рабочей технической документации.

Владеть навыками определения затрат компании на информационную безопасность и проведения зависимости между затратами и уровнем защищенности.

Владеть навыками выполнения расчетов, обработки результатов экспериментов, оценки погрешностей и достоверности результатов, навыками проведения экспериментально-исследовательских работ системы защиты информации.

3 Место практики в структуре ОПОП магистратуры

Практика входит в обязательную 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/п	Этапы практики	Виды учебной работы	Часы
-------	----------------	---------------------	------



1784087261

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.	Совершенствование навыков использования современных средств и инструментов информационной безопасности, работа с нормативными документами организации, знакомство с основными бизнес- процессами. Участие в осуществлении бизнес-процессов конкретной организации в соответствии с планом практики и поставленной индивидуальной задачей. Выполнение задания по поручению и под наблюдением работника отдела информационной безопасности (руководителя или специалиста ИТ-отдела, инженера по информационной безопасности). Участие в работе отдела в качестве наблюдателя. Изучение проблем, уязвимостей в сетях предприятия. Осуществление сбора, обработки, анализа и систематизации информации по этапам и процессам осуществления информационной безопасности. Анализ выбранного этапа осуществления информационной безопасности. Анализ документации и электронных ресурсов организации. 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. Осуществляет сбор, обработку и анализ научно-технической информации по теме исследования, разрабатывать планы и программы проведения научных исследований и технических разработок. Проводит научные исследования, включая экспериментальные, обрабатывать результаты исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи.	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.



1784087261

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 комплектка 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	Компетенции, формируемые в результате освоения дисциплины (модуля)	Индикатор(ы) достижения компетенции	Результаты обучения по дисциплине (модулю)	Уровень



1784087261

собеседование по материалам, собранным в результате прохождения каждого этапа практики	ОПК-1	Обосновывает требования к системе обеспечения информационной безопасности и способен разработать проект технического задания на ее создание	Знать уязвимости информационных ресурсов, возможные угрозы безопасности информации, информационные процессы объектов. Уметь определять информационные ресурсы, подлежащие защите информации, угрозы безопасности информации. Владеть профессиональной терминологией в области обеспечения безопасности персональных данных; методами мониторинга и аудита, выявления угроз и управления информационной безопасностью. Иметь опыт формальной постановки и решения задачи обеспечения информационной безопасности компьютерных систем.	Высокий или средний
собеседование по материалам, собранным в результате прохождения каждого этапа практики	ОПК-2	Способен разработать технические проекты систем (подсистем) либо компонента системы обеспечения информационной безопасности	Знать основы организации защиты государственной тайны и конфиденциальной информации; методы анализа информационной безопасности объектов и систем; стандарты в области информационной безопасности. Уметь отечественные и зарубежные стандарты в области компьютерной безопасности и информационной безопасности объектов для проектирования, разработки и оценки защищенности компьютерных систем. Владеть методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов. Иметь опыт разработки технических проектов систем (подсистем) либо компонента системы обеспечения информационной безопасности.	Высокий или средний
собеседование по материалам, собранным в результате прохождения каждого этапа практики	ОПК-3	Способен разработать проекты организационно-распорядительных документов по обеспечению информационной безопасности	Знать требования основных действующих государственных стандартов (ГОСТ) регламентирующие построение, проектирование и эксплуатацию информационных и аналитических систем. Уметь осуществлять подготовку технических заданий на построение и проектирование информационных и аналитических систем; осуществлять подготовку организационно-распорядительной документации (инструкции, приказы, распоряжения) регламентирующей эксплуатацию информационных систем. Владеть навыками оформления рабочей технической документации. Иметь опыт разработки проектов организационно-распорядительных документов по обеспечению информационной безопасности.	Высокий или средний



1784087261

собеседование по материалам, собранным в результате прохождения каждого этапа практики	ОПК-4	Осуществляет сбор, обработку и анализ научно-технической информации по теме исследования, разрабатывать планы и программы проведения научных исследований и технических разработок	Знать методы проектирования автоматизированных систем; основные принципы проектного управления. Уметь проектировать и сопровождать типовые специализированные автоматизированные информационные системы, локальные сети; осуществлять подготовку технико-экономических обоснований соответствующих проектных решений. Владеть навыками определения затрат компании на информационную безопасность и проведения зависимости между затратами и уровнем защищенности. Иметь опыт сбора, обработки и анализа научно-технической информации по теме исследования, разрабатывать планы и программы проведения научных исследований и технических разработок.	Высокий или средний
собеседование по материалам, собранным в результате прохождения каждого этапа практики	ОПК-5	Проводит научные исследования, включая экспериментальные, обрабатывать результаты исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи	Знать основные принципы экспериментальных исследований, соотношение теоретического и экспериментального знания, методику проведения экспериментал Уметь разбираться в лабораторном оборудовании по профилю своей деятельности и работать с оборудованием для проведения экспериментов, применять методики, обрабатывать результаты, проводить оценку погрешности, проводить экспериментально-исследовательские работы системы защиты информации. Владеть навыками выполнения расчетов, обработки результатов экспериментов, оценки погрешностей и достоверности результатов, навыками проведения экспериментально-исследовательских работ системы защиты информации. Иметь опыт оформления научно-технических отчетов, обзоров, результатов выполненных исследований, научных докладов и статей.	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 ЭИОС КузГТУ.

