Министерство науки и высшего образования Российской Федерации
федеральное государственное бюджетное образовательное учреждение
высшего образования «алтайский государственный университет»
колледж алтайского государственного университета

СОГЛАСОВАНО

Председатель ГЭК
Директор ООО «1С-ГАЛЭКС»
_____ Е.В. Акулова
«23» июня 2023 г.

УТВЕРЖДЕНО

Директор Колледжа АлтГУ
_____ Р.Ю. Ракитин
«23» июня 2023 г.

ПРОГРАММА ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ ПО СПЕЦИАЛЬНОСТИ

10.02.05. Обеспечение информационной безопасности автоматизированных систем

Барнаул 2023

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Государственная итоговая аттестация проводится с целью выявления соответствия уровня и качества подготовки выпускников требованиям федерального государственного образовательного стандарта среднего профессионального образования третьего поколения в части государственных требований к минимуму содержания по специальности 10.02.05. Обеспечение информационной безопасности автоматизированных систем.

Программа включает в себя описание вида государственной итоговой аттестации, объем времени на подготовку и проведение, сроки проведения, подготовку к защите ВКР, процедуры проведения демонстрационного экзамена и защиты дипломной работы, критерии оценки и рекомендуемую тематику дипломных работ.

К прохождению государственной итоговой аттестации (далее – ГИА) допускаются студенты, не имеющие академической задолженности и в полном объеме выполнившие учебный план или индивидуальный учебный план по программе подготовки специалистов среднего звена по специальности 10.02.05. Обеспечение информационной безопасности автоматизированных систем.

ФОРМА И ВИД ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

Формой государственной итоговой аттестации по программе подготовки специалистов среднего звена по специальности 10.02.05. Обеспечение информационной безопасности автоматизированных систем является защита выпускной квалификационной работы (ВКР).

Выпускная квалификационная работа выполняется в виде дипломной работы / проекта и демонстрационного экзамена (ДЭ).

Тематика выпускной квалификационной работы должна соответствовать содержанию одного или нескольких профессиональных модулей в соответствии с ФГОС СПО.

Демонстрационный экзамен направлен на определение уровня освоения выпускником материала, предусмотренного образовательной программой, и степени сформированности профессиональных умений и навыков путем проведения независимой экспертной оценки выполненных выпускником практических заданий в условиях реальных или смоделированных производственных процессов.

ОБЪЕМ ВРЕМЕНИ НА ПОДГОТОВКУ И ПРОВЕДЕНИЕ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

Подготовка к государственной итоговой аттестации определяется этапами выполнения форм и видов ГИА.

На подготовку к государственной итоговой аттестации отводится 4 недели:

с 18 мая по 14 июня 2026 г.

На государственную итоговую аттестацию отводится 2 недели:

с 15 по 28 июня 2026 г.

4. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ППССЗ

Выпускник должен обладать следующими общими компетенциями:

Шифр	Наименование компетенции

Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	
ОК 01	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам
ОК 02	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие
ОК 04	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами
ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке с учётом особенностей социального и культурного контекста
ОК 06	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения
ОК 07	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях
ОК 08	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности
ОК 09	Использовать информационные технологии в профессиональной деятельности
ОК 10	Пользоваться профессиональной документацией на государственном и иностранном языках
ПК 1.1.	Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.
ПК 1.2.	Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении.
ПК 1.3.	Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.
ПК 1.4.	Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.
Защита информации в автоматизированных системах программными и программно-аппаратными средствами	

ОК 01	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам
ОК 02	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие
ОК 04	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами
ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке с учётом особенностей социального и культурного контекста
ОК 06	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения
ОК 07	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях
ОК 08	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности
ОК 09	Использовать информационные технологии в профессиональной деятельности
ОК 10	Пользоваться профессиональной документацией на государственном и иностранном языках
ПК 2.1.	Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.
ПК 2.2.	Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.
ПК 2.3.	Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.
ПК 2.4.	Осуществлять обработку, хранение и передачу информации ограниченного доступа.
ПК 2.5.	Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.
ПК 2.6.	Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.
Защита информации техническими средствами	

ОК 01	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам
ОК 02	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 04	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 06	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.
ОК 07	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 08	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.
ОК 09	Использовать информационные технологии в профессиональной деятельности.
ОК 10	Пользоваться профессиональной документацией на государственном и иностранном языке.
ПК 3.1.	Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации.
ПК 3.2.	Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации.
ПК 3.3.	Осуществлять измерение параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа.
ПК 3.4.	Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.
ПК 3.5.	Организовывать отдельные работы по физической защите объектов информатизации.

5. ТРЕБОВАНИЯ К ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ

5.1. Примерная тематика выпускных квалификационных работ

1. Проект обеспечения инженерно-технической защиты объекта офиса для усиления его информационной безопасности

2. Разработка комплексной системы защиты информации объекта защиты
3. Разработка комплексной системы защиты информации (КСЗИ) предприятия.
4. Разработка основных направлений совершенствования КСЗИ предприятия.
5. Разработка сценария инженерно-технической защиты информации в кабинете/подразделении (указать название) руководителя организации
6. Совершенствование системы информационной безопасности в помещениях название организации.
7. Организация безопасности сети предприятия с использованием операционной системы Linux
8. Автоматизация обеспечения информационной безопасности группы компаний на базе ОС Unix/Linux.
9. Организация безопасного удаленного доступа к ЛВС предприятия.
10. Построение защищенной виртуальной сети на базе специализированного программного обеспечения на предприятии.
11. Автоматизация учета конфиденциальных документов на предприятии.
12. Организация процессов мониторинга конфиденциального документооборота на предприятии.
13. Автоматизация процесса проверок наличия конфиденциальных документов на предприятии.
14. Организация системы планирования и контроля функционирования КСЗИ на предприятии.
15. Организация подсистемы, обеспечивающей управление КСЗИ в условиях чрезвычайной ситуации на предприятии.
16. Разработка методологии проектирования КСЗИ.
17. Разработка моделей процессов защиты информации при проектировании КСЗИ.
18. Разработка структурно-функциональной модели управления КСЗИ предприятия.
19. Разработка проекта программно-аппаратной защиты информации предприятия.
20. Криптографические средства защиты информации на основе дискретных носителей.
21. Обоснование и разработка требований и процедур по защите информации ограниченного доступа на предприятии.
22. Разработка требований по организационной защите конфиденциальной информации, передаваемой и получаемой по сети Интернет.
23. Обоснование и разработка мер организационной защиты конфиденциальной информации при взаимодействии сотрудников предприятия со сторонними организациями.
24. Обоснование и разработка требований и процедур по защите конфиденциальной информации, обрабатываемой средствами вычислительной техники и информационными системами.
25. Организация порядка установления внутриобъектного спецрежима на объекте информатизации.
26. Организация защиты персональных данных на основе использования правовых мер.
27. Разработка комплексной системы защиты информации на предприятии, осуществляющем изготовление роботов, оснащенных программным обеспечением, представляющем коммерческую тайну.
28. Разработка и анализ эффективности внедрения мер по защите информации торговых автоматов, подключенных к глобальной сети и управляемых удаленно.
29. Разработка организационно-технических мероприятий по обеспечению безопасности функционирующей информационно-вычислительной системы при вводе в

эксплуатацию (внедрении) ее дополнительных очередей (подсистем) сторонними организациями.
30. Разработка типового проекта комплексной системы защиты информации на предприятии, осуществляющем распределенную продажу продукции с единого склада (можно взять иную сферу деятельности).
31. Разработка систем видеонаблюдения и сигнализации для обеспечения защиты информации на предприятии.
32. Организация автоматизированного пропускного режима на крупном предприятии (на примере).
33. Разработка проекта организационных мер по защите аудиоинформации в локальной сети.
34. Обоснование и разработка требований и процедур по защите информации ограниченного доступа на предприятии.
35. Разработка системы защиты информации конфиденциального характера от утечки по техническим каналам.
36. Организация системы контроля доступа и защиты информации на предприятии.
37. Защита речевой информации в каналах связи коммерческих организаций.
38. Разработка типового проекта комплексной системы защиты информации на предприятии, осуществляющем распределенную продажу продукции с единого склада.
39. Разработка мероприятий организационного характера по обеспечению комплексной защиты информации.
40. Разработка (проекта) системы видеонаблюдения и контроля доступа к объектам информатизации.

