

10.04.01.01-2025

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

Институт информационных технологий,
машиностроения и автотранспорта
Директор

Дата: 05.05.2026 Н24:31:41

Д.М. Дубинкин

Фонд оценочных средств программы практики

Вид практики: производственная

Тип практики: проектно-технологическая практика

Способ проведения: стационарная и(или) выездная

Направление подготовки «10.04.01 Информационная безопасность»

Специализация / направленность (профиль) Организация и технология защиты информации

Присваиваемая квалификация

"Магистр"

Формы обучения

очно-заочная

7.1 Паспорт комплектка оценочных материалов

Планируемые результаты обучения по дисциплине (модулю)

Практика направлена на формирование следующих компетенций выпускника:

Форма (ы) текущего контроля	Компетенции, формируемые в результате освоения дисциплины (модуля)	Индикатор(ы) достижения компетенции	Результаты обучения по дисциплине (модулю)	Уровень
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
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 экспериментальной работы. 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:

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
«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

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.

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 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) 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

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-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 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-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
«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 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

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-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 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

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.
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;

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 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 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
«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.