Примерные вопросы собеседования:



1784087261

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

Содержание вопроса (задания)	Правильный ответ
«Выбор и внедрение системы обнаружения вторжений (IDS/IPS)». Вам необходимо защитить периметр сети организации от сетевых атак. Руководство предлагает выбрать один из трех вариантов реализации системы обнаружения и предотвращения вторжений (IDS/IPS). Какое решение является наиболее полным и корректным с точки зрения проектирования системы ИБ в соответствии с государственными стандартами и требованиями регуляторов? Выберите правильный ответ и объясните свой выбор. Варианты ответа: 1. Установка бесплатной Open Source IDS Snort на старый офисный компьютер без оформления документации. 2. Закупка и внедрение программно-аппаратного комплекса (ПАК) класса IPS, имеющего действующий сертификат ФСТЭК России, с последующей разработкой ТЗ, Технического проекта и Инструкции администратора. 3. Написание собственного уникального алгоритма анализа трафика на языке Python и его запуск на сервере компании для проведения научного эксперимента без интеграции в общую систему защиты.	2
«Внедрение системы управления доступом». В компании используется файловый сервер с общими папками, доступ к которым выдается вручную администратором. В необходимо модернизировать этот процесс, так как количество ошибок доступа (утечек) возросло. Необходимо выбрать стратегию действий. Какая последовательность действий является методологически верной для реализации полноценного цикла защиты информации? Варианты ответа: 1. Срочно запретить доступ всем сотрудникам к серверу и разрешать его только по личному звонку руководителю, не составляя никаких документов. 2. Написать научную статью о методах биометрической идентификации в будущем, не предлагая решения для текущей проблемы компании. 3. Проанализировать существующие угрозы, разработать проект ТЗ на внедрение системы централизованного управления доступом, спроектировать схему её интеграции в сеть, подготовить регламент парольной политики и провести тестирование системы на устойчивость к попыткам несанкционированного входа.	3

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

Содержание вопроса (задания)	Правильный ответ
«Выбор и внедрение системы обнаружения вторжений (IDS/IPS)». Вам необходимо защитить периметр сети организации от сетевых атак. Руководство предлагает выбрать один из трех вариантов реализации системы обнаружения и предотвращения вторжений (IDS/IPS). Какое решение является наиболее полным и корректным с точки зрения проектирования системы ИБ в соответствии с государственными стандартами и требованиями регуляторов? Выберите правильный ответ и объясните свой выбор. Варианты ответа: 1. Установка бесплатной Open Source IDS Snort на старый офисный компьютер без оформления документации. 2. Закупка и внедрение программно-аппаратного комплекса (ПАК) класса IPS, имеющего действующий сертификат ФСТЭК России, с последующей разработкой ТЗ, Технического проекта и Инструкции администратора. 3. Написание собственного уникального алгоритма анализа трафика на языке Python и его запуск на сервере компании для проведения научного эксперимента без интеграции в общую систему защиты.	2



1784087261

Содержание вопроса (задания)	Правильный ответ
«Внедрение системы управления доступом». В компании используется файловый сервер с общими папками, доступ к которым выдается вручную администратором. В необходимо модернизировать этот процесс, так как количество ошибок доступа (утечек) возросло. Необходимо выбрать стратегию действий. Какая последовательность действий является методологически верной для реализации полноценного цикла защиты информации? Варианты ответа: 1. Срочно запретить доступ всем сотрудникам к серверу и разрешать его только по личному звонку руководителю, не составляя никаких документов. 2. Написать научную статью о методах биометрической идентификации в будущем, не предлагая решения для текущей проблемы компании. 3. Проанализировать существующие угрозы, разработать проект ТЗ на внедрение системы централизованного управления доступом, спроектировать схему её интеграции в сеть, подготовить регламент парольной политики и провести тестирование системы на устойчивость к попыткам несанкционированного входа.	3

ОПК-3 Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности;

Содержание вопроса (задания)	Правильный ответ
«Выбор и внедрение системы обнаружения вторжений (IDS/IPS)». Вам необходимо защитить периметр сети организации от сетевых атак. Руководство предлагает выбрать один из трех вариантов реализации системы обнаружения и предотвращения вторжений (IDS/IPS). Какое решение является наиболее полным и корректным с точки зрения проектирования системы ИБ в соответствии с государственными стандартами и требованиями регуляторов? Выберите правильный ответ и объясните свой выбора. Варианты ответа: 1. Установка бесплатной Open Source IDS Snort на старый офисный компьютер без оформления документации. 2. Закупка и внедрение программно-аппаратного комплекса (ПАК) класса IPS, имеющего действующий сертификат ФСТЭК России, с последующей разработкой ТЗ, Технического проекта и Инструкции администратора. 3. Написание собственного уникального алгоритма анализа трафика на языке Python и его запуск на сервере компании для проведения научного эксперимента без интеграции в общую систему защиты.	2
«Внедрение системы управления доступом». В компании используется файловый сервер с общими папками, доступ к которым выдается вручную администратором. В необходимо модернизировать этот процесс, так как количество ошибок доступа (утечек) возросло. Необходимо выбрать стратегию действий. Какая последовательность действий является методологически верной для реализации полноценного цикла защиты информации? Варианты ответа: 1. Срочно запретить доступ всем сотрудникам к серверу и разрешать его только по личному звонку руководителю, не составляя никаких документов. 2. Написать научную статью о методах биометрической идентификации в будущем, не предлагая решения для текущей проблемы компании. 3. Проанализировать существующие угрозы, разработать проект ТЗ на внедрение системы централизованного управления доступом, спроектировать схему её интеграции в сеть, подготовить регламент парольной политики и провести тестирование системы на устойчивость к попыткам несанкционированного входа.	3