5.2. Руководство выпускной квалификационной работой

Общее руководство дипломной работой / проектом осуществляется отделением Колледжа АлтГУ.

Руководитель дипломной работы / проекта оказывает помощь студенту в разработке плана, определяет задание по этапам, осуществляет постоянный контроль за ходом выполнения исследования, проводит необходимое научное консультирование, корректирует работу студента по подбору необходимой литературы.

По завершении работы руководитель представляет письменный отзыв, в котором делаетзаключение о готовности студента к защите дипломной работы / проекта на заседании ГЭК.

.

5.3. Выполнение выпускной квалификационной работы

Основная цель дипломной работы / проекта заключается в том, что при её выполнениидолжны быть раскрыты способности выпускника применять полученные в ходе обучения теоретические и практические знания при решении конкретных задач. Практическая значимость дипломной работы определяется тем, в какой мере содержащиеся в ней предложения и рекомендации способствуют улучшению деятельности предприятия, могут быть применены и положительно оценены его руководством.

Для достижения основной цели при написании выпускной квалификационной работы должны быть конкретизированы следующие задачи:

- систематизация (закрепление и расширение полученных теоретических знаний и практических навыков);
- овладение методикой научного исследования при решении проблемных вопросов данной темы;
- самостоятельное проведение аналитических исследований на производстве;
- выявление на основе проведенного анализа имеющихся резервов, обобщение

результатов, разработка конкретных предложений и рекомендаций.

Студентам предоставляется право выбора темы выпускной квалификационной работы.

Подготовке выпускной квалификационной работы может предшествовать написание курсовой работы, разработка темы и материалы которой могут быть начальным этапом написания выпускной квалификационной работы.

В случае необходимости может проводиться предварительная защита выпускной квалификационной работы на отделении экономики и информационных технологий. На предварительной защите студент кратко представляет работу и отвечает на вопросы преподавателей отделения. Процедуру предзащиты рекомендуется проводить с заслушиванием отзыва руководителя и представлением текста выпускной квалификационной работы с использованием мультимедийной презентации.

Важным условием подготовки к защите выпускной квалификационной работы является качественная работа на всех этапах от выбора темы до защиты выполненной работы.

После проверки руководитель ставит свою подпись на титульном листе и вместе с отзывом представляет выпускную квалификационную работу заведующему отделением не позднее, чем за 14 дней до защиты в одном экземпляре в электронном виде. В отзыве руководитель указывает степень соответствия содержания работы заявленной теме, а также требованиям, предъявляемым к написанию выпускной квалификационной работы, степень выполнения задач исследования, дает характеристику самостоятельности проведенного исследования, отмечает положительные стороны и недостатки работы.

Рецензентами могут выступать специалисты из числа работников образовательных организаций, предприятий, хорошо владеющие вопросами, связанными с тематикой работы. Рецензент оценивает актуальность тематики работы, степень соответствия содержания работы теме исследования, обоснованность и доказательность выводов работы и т.п. Содержание рецензии доводится до выпускника не позднее, чем за 2 дня до защиты дипломной работы / проекта.

Защита дипломных работ / проектов проводится на открытом заседании государственной экзаменационной комиссии с участием не менее двух третей ее состава. На защиту отводится до 30 минут. Процедура защиты устанавливается председателем ГЭК по

согласованию с членами комиссии и, как правило, включает доклад студента (не более 10 минут), чтение отзыва и рецензии, вопросы членов комиссии, ответы студента. Может быть предусмотрено выступление руководителя дипломной работы / проекта, а также рецензента, если он присутствует на заседании ГЭК. В случае его отсутствия рецензия зачитывается секретарем ГЭК.

На защите могут присутствовать руководители дипломных работ / проектов, рецензенты, работодатели. Все присутствующие могут задавать вопросы по содержанию работы.

5.4. Этапы выпускной квалификационной работы

Процесс подготовки, выполнения и защиты выпускной квалификационной работы состоит из следующих этапов:

- выбор темы и согласование её с руководителем выпускной квалификационной работы;
- составление плана выпускной квалификационной работы;
- подбор нормативно-правовых документов и литературы;
- сбор и обработка фактической информации по теме выпускной квалификационной работы;
- написание работы;
- получение отзыва от руководителя на выпускную квалификационную работу;
- получение рецензии на выпускную квалификационную работу;

- подготовка доклада и презентации для защиты;
- защита работы.

Выпускная квалификационная работа должна отвечать требованиям логичного и четкого изложения материала, доказательности и достоверности фактов, отражать умение студента пользоваться рациональными приемами поиска, отбора, обработки и систематизации информации, способности работать с нормативно- правовыми актами.

Структура, содержание и оформление ВКР

ВКР должна содержать: титульный лист; содержание; введение; основную часть; заключение; список использованных источников и литературы; приложение(-я).

ВКР должна иметь логично выстроенную структуру, которая в систематизированной форме концентрированно отражает текстуально изложенное содержание проведенного исследования, его результаты и практические рекомендации.

Титульный лист разрабатывается Колледжем АлтГУ / филиалом самостоятельно и оформляется по образцу (приложение 1).

Во **введении** описываются цель, задачи, объект и предмет исследования, актуальность, практическая значимость и т.п. Цель ВКР представляет собой формулировку результата исследовательской деятельности и путей его достижения с помощью определенных средств.

Задачи исследования – это теоретические и практические результаты, которые должны быть получены в ВКР. Это обычно делается в форме перечисления (изучить…, установить…, выяснить…, вывести формулу и т.п.).

Постановку задач следует делать как можно более тщательно, т.к. их решение составляет содержание разделов ВКР.

Объект исследования – процесс или явление, порождающие проблемную ситуацию и избранные для изучения. В качестве объекта исследования могут выступать организации, оборудование, финансовые потоки, люди и их деятельность, то есть всё, что имеет материальное и процессуальное выражение.

Предмет исследования – все то, что находится в границах объекта исследования в определенном аспекте рассмотрения. Именно предмет исследования определяет тему ВКР.

Методы исследования, используемые в работе, зависят от поставленных целей и задач, а также от специфики объекта изучения. Это могут быть методы системного анализа, математические и статистические методы, сравнения, обобщения, экспертных оценок, теоретического анализа и т.д.

Содержание ВКР определяется ее темой и направлением исследования и соответствует поставленным задачам. Содержание включает введение, наименование всех глав, параграфов, разделов, подразделов, пунктов и подпунктов (если они имеют наименование), заключение, список литературы, приложения с указанием номера страниц на которых размещается начало материала главы (параграфа и т.п.). При этом знак § не ставится.

Помимо этого, во введении должна быть обоснована актуальность темы исследования, дана оценка состояния разработанности темы исследования в зарубежной и отечественной литературе, отражен вклад наиболее значимых исследователей, теоретическая и практическая значимость темы.

Основная часть включает 2 главы. Каждая глава может включать 2-3 параграфа. Все главы ВКР должны быть связаны между собой. Особое внимание следует обращать на логические переходы от одной главы к другой, от параграфа к параграфу, а внутри параграфа – от вопроса к вопросу. В каждой главе должна быть поставлена совершенно конкретная цель и сделаны выводы, т.е. изложение материала должно быть логически завершенным. Автору нужно следить за тем, чтобы изложение материала точно

соответствовало цели и названию главы.

В первой главе отражаются, как правило, теоретические вопросы по теме ВКР, изложенные с использованием научных источников. В этой главе можно рассмотреть историю вопроса, показать степень ее изученности на основе обзора отечественной и зарубежной литературы. В первой главе должна быть дана методология вопроса, описано содержание теоретических и (или) экспериментальных исследований, раскрыты понятия и сущность изучаемого вопроса, основные проблемы и возможные пути их решения.

Вторая глава ВКР является расчетно-аналитической и содержит анализ объекта. Содержание второй главы необходимо иллюстрировать таблицами, рисунками и другими материалами, которые размещают по тексту работы или в виде приложений, если они имеют значительный объем.

Третья глава является прикладной, содержит выводы и практические рекомендации и мероприятий (предложений) по решению изучаемой проблемы и обоснование их эффективности в данной сфере.