ОПК-4 Способен осуществлять сбор, обработку и анализ научно-технической информации по теме исследования, разрабатывать планы и программы проведения научных исследований и технических разработок;



1784087261

Содержание вопроса (задания)	Правильный ответ
«Выбор и внедрение системы обнаружения вторжений (IDS/IPS)». Вам необходимо защитить периметр сети организации от сетевых атак. Руководство предлагает выбрать один из трех вариантов реализации системы обнаружения и предотвращения вторжений (IDS/IPS). Какое решение является наиболее полным и корректным с точки зрения проектирования системы ИБ в соответствии с государственными стандартами и требованиями регуляторов? Выберите правильный ответ и объясните свой выбор. Варианты ответа: 1. Установка бесплатной Open Source IDS Snort на старый офисный компьютер без оформления документации. 2. Закупка и внедрение программно-аппаратного комплекса (ПАК) класса IPS, имеющего действующий сертификат ФСТЭК России, с последующей разработкой ТЗ, Технического проекта и Инструкции администратора. 3. Написание собственного уникального алгоритма анализа трафика на языке Python и его запуск на сервере компании для проведения научного эксперимента без интеграции в общую систему защиты.	2
«Внедрение системы управления доступом». В компании используется файловый сервер с общими папками, доступ к которым выдается вручную администратором. В необходимо модернизировать этот процесс, так как количество ошибок доступа (утечек) возросло. Необходимо выбрать стратегию действий. Какая последовательность действий является методологически верной для реализации полноценного цикла защиты информации? Варианты ответа: 1. Срочно запретить доступ всем сотрудникам к серверу и разрешать его только по личному звонку руководителю, не составляя никаких документов. 2. Написать научную статью о методах биометрической идентификации в будущем, не предлагая решения для текущей проблемы компании. 3. Проанализировать существующие угрозы, разработать проект ТЗ на внедрение системы централизованного управления доступом, спроектировать схему её интеграции в сеть, подготовить регламент парольной политики и провести тестирование системы на устойчивость к попыткам несанкционированного входа.	3

ОПК-5 Способен проводить научные исследования, включая экспериментальные, обрабатывать результаты исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи.

Содержание вопроса (задания)	Правильный ответ
«Выбор и внедрение системы обнаружения вторжений (IDS/IPS)». Вам необходимо защитить периметр сети организации от сетевых атак. Руководство предлагает выбрать один из трех вариантов реализации системы обнаружения и предотвращения вторжений (IDS/IPS). Какое решение является наиболее полным и корректным с точки зрения проектирования системы ИБ в соответствии с государственными стандартами и требованиями регуляторов? Выберите правильный ответ и объясните свой выбор. Варианты ответа: 1. Установка бесплатной Open Source IDS Snort на старый офисный компьютер без оформления документации. 2. Закупка и внедрение программно-аппаратного комплекса (ПАК) класса IPS, имеющего действующий сертификат ФСТЭК России, с последующей разработкой ТЗ, Технического проекта и Инструкции администратора. 3. Написание собственного уникального алгоритма анализа трафика на языке Python и его запуск на сервере компании для проведения научного эксперимента без интеграции в общую систему защиты.	2



1784087261

Содержание вопроса (задания)	Правильный ответ
«Внедрение системы управления доступом». В компании используется файловый сервер с общими папками, доступ к которым выдается вручную администратором. В необходимо модернизировать этот процесс, так как количество ошибок доступа (утечек) возросло. Необходимо выбрать стратегию действий. Какая последовательность действий является методологически верной для реализации полноценного цикла защиты информации? Варианты ответа: 1. Срочно запретить доступ всем сотрудникам к серверу и разрешать его только по личному звонку руководителю, не составляя никаких документов. 2. Написать научную статью о методах биометрической идентификации в будущем, не предлагая решения для текущей проблемы компании. 3. Проанализировать существующие угрозы, разработать проект ТЗ на внедрение системы централизованного управления доступом, спроектировать схему её интеграции в сеть, подготовить регламент парольной политики и провести тестирование системы на устойчивость к попыткам несанкционированного входа.	3

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;
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.

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)



1784087261

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
- 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:

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

Содержание вопроса (задания)	Правильный ответ
«Выбор и внедрение системы обнаружения вторжений (IDS/IPS)». Вам необходимо защитить периметр сети организации от сетевых атак. Руководство предлагает выбрать один из трех вариантов реализации системы обнаружения и предотвращения вторжений (IDS/IPS). Какое решение является наиболее полным и корректным с точки зрения проектирования системы ИБ в соответствии с государственными стандартами и требованиями регуляторов? Выберите правильный ответ и объясните свой выбор. Варианты ответа: 1. Установка бесплатной Open Source IDS Snort на старый офисный компьютер без оформления документации. 2. Закупка и внедрение программно-аппаратного комплекса (ПАК) класса IPS, имеющего действующий сертификат ФСТЭК России, с последующей разработкой ТЗ, Технического проекта и Инструкции администратора. 3. Написание собственного уникального алгоритма анализа трафика на языке Python и его запуск на сервере компании для проведения научного эксперимента без интеграции в общую систему защиты.	2
«Внедрение системы управления доступом». В компании используется файловый сервер с общими папками, доступ к которым выдается вручную администратором. В необходимо модернизировать этот процесс, так как количество ошибок доступа (утечек) возросло. Необходимо выбрать стратегию действий. Какая последовательность действий является методологически верной для реализации полноценного цикла защиты информации? Варианты ответа: 1. Срочно запретить доступ всем сотрудникам к серверу и разрешать его только по личному звонку руководителю, не составляя никаких документов. 2. Написать научную статью о методах биометрической идентификации в будущем, не предлагая решения для текущей проблемы компании. 3. Проанализировать существующие угрозы, разработать проект ТЗ на внедрение системы централизованного управления доступом, спроектировать схему её интеграции в сеть, подготовить регламент парольной политики и провести тестирование системы на устойчивость к попыткам несанкционированного входа.	3

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



1784087261

Содержание вопроса (задания)	Правильный ответ
«Выбор и внедрение системы обнаружения вторжений (IDS/IPS)». Вам необходимо защитить периметр сети организации от сетевых атак. Руководство предлагает выбрать один из трех вариантов реализации системы обнаружения и предотвращения вторжений (IDS/IPS). Какое решение является наиболее полным и корректным с точки зрения проектирования системы ИБ в соответствии с государственными стандартами и требованиями регуляторов? Выберите правильный ответ и объясните свой выбор. Варианты ответа: 1. Установка бесплатной Open Source IDS Snort на старый офисный компьютер без оформления документации. 2. Закупка и внедрение программно-аппаратного комплекса (ПАК) класса IPS, имеющего действующий сертификат ФСТЭК России, с последующей разработкой ТЗ, Технического проекта и Инструкции администратора. 3. Написание собственного уникального алгоритма анализа трафика на языке Python и его запуск на сервере компании для проведения научного эксперимента без интеграции в общую систему защиты.	2
«Внедрение системы управления доступом». В компании используется файловый сервер с общими папками, доступ к которым выдается вручную администратором. В необходимо модернизировать этот процесс, так как количество ошибок доступа (утечек) возросло. Необходимо выбрать стратегию действий. Какая последовательность действий является методологически верной для реализации полноценного цикла защиты информации? Варианты ответа: 1. Срочно запретить доступ всем сотрудникам к серверу и разрешать его только по личному звонку руководителю, не составляя никаких документов. 2. Написать научную статью о методах биометрической идентификации в будущем, не предлагая решения для текущей проблемы компании. 3. Проанализировать существующие угрозы, разработать проект ТЗ на внедрение системы централизованного управления доступом, спроектировать схему её интеграции в сеть, подготовить регламент парольной политики и провести тестирование системы на устойчивость к попыткам несанкционированного входа.	3

ОПК-3 Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности;

Содержание вопроса (задания)	Правильный ответ
«Выбор и внедрение системы обнаружения вторжений (IDS/IPS)». Вам необходимо защитить периметр сети организации от сетевых атак. Руководство предлагает выбрать один из трех вариантов реализации системы обнаружения и предотвращения вторжений (IDS/IPS). Какое решение является наиболее полным и корректным с точки зрения проектирования системы ИБ в соответствии с государственными стандартами и требованиями регуляторов? Выберите правильный ответ и объясните свой выбор. Варианты ответа: 1. Установка бесплатной Open Source IDS Snort на старый офисный компьютер без оформления документации. 2. Закупка и внедрение программно-аппаратного комплекса (ПАК) класса IPS, имеющего действующий сертификат ФСТЭК России, с последующей разработкой ТЗ, Технического проекта и Инструкции администратора. 3. Написание собственного уникального алгоритма анализа трафика на языке Python и его запуск на сервере компании для проведения научного эксперимента без интеграции в общую систему защиты.	2



1784087261

Содержание вопроса (задания)	Правильный ответ
«Внедрение системы управления доступом». В компании используется файловый сервер с общими папками, доступ к которым выдается вручную администратором. В необходимо модернизировать этот процесс, так как количество ошибок доступа (утечек) возросло. Необходимо выбрать стратегию действий. Какая последовательность действий является методологически верной для реализации полноценного цикла защиты информации? Варианты ответа: 1. Срочно запретить доступ всем сотрудникам к серверу и разрешать его только по личному звонку руководителю, не составляя никаких документов. 2. Написать научную статью о методах биометрической идентификации в будущем, не предлагая решения для текущей проблемы компании. 3. Проанализировать существующие угрозы, разработать проект ТЗ на внедрение системы централизованного управления доступом, спроектировать схему её интеграции в сеть, подготовить регламент парольной политики и провести тестирование системы на устойчивость к попыткам несанкционированного входа.	3

ОПК-4 Способен осуществлять сбор, обработку и анализ научно-технической информации по теме исследования, разрабатывать планы и программы проведения научных исследований и технических разработок;