Заключение работы должно быть лаконичным и содержать основные результаты выполненной работы, краткие выводы и рекомендации по ВКР в целом.

Список использованных источников и литературы является органической частью любой учебной или научно-исследовательской работы и помещается после основного текста работы; позволяет автору документально подтвердить достоверность и точность, приводимых в тексте заимствований, таблиц, иллюстраций, формул, цитат, фактов, текстов памятников и документов; характеризует степень изученности конкретной проблемы автором; представляет самостоятельную ценность, так как может служить справочным аппаратом для других исследователей.

Выполненные выпускные квалификационные работы рецензируются специалистами из числа работников образовательных организаций, предприятий, владеющих вопросами, связанными с тематикой выпускных квалификационных работ, но не являющимися руководителями или консультантами по отдельным вопросам.

Рецензия должна включать:

– оценку качества выполнения каждого раздела выпускной квалификационной работы;

– оценку степени разработки новых вопросов, оригинальности решений (предложений), теоретической и практической значимости работы;

– оценку выпускной квалификационной работы.

Содержание рецензии доводится до сведения обучающегося не позднее, чем за 2 дня до защиты ВКР. Внесение изменений в выпускную квалификационную работу после получения рецензии не допускается.

Формат предоставления и хранения пакета документов по защите ВКР формируется исключительно в электронном формате в строгом соответствии п. 2.5 РЕГЛАМЕНТА подготовки к защите выпускной квалификационной работы и проведения процедуры защиты выпускной квалификационной работы в дистанционном формате (ПРИЛОЖЕНИЕ 2 к Распоряжению первого проректора по УР № 184 от 07.04.2022).

5.5. Подготовка доклада

Процедура защиты дипломной работы / проекта включает доклад студента по теме дипломной работы / проекта, на который отводится до 10 минут.

При разработке доклада целесообразно соблюдение структурного и методологического единства материалов доклада и иллюстраций к докладу. Тезисы доклада к защите должны содержать обязательное обращение к членам ГЭК, представление темы дипломной работы / проекта, обоснование актуальности выбранной темы, основную цель исследования и перечень необходимых для ее решения задач. В докладе должны найти обязательное отражение результаты проведенного анализа.

Текст доклада должен быть максимально приближен к тексту дипломной работы, поэтому основу выступления составляют Введение и Заключение. В докладе должны быть использованы только те графики, диаграммы и схемы, которые приведены в дипломной работе. Использование при выступлении данных, не имеющихся в дипломной работе / проекте, недопустимо. Студент должен излагать основное содержание дипломной работы / проекта свободно, отрываясь от письменного текста.

5.7. Рекомендации по составлению компьютерной презентации (КП) дипломной работы

Для презентации 10-минутного доклада разрабатывается не более 13-15 слайдов. В это число входят три обязательных текстовых слайда:

- титульный слайд с названием темы, фамилией автора и руководителя дипломной работы / проекта;
- слайд с указанием цели и задач исследования, объект и предмет исследования;
- слайд по итоговым выводам дипломной работы / проекта.

Остальные слайды должны схематично раскрывать содержание дипломной работы/проекта, включать минимальный объем поясняющего текста и в наглядной форме представлять основные положения работы. В презентации должны быть не только текстовые слайды, но и слайды, содержащие схемы, таблицы и т.п.

Состав и содержание слайдов презентации должны демонстрировать глубину проработки и понимания выбранной темы дипломной работы/проекта, а также навыки владения современными информационными технологиями.

Основными принципами при составлении подобной презентации являются лаконичность, ясность, уместность, сдержанность, наглядность.

Требования к демонстрационному экзамену

Демонстрационный экзамен проводится на площадке АлтГУ – центре проведения демонстрационного экзамена.

Оценку выполнения заданий ДЭ осуществляют эксперты.

В ходе проведения ДЭ председатель и члены ГЭК присутствуют на демонстрационномэкзамене в качестве наблюдателей.

Для проведения демонстрационного экзамена выбирается комплект оценочной документации (КОД) по специальности 10.02.05. Обеспечение информационной безопасности автоматизированных систем.

Комплект оценочной документации включает требования к оборудованию и оснащению, застройке площадки проведения демонстрационного экзамена, к составу экспертных групп, участвующих в оценке заданий демонстрационного экзамена, а также инструкцию по технике безопасности.

Обучающиеся с инвалидностью и ограниченными возможностями здоровья (далее – лица с ОВЗ и инвалиды) сдают демонстрационный экзамен в соответствии с комплектами оценочной документации с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.

5.8 Критерии оценивания выпускной квалификационной работы

Результаты защиты ВКР определяются на основе оценочных суждений, представленных в отзыве руководителя ВКР, письменных рецензиях и выступлениях рецензентов, замечаниях председателя и членов ГЭК, данных по поводу основного содержания работы, и ответов студента на вопросы, поставленные в ходе защиты. ГЭК оценивает все этапы защиты ВКР – презентацию результатов работы, понимание вопросов и ответы на них, умение вести научную дискуссию (в том числе с рецензентами), общий

уровень подготовленности студента, демонстрируемые в ходе защиты компетенции.

Основными критериями оценки ВКР являются:

1. Степень соответствия работы уровню квалификационных требований, предъявляемых к подготовке студентов, а также требованиям, предъявляемым к ВКР;
2. Соответствие темы ВКР специализации программы, актуальность, степень разработанности темы;
3. Качество и самостоятельность проведенного исследования/выполненного проекта, в том числе:

– обоснование собственного подхода к решению дискуссионных проблем теории и практики, самостоятельный выбор и обоснование методологии исследования, валидность и репрезентативность, оригинальность использованных источников, методов работы, самостоятельность анализа материала или работы с материалами проекта, разработки модели, вариантов решения, полнота и системность вносимых предложений по рассматриваемой проблеме, самостоятельная и обоснованная формулировка выводов по результатам исследования, полнота решения поставленных в работе задач;

– язык и стиль ВКР;

– соблюдение требований к оформлению ВКР.

Оценивание выпускной квалификационной работы

4-балльная шкала	**Критерии**
Отлично (повышенный уровень)	• Содержание как целой работы, так и ее частей связано с темой работы. Тема сформулирована конкретно, отражает направленность работы. • Доклад на тему представленной к защите ВКР, выполнен студентом грамотно, четко и аргументировано. • Во время защиты студент демонстрирует знание проблемы, понимание материала, дает точные определения и правильные формулировки в представленной ВКР. При этом речь студента отличается логической последовательностью, четкостью, прослеживается умение делать выводы, обобщать знания и практический опыт. • Соблюдены все правила оформления работы. • На дополнительные вопросы членов ГЭК студент дает полные и исчерпывающие ответы.
Хорошо (базовый уровень)	• Содержание как целой работы, так и ее частей связано с темой работы,имеются небольшие отклонения. • Доклад на тему представленной к защите ВКР выполнен студентом грамотно, четко и аргументировано. • Во время защиты студент не всегда обоснованно и конкретно выражает свое мнение по поводу основных аспектов содержания работы. • Есть некоторые недочеты в оформлении работы, в оформлении ссылок. • Автор достаточно уверенно владеет содержанием работы, в основном, отвечает на поставленные вопросы, но допускает незначительные неточности при ответах.

Удовлетворительно (пороговый уровень)	• Некоторые части работы не связаны с целью и задачами работы. • Доклад на тему представленной к защите ВКР, содержит неточности в формулировке понятий, терминов. Изложение материала недостаточно связано и последовательно. • Во время защиты студент показывает знание и понимание основных вопросов представленной ВКР. • На поставленные по тематике данной ВКР вопросы даны неполные, слабо аргументированные ответы. • Оформление работы не во всем соответствует предъявляемым требованиям. • Имеет удовлетворительный отзыв рецензента и руководителя ВКР.
Неудовлетворительно (уровень не сформирован)	• Содержание и тема работы плохо согласуются между собой. • Доклад на тему представленной к защите ВКР содержит ошибки вформулировке понятий, терминов. • Много нарушений правил оформления и низкая культура ссылок. • Автор совсем не ориентируется в тематике, не может назвать и краткоизложить содержание используемых книг. • Студент неуверенно излагает материал при защите, допускает ошибки при ответе или не отвечает на большинство дополнительныхвопросов, заданных членами ГЭК при защите.