Содержание вопроса (задания)	Правильный ответ
«Выбор и внедрение системы обнаружения вторжений (IDS/IPS)». Вам необходимо защитить периметр сети организации от сетевых атак. Руководство предлагает выбрать один из трех вариантов реализации системы обнаружения и предотвращения вторжений (IDS/IPS). Какое решение является наиболее полным и корректным с точки зрения проектирования системы ИБ в соответствии с государственными стандартами и требованиями регуляторов? Выберите правильный ответ и объясните свой выбора. Варианты ответа: 1. Установка бесплатной Open Source IDS Snort на старый офисный компьютер без оформления документации. 2. Закупка и внедрение программно-аппаратного комплекса (ПАК) класса IPS, имеющего действующий сертификат ФСТЭК России, с последующей разработкой ТЗ, Технического проекта и Инструкции администратора. 3. Написание собственного уникального алгоритма анализа трафика на языке Python и его запуск на сервере компании для проведения научного эксперимента без интеграции в общую систему защиты.	2
«Внедрение системы управления доступом». В компании используется файловый сервер с общими папками, доступ к которым выдается вручную администратором. В необходимо модернизировать этот процесс, так как количество ошибок доступа (утечек) возросло. Необходимо выбрать стратегию действий. Какая последовательность действий является методологически верной для реализации полноценного цикла защиты информации? Варианты ответа: 1. Срочно запретить доступ всем сотрудникам к серверу и разрешать его только по личному звонку руководителю, не составляя никаких документов. 2. Написать научную статью о методах биометрической идентификации в будущем, не предлагая решения для текущей проблемы компании. 3. Проанализировать существующие угрозы, разработать проект ТЗ на внедрение системы централизованного управления доступом, спроектировать схему её интеграции в сеть, подготовить регламент парольной политики и провести тестирование системы на устойчивость к попыткам несанкционированного входа.	3

ОПК-5 Способен проводить научные исследования, включая экспериментальные, обрабатывать результаты исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи.



1784087261

Содержание вопроса (задания)	Правильный ответ
«Выбор и внедрение системы обнаружения вторжений (IDS/IPS)». Вам необходимо защитить периметр сети организации от сетевых атак. Руководство предлагает выбрать один из трех вариантов реализации системы обнаружения и предотвращения вторжений (IDS/IPS). Какое решение является наиболее полным и корректным с точки зрения проектирования системы ИБ в соответствии с государственными стандартами и требованиями регуляторов? Выберите правильный ответ и объясните свой выбор. Варианты ответа: 1. Установка бесплатной Open Source IDS Snort на старый офисный компьютер без оформления документации. 2. Закупка и внедрение программно-аппаратного комплекса (ПАК) класса IPS, имеющего действующий сертификат ФСТЭК России, с последующей разработкой ТЗ, Технического проекта и Инструкции администратора. 3. Написание собственного уникального алгоритма анализа трафика на языке Python и его запуск на сервере компании для проведения научного эксперимента без интеграции в общую систему защиты.	2
«Внедрение системы управления доступом». В компании используется файловый сервер с общими папками, доступ к которым выдается вручную администратором. В необходимо модернизировать этот процесс, так как количество ошибок доступа (утечек) возросло. Необходимо выбрать стратегию действий. Какая последовательность действий является методологически верной для реализации полноценного цикла защиты информации? Варианты ответа: 1. Срочно запретить доступ всем сотрудникам к серверу и разрешать его только по личному звонку руководителю, не составляя никаких документов. 2. Написать научную статью о методах биометрической идентификации в будущем, не предлагая решения для текущей проблемы компании. 3. Проанализировать существующие угрозы, разработать проект ТЗ на внедрение системы централизованного управления доступом, спроектировать схему её интеграции в сеть, подготовить регламент парольной политики и провести тестирование системы на устойчивость к попыткам несанкционированного входа.	3

Критерии оценивания при тестировании:

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

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

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

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

Содержание вопроса (задания)	Правильный ответ
Кейс-задача: «Организация защищенного удаленного доступа к корпоративной сети». Руководство компании приняло решение перевести ИТ-отдел на удаленный режим работы. Вам, как специалисту по защите информации, поручено реализовать проект по обеспечению безопасности этого процесса. Задание: Обоснуйте выбор технологии доступа и сформулируйте одно ключевое требование для раздела ТЗ «Технические требования».	Для защиты данных при передаче через интернет необходимо использовать технологию VPN. Это обосновано необходимостью создания защищенного канала между домашним ПК и офисом.



1784087261

Содержание вопроса (задания)	Правильный ответ
Кейс-задача: «Внедрение системы защиты от утечек (DLP) в юридическом департаменте». В юридическом департаменте крупной компании участились случаи случайной пересылки конфиденциальных договоров на личные адреса сотрудников. Вам поручено проработать вопрос внедрения системы контроля почтового трафика. Задание: Обоснуйте необходимость внедрения DLP-системы для почты и сформулируйте одно требование к функционалу для ТЗ.	Юридическая документация содержит коммерческую тайну и персональные данные. Утечка таких сведений грозит компании репутационными рисками и штрафами. DLP-система необходима для автоматического блокирования писем, содержащих ключевые слова (например, «Договор №», «Конфиденциально»).
«Выбор и внедрение системы обнаружения вторжений (IDS/IPS)». Вам необходимо защитить периметр сети организации от сетевых атак. Руководство предлагает выбрать один из трех вариантов реализации системы обнаружения и предотвращения вторжений (IDS/IPS). Какое решение является наиболее полным и корректным с точки зрения проектирования системы ИБ в соответствии с государственными стандартами и требованиями регуляторов? Выберите правильный ответ и объясните свой выбор. Варианты ответа: 1. Установка бесплатной Open Source IDS Snort на старый офисный компьютер без оформления документации. 2. Закупка и внедрение программно-аппаратного комплекса (ПАК) класса IPS, имеющего действующий сертификат ФСТЭК России, с последующей разработкой ТЗ, Технического проекта и Инструкции администратора. 3. Написание собственного уникального алгоритма анализа трафика на языке Python и его запуск на сервере компании для проведения научного эксперимента без интеграции в общую систему защиты.	2
«Внедрение системы управления доступом». В компании используется файловый сервер с общими папками, доступ к которым выдается вручную администратором. В необходимо модернизировать этот процесс, так как количество ошибок доступа (утечек) возросло. Необходимо выбрать стратегию действий. Какая последовательность действий является методологически верной для реализации полноценного цикла защиты информации? Варианты ответа: 1. Срочно запретить доступ всем сотрудникам к серверу и разрешать его только по личному звонку руководителю, не составляя никаких документов. 2. Написать научную статью о методах биометрической идентификации в будущем, не предлагая решения для текущей проблемы компании. 3. Проанализировать существующие угрозы, разработать проект ТЗ на внедрение системы централизованного управления доступом, спроектировать схему её интеграции в сеть, подготовить регламент парольной политики и провести тестирование системы на устойчивость к попыткам несанкционированного входа.	3

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



1784087261

Содержание вопроса (задания)	Правильный ответ
Кейс-задача: «Организация защищенного удаленного доступа к корпоративной сети». Руководство компании приняло решение перевести ИТ-отдел на удаленный режим работы. Вам, как специалисту по защите информации, поручено реализовать проект по обеспечению безопасности этого процесса. Задание: Разработайте концептуальную схему размещения оборудования. Где именно в сети должен находиться VPN-шлюз?	VPN-шлюз следует разместить в качестве пограничного устройства между интернетом и внутренней сетью. Он должен находиться перед внутренним межсетевым экраном, чтобы трафик проверялся до попадания в основной сегмент сети.
Кейс-задача: «Внедрение системы защиты от утечек (DLP) в юридическом департаменте». В юридическом департаменте крупной компании участились случаи случайной пересылки конфиденциальных договоров на личные адреса сотрудников. Вам поручено проработать вопрос внедрения системы контроля почтового трафика. Задание: Определите место установки DLP-шлюза в сетевой инфраструктуре. Как он должен взаимодействовать с почтовым сервером?	DLP-шлюз следует интегрировать с корпоративным почтовым сервером по протоколу SMTP (в разрыв) или через Smart Host. Почтовый сервер должен перенаправлять все исходящие сообщения на DLP-шлюз для анализа перед их фактической отправкой во внешнюю сеть.
«Выбор и внедрение системы обнаружения вторжений (IDS/IPS)». Вам необходимо защитить периметр сети организации от сетевых атак. Руководство предлагает выбрать один из трех вариантов реализации системы обнаружения и предотвращения вторжений (IDS/IPS). Какое решение является наиболее полным и корректным с точки зрения проектирования системы ИБ в соответствии с государственными стандартами и требованиями регуляторов? Выберите правильный ответ и объясните свой выбор. Варианты ответа: 1. Установка бесплатной Open Source IDS Snort на старый офисный компьютер без оформления документации. 2. Закупка и внедрение программно-аппаратного комплекса (ПАК) класса IPS, имеющего действующий сертификат ФСТЭК России, с последующей разработкой ТЗ, Технического проекта и Инструкции администратора. 3. Написание собственного уникального алгоритма анализа трафика на языке Python и его запуск на сервере компании для проведения научного эксперимента без интеграции в общую систему защиты.	2
«Внедрение системы управления доступом». В компании используется файловый сервер с общими папками, доступ к которым выдается вручную администратором. В необходимо модернизировать этот процесс, так как количество ошибок доступа (утечек) возросло. Необходимо выбрать стратегию действий. Какая последовательность действий является методологически верной для реализации полноценного цикла защиты информации? Варианты ответа: 1. Срочно запретить доступ всем сотрудникам к серверу и разрешать его только по личному звонку руководителю, не составляя никаких документов. 2. Написать научную статью о методах биометрической идентификации в будущем, не предлагая решения для текущей проблемы компании. 3. Проанализировать существующие угрозы, разработать проект ТЗ на внедрение системы централизованного управления доступом, спроектировать схему её интеграции в сеть, подготовить регламент парольной политики и провести тестирование системы на устойчивость к попыткам несанкционированного входа.	3

ОПК-3 Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности;