Методика перевода результатов демонстрационного экзамена в оценку

Баллы за выполнение заданий демонстрационного экзамена выставляются в соответствии со схемой начисления баллов, приведенной в комплекте оценочной документации.

После проведения ДЭ баллы переводятся в оценки «отлично», «хорошо», «удовлетворительно», «неудовлетворительно» в соответствии с шкалой перевода.

5.9. Определение результатов защиты ВКР

Результаты ВКР определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно» и объявляются в день защиты после оформления в установленном порядке протоколов заседания ГЭК.

Итоговая оценка, выставляемая в ходе проведения процедуры ГИА, определяется результатами демонстрационного экзамена и защиты дипломной работы. Итоговая оценка определяется как средняя арифметическая из двух оценок. При этом ГЭК при выставлении итоговой оценки может отдать приоритет результату демонстрационного экзамена.

Решения ГЭК принимаются на закрытых заседаниях большинством голосов членов комиссии, участвующих в заседании, при обязательном присутствии председателя комиссии или его заместителя. При равном числе голосов председатель комиссии (или заменяющий его заместитель председателя комиссии) обладает правом решающего голоса.

По положительным результатам государственной итоговой аттестации ГЭК принимает решение о присвоении выпускнику квалификации по направлению подготовки и выдаче диплома о среднем профессиональном образовании государственного образца.

6. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ВЫПУСКНИКОВ ДЛЯ ПОДГОТОВКИ К ГИА

Методические рекомендации по написанию и оформлению дипломной работы /

проекта размещены в ЭБС АлтГУ, режим доступа: http://eli57brary.asu.ru/xmlui/handle/asu/69.

Методические рекомендации для подготовки и проведения демонстрационного экзамена соответствуют КОД по специальности 10.02.05. Обеспечение информационной безопасности автоматизированных систем, размещенной на официальном сайте Оператора демонстрационного экзамена.

ПРИЛОЖЕНИЕ 1

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшегообразования
«Алтайский государственный университет»Колледж АлтГУ

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

(дипломная работа / дипломный проект)

Тема: _____

Выпускную квалификационную работу выполнил(а) студент(ка) курса, группыФИО

_____
(подпись)

Научный руководитель:ФИО

_____
(подпись)

Выпускная квалификационная работа защищена:
«_ _»_____202_г. Оценка _____

_____

Председатель ГЭК:ФИО

_____
(подпись)

_____202_ г.

Министерство науки и высшего образования Российской Федерации
федеральное государственное бюджетное образовательное учреждение
высшего образования «Алтайский государственный университет»
Колледж Алтайского государственного университета
Отделение Экономики и информационных технологий

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

для государственной итоговой аттестации
программы подготовки специалистов среднего звена

10.02.05 Обеспечение информационной безопасности автоматизированных систем

Разработчик(и):
Кочкин А.С.
преподаватель, высшая к.к

_____
(подпись)

Одобрено на заседании отделения
Экономики и информационных технологий

Протокол № 6 от «21» февраля 2023 г.

Согласовано:
Председатель организации-работодателя
Акулова Е.В.,
директор ООО «1С-Галэкс»

_____

Барнаул 2023

Визирование ФОС для исполнения в очередном учебном году

Фонд оценочных средств пересмотрен, обсужден и одобрен для исполнения в _____-_____ учебном году на заседании отделения _____

Внесены следующие изменения и дополнения:

1. Переработаны задания (оценочные средства) по учебной и производственной практикам
2. Обновлен список используемых источников литературы

Протокол от_____ №_____
Зав. отделением
_____
(фамилия, инициалы)

_____
(подпись)

Визирование ФОС для исполнения в очередном учебном году

Фонд оценочных средств пересмотрен, обсужден и одобрен для исполнения в _____-_____ учебном году на заседании отделения _____

Внесены следующие изменения и дополнения:

Протокол от_____ №_____
Зав. отделением
_____
(фамилия, инициалы)

_____
(подпись)

Визирование ФОС для исполнения в очередном учебном году

Фонд оценочных средств пересмотрен, обсужден и одобрен для исполнения в _____-_____ учебном году на заседании отделения _____

Внесены следующие изменения и дополнения:

Протокол от_____ №_____
Зав. отделением
_____
(фамилия, инициалы)

_____
(подпись)

Перечень компетенций, которыми должны овладеть обучающиеся в результате освоения образовательной программы

Результаты освоения образовательной программы согласно ФГОС СПО по специальности **10.02.05. Обеспечение информационной безопасности автоматизированных систем.**

Ком**петенции**	Форма проверки освоения компетенций
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам. ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности. ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами. ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста. ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей. ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях. ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности. ОК 09. Использовать информационные технологии в профессиональной деятельности. ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языке	дипломная работа и демонстрационный экзамен
ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	
ПК 1.1. Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.	дипломная работа и демонстрационный экзамен
ПК 1.2. Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении.	дипломная работа и демонстрационный экзамен
ПК 1.3. Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями	дипломная работа и демонстрационный экзамен

эксплуатационной документации.	
ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.	дипломная работа и демонстрационный экзамен
ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами	
ПК 2.1 Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.	дипломная работа и демонстрационный экзамен
ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами	дипломная работа и демонстрационный экзамен
ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.	дипломная работа и демонстрационный экзамен
ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.	дипломная работа и демонстрационный экзамен
ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.	дипломная работа и демонстрационный экзамен
ПК 2.6. Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.	дипломная работа и демонстрационный экзамен
ПМ. 03 Защита информации техническими средствами	
ПК 3.1 Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации.	дипломная работа и демонстрационный экзамен
ПК 3.2 Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации.	дипломная работа и демонстрационный экзамен
ПК 3.3 Осуществлять измерение параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа.	дипломная работа и демонстрационный экзамен
ПК 3.4 Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.	дипломная работа и демонстрационный экзамен
ПК 3.5 Организовывать отдельные работы по физической защите объектов информатизации.	дипломная работа и демонстрационный экзамен

Заключительный этап формирования компетенций, направлен на закрепление ряда полученных в процессе обучения знаний, умений, навыков и (или) опыта деятельности. ГИА проводится в целях определения соответствия результатов освоения обучающимися основных образовательных программ соответствующим требованиям ФГОС СПО.

Компетенции	Показатели
ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	
ПК 1.1 Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.	**Знать:** состав и принципы работы автоматизированных систем, операционных систем и сред; принципы разработки алгоритмов программ, основных приемов программирования; модели баз данных; принципы построения, физические основы работы периферийных устройств; **Уметь:** осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении и компонент систем защиты информации автоматизированных систем; **Иметь практический опыт:** установка и настройка компонентов систем защиты информации автоматизированных (информационных) систем
ПК 1.2 Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении	**Знать**: теоретические основы компьютерных сетей и их аппаратных компонент, сетевых моделей, протоколов и принципов адресации **Уметь:** организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней; осуществлять конфигурирование, настройку компонент систем защиты информации автоматизированных систем; производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы **Иметь практический опыт:** администрирование автоматизированных систем в защищенном исполнении
ПК 1.3 Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации	**Знать:** порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях **Уметь:** настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам **Иметь практический опыт:** эксплуатация компонентов систем защиты информации автоматизированных систем
ПК 1.4 Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в	**Знать:** принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации **Уметь:** обеспечивать работоспособность, обнаруживать и устранять неисправности **Иметь практический опыт:** диагностика компонентов систем защиты информации автоматизированных систем, устранение отказов и

защищенном исполнении	восстановление работоспособности автоматизированных (информационных) систем в защищенном исполнении
ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами	
ПК 2.1 Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.	Знать: особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных Уметь: устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; Иметь практический опыт: установка, настройка программных средств защиты информации в автоматизированной системе
ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами	Знать: особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных Уметь: устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями; устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; Иметь практический опыт: обеспечение защиты автономных автоматизированных систем программными и программно-аппаратными средствами; использование программных и программно-аппаратных средств для защиты информации в сети
ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.	Знания: методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации Умения: диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации; Практический опыт: тестирование функций, диагностика, устранение отказов и восстановление работоспособности программных и программно-аппаратных средств защиты информации
ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.	Знания: особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных; типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации; основные понятия криптографии и типовых криптографических методов и средств защиты информации Умения: применять программные и программно-аппаратные средства для защиты информации в базах