Содержание вопроса (задания)	Правильный ответ
Кейс-задача: «Организация защищенного удаленного доступа к корпоративной сети». Руководство компании приняло решение перевести ИТ-отдел на удаленный режим работы. Вам, как специалисту по защите информации, поручено реализовать проект по обеспечению безопасности этого процесса. Задание: Подготовьте структуру краткого приказа о введении режима удаленной работы с точки зрения ИБ.	Документ должен включать: 1. Список сотрудников, допущенных к удаленной работе. 2. Обязанность сотрудников использовать только корпоративное ПО для связи. 3. Запрет на передачу учетных данных третьим лицам. 4. Ответственность за нарушение правил работы с конфиденциальной информацией.
Кейс-задача: «Внедрение системы защиты от утечек (DLP) в юридическом департаменте». В юридическом департаменте крупной компании участились случаи случайной пересылки конфиденциальных договоров на личные адреса сотрудников. Вам поручено проработать вопрос внедрения системы контроля почтового трафика. Задание: Какой локальный нормативный акт необходимо разработать, чтобы проверка почты сотрудников была законной? Перечислите 2 ключевых раздела этого документа.	Необходимо разработать «Положение о порядке использования корпоративной электронной почты». Разделы: 1. Уведомление сотрудников о том, что почта используется исключительно в рабочих целях и подлежит автоматизированному контролю. 2. Ответственность за попытки обхода средств защиты информации.
«Выбор и внедрение системы обнаружения вторжений (IDS/IPS)». Вам необходимо защитить периметр сети организации от сетевых атак. Руководство предлагает выбрать один из трех вариантов реализации системы обнаружения и предотвращения вторжений (IDS/IPS). Какое решение является наиболее полным и корректным с точки зрения проектирования системы ИБ в соответствии с государственными стандартами и требованиями регуляторов? Выберите правильный ответ и объясните свой выбор. Варианты ответа: 1. Установка бесплатной Open Source IDS Snort на старый офисный компьютер без оформления документации. 2. Закупка и внедрение программно-аппаратного комплекса (ПАК) класса IPS, имеющего действующий сертификат ФСТЭК России, с последующей разработкой ТЗ, Технического проекта и Инструкции администратора. 3. Написание собственного уникального алгоритма анализа трафика на языке Python и его запуск на сервере компании для проведения научного эксперимента без интеграции в общую систему защиты.	2
«Внедрение системы управления доступом». В компании используется файловый сервер с общими папками, доступ к которым выдается вручную администратором. В необходимо модернизировать этот процесс, так как количество ошибок доступа (утечек) возросло. Необходимо выбрать стратегию действий. Какая последовательность действий является методологически верной для реализации полноценного цикла защиты информации? Варианты ответа: 1. Срочно запретить доступ всем сотрудникам к серверу и разрешать его только по личному звонку руководителю, не составляя никаких документов. 2. Написать научную статью о методах биометрической идентификации в будущем, не предлагая решения для текущей проблемы компании. 3. Проанализировать существующие угрозы, разработать проект ТЗ на внедрение системы централизованного управления доступом, спроектировать схему её интеграции в сеть, подготовить регламент парольной политики и провести тестирование системы на устойчивость к попыткам несанкционированного входа.	3

ОПК-4 Способен осуществлять сбор, обработку и анализ научно-технической информации по



1784087261

теме исследования, разрабатывать планы и программы проведения научных исследований и технических разработок;

Содержание вопроса (задания)	Правильный ответ
Кейс-задача: «Организация защищенного удаленного доступа к корпоративной сети». Руководство компании приняло решение перевести ИТ-отдел на удаленный режим работы. Вам, как специалисту по защите информации, поручено реализовать проект по обеспечению безопасности этого процесса. Задание: Составьте план сравнительного анализа двух решений для VPN.	План включает: 1. Поиск документации и отзывов об уязвимостях обоих протоколов. 2. Сравнение поддерживаемых алгоритмов шифрования. 3. Анализ сложности настройки и поддержки. 4. Оценка производительности на основе технических обзоров.
Кейс-задача: «Внедрение системы защиты от утечек (DLP) в юридическом департаменте». В юридическом департаменте крупной компании участились случаи случайной пересылки конфиденциальных договоров на личные адреса сотрудников. Вам поручено проработать вопрос внедрения системы контроля почтового трафика. Задание: Составьте план поиска информации для выбора между «коробочным» DLP-решением и Open Source аналогом.	1. Изучение реестра отечественного ПО для подбора решений, соответствующих требованиям импортозамещения. 2. Анализ документации вендоров для оценки качества лингвистического анализа. 3. Сбор статистики по известным уязвимостям выбранных решений в базах БДУ ФСТЭК.
«Выбор и внедрение системы обнаружения вторжений (IDS/IPS)». Вам необходимо защитить периметр сети организации от сетевых атак. Руководство предлагает выбрать один из трех вариантов реализации системы обнаружения и предотвращения вторжений (IDS/IPS). Какое решение является наиболее полным и корректным с точки зрения проектирования системы ИБ в соответствии с государственными стандартами и требованиями регуляторов? Выберите правильный ответ и объясните свой выбор. Варианты ответа: 1. Установка бесплатной Open Source IDS Snort на старый офисный компьютер без оформления документации. 2. Закупка и внедрение программно-аппаратного комплекса (ПАК) класса IPS, имеющего действующий сертификат ФСТЭК России, с последующей разработкой ТЗ, Технического проекта и Инструкции администратора. 3. Написание собственного уникального алгоритма анализа трафика на языке Python и его запуск на сервере компании для проведения научного эксперимента без интеграции в общую систему защиты.	2
«Внедрение системы управления доступом». В компании используется файловый сервер с общими папками, доступ к которым выдается вручную администратором. В необходимо модернизировать этот процесс, так как количество ошибок доступа (утечек) возросло. Необходимо выбрать стратегию действий. Какая последовательность действий является методологически верной для реализации полноценного цикла защиты информации? Варианты ответа: 1. Срочно запретить доступ всем сотрудникам к серверу и разрешать его только по личному звонку руководителю, не составляя никаких документов. 2. Написать научную статью о методах биометрической идентификации в будущем, не предлагая решения для текущей проблемы компании. 3. Проанализировать существующие угрозы, разработать проект ТЗ на внедрение системы централизованного управления доступом, спроектировать схему её интеграции в сеть, подготовить регламент парольной политики и провести тестирование системы на устойчивость к попыткам несанкционированного входа.	3

ОПК-5 Способен проводить научные исследования, включая экспериментальные, обрабатывать результаты исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам



1784087261

выполненных исследований научные доклады и статьи.