	данных; проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации; применять математический аппарат для выполнения криптографических преобразований; использовать типовые программные криптографические средства, в том числе электронную подпись Практический опыт: решение задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации; применение электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных
ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.	Знания: особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации Умения: применять средства гарантированного уничтожения информации Практический опыт: учёт, обработка, хранение и передача информации, для которой установлен режим конфиденциальности
ПК 2.6. Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.	Знания: типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа Умения: устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак Практический опыт: работа с подсистемами регистрации событий; выявление событий и инцидентов безопасности в автоматизированной системе
ПМ. 03 Защита информации техническими средствами	
ПК 3.1 Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации.	**Знать:** порядок технического обслуживания технических средств защиты информации; номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам; **Уметь:** применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных; **Иметь практический опыт:** установка, монтаж и настройка технических средств защиты информации; техническое обслуживание технических средств защиты информации; применение основных типов

	технических средств защиты информации
ПК 3.2 Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации.	Знать: физические основы, структуру и условия формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации; порядок устранения неисправностей технических средств защиты информации и организации ремонта технических средств защиты информации; методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации; номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам Уметь: применять технические средства для криптографической защиты информации конфиденциального характера; применять технические средства для уничтожения информации и носителей информации; применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами Иметь практический опыт: применение основных типов технических средств защиты информации; выявление технических каналов утечки информации; участие в мониторинге эффективности технических средств защиты информации; диагностика, устранение отказов и неисправностей, восстановление работоспособности технических средств защиты информации
ПК 3.3 Осуществлять измерение параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа.	Знать: номенклатуру и характеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации; структуру и условия формирования технических каналов утечки информации; Уметь: применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных Иметь практический опыт: проведение измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов информатизации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации
ПК 3.4 Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими	Знать: номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам Уметь: применять технические средства для защиты

средствами защиты информации.	информации в условиях применения мобильных устройств обработки и передачи данных Иметь практический опыт: проведение измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации; выявление технических каналов утечки информации
ПК 3.5 Организовывать отдельные работы по физической защите объектов информатизации.	Знать: основные принципы действия и характеристики технических средств физической защиты; основные способы физической защиты объектов информатизации; номенклатуру применяемых средств физической защиты объектов информатизации Уметь: применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом; применять инженерно-технические средства физической защиты объектов информатизации Иметь практический опыт: установка, монтаж и настройка, техническое обслуживание, диагностика, устранение отказов и неисправностей, восстановление работоспособности инженерно-технических средств физической защиты

Требования к содержанию демонстрационного экзамена по специальности 10.02.05. Обеспечение информационной безопасности автоматизированных систем в соответствии с ФГОС СПО

№ п/п	**Модуль задания** (вид деятельности, вид профессиональной деятельности)	**Перечень оцениваемых ПК (ОК)**	**Перечень оцениваемых умений и навыков / практического опыта**
1	2	3	4
1	Эксплуатация автоматизированных (информационных) систем в автоматизированных защищенном исполнении	ПК Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении. ПК Администрировать программные и программно-аппаратные	**Знать:** состав и принципы работы автоматизированных систем, операционных систем и сред; принципы разработки алгоритмов программ, основных приемов программирования; модели баз данных; принципы построения, физические основы работы периферийных устройств. **Уметь:** осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении и компонент систем защиты информации автоматизированных систем. **Иметь практический опыт:** установка и настройка компонентов систем защиты информации автоматизированных (информационных) систем

		компоненты автоматизированной (информационной) системы в защищенном исполнении. ПК Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.	
2	Защита информации в Автоматизированных системах. программными и программно-Аппаратным и средствами	ПК Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации ПК Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами ПК Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств. ПК Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.	**Знать:** особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных **Уметь:** устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями; устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации. **Иметь практический опыт:** обеспечение защиты автономных автоматизированных систем программными и программно-аппаратными средствами; использование программных и программно-аппаратных средств для защиты информации в сети.

Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Примерные требования к оцениванию

	Максимально возможное количество баллов		100
№ п/п	**Модуль задания** (вид деятельности, вид профессиональной деятельности)	**Критерий оценивания**	**Баллы**
1	2	3	4
1	Эксплуатация автоматизированных (информационных) систем в автоматизированных защищенном исполнении	Установка и настройка компонентов автоматизированных (информационных) систем в Защищенном исполнении в Соответствии с требованиями Эксплуатационной документации. Администрирование программных и программно-аппаратных компонентов автоматизированной (информационной) системы в защищённом исполнении	50
2	Защита информации в Автоматизированных системах. программными и программно-Аппаратными средствами	Установка и настройка отдельных программных, программно-аппаратных средств защиты информации. Обеспечение защиты информации в автоматизированных системах отдельными программными, программно-аппаратными средствами. Тестирование функций отдельных программных и программно-аппаратных средств защиты информации.	50
		итого	100

Образец задания базового уровня

В компании «SoC» возникла необходимость внедрения DLP системы для лучшей защиты корпоративной информации и предотвращения утечек данных. Вам необходимо установить и настроить компоненты системы в соответствии с выданным заданием. Серверные компоненты установлены, сетевые интерфейсы настроены.

Подготовлены следующие виртуальные машины для дальнейшей работы:

• Контроллер домена;

• DLP сервер установлен, активирована лицензия, есть LDAP синхронизация;

• Виртуальная машина с установленным сервером агентского мониторинга;

• Виртуальная машина «нарушителя» в домене (1 шт).

В компании развернут домен со всеми сотрудниками с указанием ФИО, должности и контактов.

При выполнении заданий можно пользоваться разрешенными справочными ресурсами в сети Интернет и/или документацией на компьютерах и/или в общем сетевом каталоге.

Все логины, пароли, сетевые настройки и прочее указаны в дополнительной карточке задания.

Модуль 1: Эксплуатация автоматизированных (информационных) систем в защищенном исполнении

При выполнении задания модуля необходимо достичь следующих целей:

1. Настроенный контроллер домена.
2. Работоспособный сервер мониторинга сетевого трафика.
3. Установленный и работоспособный сервер агентского мониторинга.
4. Установленные и работоспособные агент мониторинга на клиентском устройстве.

Если в задании указано сделать скриншот, необходимо называть его по номеру задания, например, «Задание_5_копирование.jpg». Все скриншоты и отчеты сохраняются на рабочий стол физического компьютера в один каталог или документ (важно соблюдать последовательность заданий). При создании снимков экрана необходимо делать либо полный снимок экрана, либо целого окна. Не стоит вырезать только маленький кусочек (например, сообщение о событии), т. к. это не будет являться явным подтверждением работы.

Допускается последующее выделение рамкой, стрелкой или иным способом результата работы.

Задание модуля 1:

Задача 1: Настройка контроллера домена

Создать подразделение “DemoExam” в контроллере домена.

Внутри созданного подразделения “DemoExam” необходимо создать и настроить следующих доменных пользователей с соответствующими правами:

– Логин: web-officer, пароль: xxXX3344, права пользователя домена;

– Логин: ldap-sync, пароль: xxXX3344, права пользователя домена;

– Логин: device-officer, пароль: xxXX3344, права администратора домена и локального администратора;

– Логин: violator, пароль xxXX3344, права пользователя домена.

Задача 2: Настройка DLP сервера

DLP-сервер контроля сетевого трафика уже предустановлен, но не настроен:

– необходимо узнать IP-адрес сервера через локальную консоль виртуальной машины и проверить настройки DNS на сервере для корректной работы, в случае несовпадений настроить DNS правильно;

– синхронизировать каталог пользователей и компьютеров LDAP с домена с помощью ранее созданного пользователя ldap-sync;

– для входа в веб-консоль необходимо настроить использование ранее созданного пользователя домена web-officer с полными правами системы.

Запишите IP-адреса, токен, логины и пароли от учетных записей, а также все прочие нестандартные данные (измененные вами) вашей системы в текстовом файле «отчет.txt» на рабочем столе компьютера.

Задача 3: Установка и настройка сервера агентского мониторинга

Используя виртуальную машину агентского мониторинга:

– необходимо ввести сервер в домен, после перезагрузки войти в систему от ранее созданного пользователя device-officer (важно);

– после входа в систему необходимо переместить введенный в домен компьютер в ранее созданное подразделение “DemoExam” на домене;

– установить базу данных PostgreSQL или функциональный аналог с паролем суперпользователя QWEasd123;

– установить сервер агентского мониторинга с параметрами по умолчанию, подключившись к ранее созданной БД;

– при установке сервера агентского мониторинга необходимо установить соединение с DLP-сервером по IP-адресу и токену, но можно сделать это и после установки. При установке настроить локального пользователя консоли управления: web-officer с паролем QWEasd123;

– синхронизировать каталог пользователей и компьютеров с контроллером домена.

Запишите IP-адреса, логины и пароли от учетных записей, а также все прочие данные, измененные вами, в текстовом файле «отчет.txt» с на рабочем столе компьютера.

Задача 4: Установка агента мониторинга на машине нарушителя

Используя виртуальную машину нарушителя:

– необходимо ввести клиентскую машину в домен, после перезагрузки войти в систему от ранее созданного пользователя violator;

– после входа в систему необходимо переместить введённый в домен компьютер в ранее созданное подразделение “DemoExam” на домене.

На машину нарушителя (violator) средствами групповых политик или сервера мониторинга установить агент мониторинга. Необходимо учесть, что установка осуществляется только с правами администратора (доменного или локального).

Ручная установка с помощью создания и переноса любым способом пакета установки является некорректным выполнением задания.

В случае проблем при установке компонентов стоит проверить настройки брандмауэра и DNS.

Задача 5: Защита системы с помощью сертификатов

Создайте дерево сертификатов формата PKCS для защиты веб-соединения с

DLPсервером по протоколу HTTPS. Сертификат и используемый ключ должен удовлетворять общепринятым на сегодня стандартам и требованиям (по длительности не более 1 года, длине ключа не менее 2048 бит и т. п.), параметры сертификата должны соответствовать атрибутам компании. Утилита для создания сертификата — на выбор участника из доступных в операционных системах и дистрибутивах (openssl или аналоги).

Дерево сертификатов должно включать:

корневой root-сертификат (ca);

серверный (server) сертификат;

по желанию допускается использование пользовательского и промежуточного сертификата.

Дополнительная информация сертификатов должна включать в себя:

Страна: RU.

Город: Moscow.

Компания (и иные дополнительные поля): DemoExam.

Отдел: SoC.

Пароли ключей (если применимо): QWEasd123.

Остальные поля заполняются самостоятельно.

После генерации сертификатов необходимо установить серверный сертификат на вебсервер DLP-системы, а также установить корневой сертификат как доверенный в контроллер домена для использования на всех компьютерах в сети.

В случае невозможности — это сделать, установить сертификат на машину домена и отобразить это в отчете.

Итоговый результат должен включать:

– Дерево из сертификатов, упакованных в пакет PKCS (.p12), а также представленные в виде отдельных файлов ключей и сертификатов, расположенных на рабочем столе в каталоге «Сертификаты».

– Содержимое команд по генерации ключей и сертификатов в текстовом файле «сертификаты.txt» на рабочем столе с комментариями.

– Скриншоты успешного подключения к консоли сервера DLP без ошибок сертификата, скриншоты окон просмотра сертификата в системе с помощью оснастки «Сертификаты» операционной системы (вкладки «Общие», «Путь сертификации»).

– Сертификаты не должны содержать ошибок, предупреждений (warnings), неверной информации и т. п.

Модуль 2: Защита информации в автоматизированных системах программными и программно-аппаратными средствами

При выполнении задания модуля необходимо достичь следующих целей:

1.Настройка сервера агентского мониторинга для правильной работы системы.

2. Разработка политик и правил безопасности, предотвращающих утечки или попытку использования устройств и сервисов пользователями.

3. Разработка групповых политик домена для ограничения пользовательских действий.

4. Проверка работоспособности политик и правил безопасности

Задания выполняются только с помощью компонентов DLP системы или групповых политик (указано в задании).

Все сценарии заданий (где применимо) необходимо воспроизвести и зафиксировать результат. Называйте созданные вами разделы/политики/группы и т. п. в соответствии с заданием, например, «Политика 1» или «Правило 1.2» и т. д., иначе проверка заданий может быть невозможна.

Выполнение отдельных заданий необходимо подтвердить скриншотом. В этом случае необходимо протоколировать свои результаты с помощью двух и более скриншотов для каждого задания (скриншот заданной политики и скриншот ее работы). Для некоторых заданий необходимо после фиксации результатов в виде скриншотов удалить заданную политику, что будет оговорено отдельно в тексте задания. Все скриншоты необходимо сохранить в папке «Модуль 2».

Формат названия скриншотов политик:

Пример 1 для сохранения скриншота созданной политики: CR-1.jpg где CR – сокращение от англ. creating a rule, 1 – номер задания

Пример 2 для сохранения скриншота работающей политики: RW-1.jpg где RW – сокращение от англ. rule work, 1 – номер задания.

Пример 3 для сохранения нескольких скриншотов одной работающей политики: RW-1-2.jpg где RW – сокращение от англ. rule1 work, 1 – номер задания; 2 – номер скриншота для задания 1.

Задание модуля 2:

Задача 1: Проверка работоспособности системы

Необходимо создать проверочную политику на правило передачи, копирования, хранения и буфера обмена (или работы в приложениях), все 4 варианта срабатывания событий для данных, содержащих термин «Проверка системы» (в любом регистре), установить низкий уровень угрозы для всех событий, добавить тег «Проверка». Для отработки правил через сервер агентского мониторинга необходимо создавать правила в отдельной политике «Модуль 2». После отработки политик необходимо оставить политику и открепить ее от групп компьютеров или выключить правила, но не удалять.

Проверить срабатывание всеми четырьмя возможными способами (передачи, копирования, хранения и буфера обмена, хотя бы 1 событие на каждый тип) с помощью виртуальной машины нарушителя с установленным агентом. Сделать одну выборку, в которой будет отображено только по одному событию каждого типа (суммарно 4 события: передачи, копирования, хранения и буфера обмена), настроив конструктор выборки

вручную.

Задача 2: подготовка сервера агентского мониторинга

Необходимо создать новую группу компьютеров: «DemoGroup», а также создать новую политику: «DemoPolicy». Политика должна применяться на ранее созданную группу компьютеров. Компьютер нарушителя необходимо переместить в группу «DemoGroup»

Зафиксировать выполнение скриншотом.

Задача 3: смена пароля удаления агента

Необходимо установить (сменить) пароль для удаления агента мониторинга на всех машинах нарушителей с помощью средств сервера агентского мониторинга (удаленно).

Пароль: QWEasd123

Зафиксировать выполнение скриншотом.

Следующие правила создаются в политике «DemoPolicy».

Правило 1

Запретить печать документов на сетевых принтерах. Также необходимо отдельным правилом разрешить печать на локальных принтерах.

Зафиксировать факт настройки правил (политик) скриншотами.

Правило 2

Необходимо полностью запретить использование облачного сервиса GoogleDrive, разрешить полное использование сервиса YandexDisk, остальные сервисы настроить только в режиме чтения (разрешить скачивание).

Зафиксировать факт настройки правил (политик) скриншотами.

Правило 3

Запретить запуск приложения wordpad или Libre/Open office Writer.

Проверить работоспособность, зафиксировать факт настройки правил (политик) и их работоспособность скриншотами.

Правило 4

Необходимо запретить создание снимков экрана в текстовых редакторах для предотвращения утечки.

Проверить работоспособность, зафиксировать факт настройки правил (политик) и их работоспособность скриншотами.

Правило 5

Необходимо запретить запись файлов на все съемные носители информации (флешки), оставив возможность чтения и копирования с них. В случае отсутствия USB-накопителей создать правило на сетевые расположения.

Проверить работоспособность, зафиксировать факт настройки правил (политик) и их работоспособность скриншотами.

Правило 6

С учетом ранее созданной блокировки необходимо разрешить копирование только на

один доверенный USB-накопитель.

Проверить работоспособность, зафиксировать факт настройки правил (политик) и их работоспособность скриншотами.