Содержание вопроса (задания)	Правильный ответ
Кейс-задача: «Организация защищенного удаленного доступа к корпоративной сети». Руководство компании приняло решение перевести ИТ-отдел на удаленный режим работы. Вам, как специалисту по защите информации, поручено реализовать проект по обеспечению безопасности этого процесса. Задание: Опишите методику эксперимента по проверке влияния VPN на скорость работы корпоративной CRM-системы.	1. Замерить время загрузки главной страницы без VPN (5 попыток). 2. Включить VPN и провести аналогичные замеры. 3. Вычислить среднее значение и процент задержки. 4. Оформить результат в виде краткого отчета с выводом: «Внедрение защиты замедляет работу системы на X%, что является допустимым в рамках требований бизнеса».
Кейс-задача: «Внедрение системы защиты от утечек (DLP) в юридическом департаменте». В юридическом департаменте крупной компании участились случаи случайной пересылки конфиденциальных договоров на личные адреса сотрудников. Вам поручено проработать вопрос внедрения системы контроля почтового трафика. Задание: Проведите эксперимент: проверьте, распознает ли система документ, если его заархивировать с паролем. Опишите результат в отчете.	• Ход эксперимента: Отправка тестового письма с обычным файлом (контроль) и файла в запароленном архиве .zip. • Результат для отчета: Система заблокировала обычный файл, но пропустила архив, так как не смогла его вскрыть для анализа.
«Выбор и внедрение системы обнаружения вторжений (IDS/IPS)». Вам необходимо защитить периметр сети организации от сетевых атак. Руководство предлагает выбрать один из трех вариантов реализации системы обнаружения и предотвращения вторжений (IDS/IPS). Какое решение является наиболее полным и корректным с точки зрения проектирования системы ИБ в соответствии с государственными стандартами и требованиями регуляторов? Выберите правильный ответ и объясните свой выбор. Варианты ответа: 1. Установка бесплатной Open Source IDS Snort на старый офисный компьютер без оформления документации. 2. Закупка и внедрение программно-аппаратного комплекса (ПАК) класса IPS, имеющего действующий сертификат ФСТЭК России, с последующей разработкой ТЗ, Технического проекта и Инструкции администратора. 3. Написание собственного уникального алгоритма анализа трафика на языке Python и его запуск на сервере компании для проведения научного эксперимента без интеграции в общую систему защиты.	2



1784087261

Содержание вопроса (задания)	Правильный ответ
«Внедрение системы управления доступом». В компании используется файловый сервер с общими папками, доступ к которым выдается вручную администратором. В необходимо модернизировать этот процесс, так как количество ошибок доступа (утечек) возросло. Необходимо выбрать стратегию действий. Какая последовательность действий является методологически верной для реализации полноценного цикла защиты информации? Варианты ответа: 1. Срочно запретить доступ всем сотрудникам к серверу и разрешать его только по личному звонку руководителю, не составляя никаких документов. 2. Написать научную статью о методах биометрической идентификации в будущем, не предлагая решения для текущей проблемы компании. 3. Проанализировать существующие угрозы, разработать проект ТЗ на внедрение системы централизованного управления доступом, спроектировать схему её интеграции в сеть, подготовить регламент парольной политики и провести тестирование системы на устойчивость к попыткам несанкционированного входа.	3

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. 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, 2025. — 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/2178344> (дата обращения: 07.09.2026). - Режим доступа: по подписке.

3. Прохорова, О. В. Информационная безопасность и защита информации : учебник для вузов / О.



1784087261

В. Прохорова. — 6-е изд., стер. — Санкт-Петербург : Лань, 2025. — 124 с. — ISBN 978-5-507-52899-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/462293> (дата обращения: 30.03.2026). — Режим доступа: для авториз. пользователей.

4. 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.

8.2 Дополнительная литература

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: 30.03.2026). — 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).

3. Партыка, Т. Л. Информационная безопасность : учебное пособие для студентов учреждений СПО, обучающихся по специальностям информатики и вычислительной техники / Т. Л. Партыка, И. И. Попов. — 5-е изд., перераб. и доп. — Москва : Форум, 2025. — 432 с. — (Среднее профессиональное образование). — Текст : непосредственный.

4. Баланов, А. Н. Комплексная информационная безопасность : учебное пособие для вузов / А. Н. Баланов. — 2-е изд., стер. — Санкт-Петербург : Лань, 2025. — 400 с. — ISBN 978-5-507-52839-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/460715> (дата обращения: 30.03.2026). — Режим доступа: для авториз. пользователей.

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»



1784087261

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. 7-zip
5. Microsoft Windows
6. ESET NOD32 Smart Security Business Edition
7. Kaspersky Endpoint Security
8. 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;amp;amp;amp;amp;amp;quot;Соболь-4&amp;amp;amp;amp;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;amp;amp;amp;quot;Соната-PC3&amp;amp;amp;amp;amp;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



1784087261

23.6&amp;amp;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) Соболев.

Специальное помещение для самостоятельной работы № 1211

Перечень основного оборудования:

специализированная мебель (столы и стулья);

компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду КузГТУ;

проектор, экран настенный моторизованный.

Специальное помещение для самостоятельной работы № 3210

Перечень основного оборудования:

специализированная мебель (столы и стулья);

компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду КузГТУ.

11 Иные сведения и (или) материалы

1. Образовательный процесс осуществляется с использованием как традиционных так и современных интерактивных технологий.

В рамках аудиторных занятий применяются следующие интерактивные методы:

- разбор конкретных примеров;

- мультимедийная презентация.

2. Проведение групповых и индивидуальных консультаций осуществляется в соответствии с расписанием консультаций по темам, заявленным в рабочей программе дисциплины, в период освоения дисциплины и перед промежуточной аттестацией с учетом результатов текущего контроля.



1784087261



1784087261