Правило 7

Полностью заблокируйте доступ к CD/DVD на клиентском компьютере (виртуальной машине). В случае отсутствия CD/DVD привода его необходимо создать.

Проверить работоспособность, зафиксировать факт настройки правил (политик) и их работоспособность скриншотами.

Правило 8

Осуществить выдачу временного доступа (30 минут) клиенту до заблокированного CD/DVD привода.

Проверить работоспособность, зафиксировать факт настройки правил (политик) и их работоспособность скриншотами. Необходимо зафиксировать основные шаги выдачи доступа (например, ввод кода).

Правило 9

Необходимо установить контроль за компьютером потенциального нарушителя в случае использования браузера путем создания снимков экрана каждые 30 секунд или при переходе в другое окно.

Проверить работоспособность, зафиксировать факт настройки правил (политик) и их работоспособность скриншотами. Также необходим скриншот сохраненных снимков экрана в системе.

Правило 10

Запретить передачу файлов документов типа PDF на съемные носители информации и в сетевые каталоги.

Проверить работоспособность любым из правил, зафиксировать факт настройки правил (политик) и их работоспособность скриншотами.

Групповые политики домена

Групповые применяются только на компьютер нарушителя (violator), должны быть созданы в домене, необходимо создать или 1 общий объект для всех политик и применить его к группе компьютеров/пользователей (или к конкретному компьютеру/пользователю), или по 1 объекту на каждую политику и применить их к группе компьютеров/пользователей (или к конкретному компьютеру/пользователю).

Зафиксировать настройку политик скриншотами, при возможности проверки зафиксировать скриншотами проверку политик (например, запрет запуска).

Использование компонентов DLP будет считаться некорректным выполнением задания.

Групповая политика 1

1. Настроить политику паролей и блокировки:
2. Максимальный срок действия пароля: 47 дней
3. Минимальная длина пароля: 8 символов
4. Блокировка пользователя при неправильном вводе пароля: 5

5. Блокировка учетной записи при вводе пароля: 20 минут

Зафиксировать настройки политики скриншотами.

Групповая политика 2

Отключить анимацию первого входа в систему

Зафиксировать настройки политики скриншотами

Групповая политика 3

Запретить использование командной строки (терминала) пользователем стандартной политикой запрета (не с помощью списка, при наличии).

Зафиксировать настройки политики и выполнение скриншотами.

Групповая политика 4

Запретить пользователю самостоятельный запуск панели управления.

Зафиксировать настройки политики и выполнение скриншотами.

Групповая политика 5

Изменить изображение рабочего стола пользователя групповыми политиками. Изображение необходимо создать самостоятельно, должно содержать в себе название компании («DemoExam») текстом в картинке.

Изменение изображения вручную не будет считаться корректным выполнением задания.

Пример задания демонстрационного экзамена профильного уровня

Описание модуля А: «Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз» Задание выполняется на подготовленных виртуальных машинах:

контроллер домена с поднятым DNS и AD, чистая серверная система, чистая клиентская система (2 шт), предустановленный, но не настроенный DLP-сервер (с установленной лицензией).

В компании «Демо Лаб» возникла необходимость внедрения DLP системы для лучшей защиты разработок и предотвращения утечек прочей информации. Вам необходимо установить и настроить компоненты системы в соответствии с выданным заданием.

Основными каналами потенциальной утечки данных являются электронная почта и различные интернет-ресурсы, если не указано иное.

Серверные компоненты устанавливаются в виртуальной среде, сетевые интерфейсы настроены, но IP адреса (и/или DNS сервер) нужно назначить согласно прилагаемой карточке.

Подготовлены следующие виртуальные машины для дальнейшей работы:

• AD и DNS сервер (контроллер домена)

• DLP сервер установлен (но не настроен), активирована лицензия

• Виртуальная машина для установки сервера агентского мониторинга •

Виртуальные машины «нарушителей» (2 шт)

В компании развернут домен со всеми сотрудниками с указанием ФИО, должности и контактов.

Стоит отметить, что имена всех компьютеров (hostname) должны быть уникальными

(проверить и исправить самостоятельно).

При выполнении заданий можно пользоваться разрешенными справочными ресурсами в сети Интернет и документацией на компьютерах и/или в общем сетевом каталоге.

Все дистрибутивы находятся в каталоге, указанном в дополнительной карточке задания. Все логины, пароли, сетевые настройки и прочее указаны в дополнительной карточке задания.

В случае отсутствия необходимых для выполнения задания данных, обратитесь к экспертам.

Если в задании указано сделать скриншот, необходимо называть его по номеру задания, например: Задание_5_копирование.jpg, все скриншоты и отчеты сохраняются на рабочий стол физического компьютера в один каталог или документ (важно соблюдать последовательность заданий) или передаются экспертам иным способом по запросу.

При создании снимков экрана необходимо делать либо полный снимок экрана, либо целого окна. Не стоит вырезать только маленький кусочек (например, сообщение о событии), т. к. это не будет являться явным подтверждением работы. Допускается последующее выделение рамкой, стрелкой или иным способом результата работы.

При выполнении модуля А ставятся следующие цели:

1. Настроенный контроллер домена.
2. Работоспособный сервер мониторинга сетевого трафика.
3. Установленный и работоспособный сервер агентского мониторинга.
4. Установленные и работоспособные агенты мониторинга на клиентских устройствах
5. Настроенный компонент контроля сетевых хранилищ.
6. Сгенерированные сертификаты безопасности. Установленные на сервер мониторинга сетевого трафика.

При выполнении данного модуля А ставятся следующие задачи:

Задача 1: Настройка контроллера домена

Для удобства работы рекомендуется создать подразделение “Test” в корневом каталоге оснастки “Пользователи и компьютеры” AD сервера.

Внутри созданного подразделения “Test” необходимо создать и настроить следующих доменных пользователей с соответствующими правами:

Логин: user1, пароль: xxXX1234, права пользователя домена Логин: user2, пароль: xxXX1234, права пользователя домена Логин: admin1, пароль: xxXX1234, права администратора домена Логин: user3, пароль: xxXX1234, права пользователя домена Логин: user4, пароль: xxXX1234, права пользователя домена

Задача 2: Настройка DLP сервера DLP-сервер контроля сетевого трафика уже предустановлен, но не настроен.

Необходимо синхронизировать каталог пользователей и компьютеров LDAP с домена с помощью ранее созданного пользователя user4.

Для входа в веб-консоль необходимо настроить использование ранее созданного пользователя домена user3 с полными правами офицера безопасности и на администрирование системы, полный доступ на все области видимости.

Запишите IP-адреса, токен, логины и пароли от учетных записей, а также все прочие нестандартные данные (измененные вами) вашей системы в текстовом файле «отчет.txt» на

рабочем столе компьютера.

Задача 3: Установка и настройка сервера агентского мониторинга

Необходимо ввести сервер в домен, после перезагрузки войти в систему от ранее созданного пользователя admin1 (важно). После входа в систему необходимо переместить введенный в домен компьютер в ранее созданное подразделение “Test” на домене.

Установить базуданных PostgreSQLили функциональный аналог с паролем суперпользователя xxXX1234.

Установить сервер агентского мониторинга с параметрами по умолчанию, подключившись к ранее созданной БД.

При установке сервера агентского мониторинга необходимо установить соединение с DLP-сервером по IP-адресу и токену, но можно сделать это и после установки. При установке настроить локального пользователя консоли управления: officer с паролем xxXX1234

Синхронизировать каталог пользователей и компьютеров с Active Directory или функциональным аналогом.

После синхронизации настроить беспарольный вход в консоль управления от ранее созданного доменного пользователя admin1, установить полный доступ к системе, установить все области видимости.

Проверить работоспособность входа в консоль управления без ввода пароля. Если сервер не введен в домен или работает от другого пользователя, данная опция работать не будет.

Задача 4: Установка агента мониторинга на машине нарушителя

Необходимо ввести клиентскую машину 1 в домен, после перезагрузки войти в систему от ранее созданного пользователя user1.

Необходимо ввести клиентскую машину 2 в домен, после перезагрузки войти в систему от ранее созданного пользователя user2.

После входа в систему необходимо переместить веденные в домен компьютеры в ранее созданное подразделение “Test” на домене.

Установить агент мониторинга:

На машину 1 с помощью задачи первичного распространения с сервера агентского мониторинга.

На машину 2 с помощью групповых политик домена.

Необходимо создавать отдельные объекты групповых политик на каждое Задача и делать снимки экрана для подтверждения создания и выполнения политик.

Ручная установка с помощью переноса на машину нарушителя пакета установки является некорректным выполнением задания

Задача 5: Установка и настройка подсистемы сканирования сетевых ресурсов.

Необходимо установить и настроить подсистему сканирования сетевых ресурсов на сервер с установленным сервером агентского мониторинга с настройками по умолчанию.

Необходимо создать общий каталог Test в корне диска сервера и установить права доступа на запись и чтение для всех пользователей домена.

Необходимо настроить подсистему сканирования сетевых ресурсов на автоматическое ежедневное сканирование только ранее созданного каталога. Для работы подсистемы может потребоваться редактирования конфигурационных файлов (для устранения

предупреждения).

Задача 6: Проверка работоспособности системы

Необходимо создать проверочную политику на правило передачи, копирования, хранения и буфера обмена (или работы в приложениях), все 4 варианта срабатывания событий для данных, содержащих некий термин, установить уровень угрозы для всех событий, добавить тег.

Проверить срабатывание всеми четырьмя возможными способами (передачи, копирования, хранения и буфера обмена, хотя бы 1 событие на каждый тип) с помощью виртуальной машины нарушителя 1 с установленным агентом.

Сделать одну выборку, в которой будет отображено только по одному событию каждого типа, настроив конструктор выборки вручную.

Зафиксировать выполнение скриншотом выполненной выборки или конструктора выборки.

Задача 7: Защита системы с помощью сертификатов

Создайте дерево сертификатов формата PKCS для защиты веб-соединения с DLPсервером по протоколу HTTPS. Сертификат и используемый ключ должен удовлетворять общепринятым на сегодня стандартам и требованиям, параметры сертификата должны соответствовать атрибутам компании. Утилита для создания сертификата — на выбор участника из доступных в операционных системах и дистрибутивах (openssl или аналоги).

Дерево сертификатов должно включать: 1. корневой root-сертификат (ca)

2. серверный (server) сертификат

3. по желанию допускается использование пользовательского и промежуточного сертификата

Поля сертификата заполняются по вариантам заданий.

После генерации сертификатов необходимо установить серверный сертификат на веб-сервер DLP-системы, а также установить корневой сертификат как доверенный в контроллер домена для использования на всех компьютерах в сети для доверенного подключения к веб-консоли DLP-системы уровня сети.

Итоговый результат должен включать:

Дерево из 2-3 сертификатов, упакованных в пакет PKCS (.p12), а также представленные в виде отдельных файлов ключей сертификатов, расположенных на рабочем столе. Содержимое команд по генерации ключей и сертификатов в текстовом файле на рабочем столе с комментариями.

Скриншоты успешного подключения к консоли сервера DLP без ошибок сертификата, скриншоты окон просмотра сертификата в системе с помощью оснастки «Сертификаты» операционной системы (вкладки «Общие», «Путь сертификации»).

Описание модуля E: «Технологии защиты узла и агентского мониторинга» Задания выполняются только с помощью компонентов DLP системы или групповых политик (указано в задании). Все сценарии заданий (где применимо) необходимо воспроизвести и зафиксировать результат.

Называйте созданные вами разделы/политики/группы и т. п. в соответствии с заданием, например, «Политика 1» или «Правило 1.2» и т. д., иначе проверка заданий может быть

невозможна. Выполнение отдельных заданий необходимо подтвердить скриншотом (это всегда указывается отдельно).

При выполнении модуля Е ставятся следующие цели:

1. Настройка сервера агентского мониторинга для правильной работы системы.
2. Разработка политик и правил безопасности, предотвращающих утечки или попытку использования устройств и сервисов пользователями.
3. Разработка групповых политик домена для ограничения пользовательских действий.
4. Проверка работоспособности политик и правил безопасности.

При выполнении модуля Е ставятся следующие задачи:

Задача 1

Необходимо создать 2 новых группы компьютеров: «Test1» и «Test2», а также создать 2 новых политики: «Test1» и «Test2». Каждая из политик должна применяться только на соответствующие группы. Компьютер 1 необходимо перенести в Test1, а компьютер 2 — в Test2.

Зафиксировать выполнение скриншотом.

Задача 2

Для удобства работы офицера безопасности необходимо установить дополнительную консоль управления сервером агентского мониторинга на другую машину для удаленного доступа к серверу агентского мониторинга.

Задача 3: разработать правила агентского мониторинга. Следующие правила создаются в политике «Test1».

Правило 1

Необходимо запретить пользоваться Microsoft Paint, так как участились случаи подделки печатей компании.

Проверить работоспособность и зафиксировать выполнение скриншотом.

Правило 2

Необходимо запретить создание снимков экрана в табличных процессорах для предотвращения утечки секретных расчетов и баз данных.

Проверить работоспособность и зафиксировать выполнение скриншотом.

Правило 3

Ограничить доступ к определенным облачным хранилищам (по вариантам). Проверить работоспособность и зафиксировать выполнение

Правило 4

Необходимо запретить печать на сетевых принтерах.

Зафиксировать создание политики скриншотом.

Правило 5

Необходимо запретить запись файлов на определенные носители информации, при этом оставить возможность считывания информации.

Проверить работоспособность и зафиксировать выполнение

Правило 6

С учетом ранее созданной блокировки необходимо разрешить использование доверенного носителя информации.

Проверить работоспособность и зафиксировать выполнение

Правило 7

Полностью запретить использование определенного устройства для пользователя.

Проверить работоспособность и зафиксировать выполнение

Правило 8

С учетом ранее выполненного запрета необходимо предоставить временный доступ для определенного устройства не определенное время для пользователя.

Зафиксировать этапы выдачи доступа и работоспособность скриншотами.

Задача 4: разработать правила агентского мониторинга. Следующие правила создаются в политике «Test2».

Правило 9

Необходимо поставить на контроль буфер обмена в блокноте и notepad++. Проверить занесение нескольких событий в WEB-консоль.

Проверить работоспособность и зафиксировать выполнение скриншотом.

Правило 10

Необходимо запретить использовать терминальные сессиидля пользователя.

Проверить работоспособность и зафиксировать выполнение

Правило 11

Необходимо установить контроль за компьютером потенциального нарушителя путем создания снимков экрана каждые 60 секунд или при смене окна.

Проверить работоспособность и зафиксировать выполнение

Правило 12

Запретить передачу файлов определенного типа на съемные носители информации или в сетевое расположение.

Проверить работоспособность и зафиксировать выполнение

Задача 5: разработать и применить групповые политики домена.

Групповые применяются только на компьютер 2, должны быть созданы в домене.

Зафиксировать настройку политик скриншотами, при возможности проверки зафиксировать скриншотами проверку политик (например, запрет запуска).

Групповая политика 1

Настроить политику паролей и блокировки: Максимальный срок действия пароля, Минимальная длина пароля, Сложность пароля, Блокировка учетной записи при неверном вводе пароля.

Зафиксировать настройки политики скриншотами.

Групповая политика 2

Запретить запуск приложений по списку (по вариантам задания). Зафиксировать настройки политики и выполнение скриншотами.

Групповая политика 3

Запретить использование элементов системы стандартными политиками.

Зафиксировать настройки политики и выполнение скриншотами.

Групповая политика 4

Запретить пользователю самостоятельно менять параметры системы (по вариантам задания).

Зафиксировать настройки политики и выполнение скриншотами.

Групповая политика 5

Настроить дополнительные параметры системы, которые должны применяться для пользователя или компьютера (по вариантам задания).

Зафиксировать настройки политики и выполнение скриншотами.

Описание модуля С: «Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз»

Создайте в DLP-системе политики безопасности согласно нижеперечисленным заданиям. Политики должны автоматически блокировать трафик и/или предупреждать о нарушении в соответствии с заданием. Способ, которым создана корректная политика, оставлен на усмотрение самого экзаменуемого.

При выявлении уязвимости DLP-система должна автоматически устанавливать уровень угрозы в соответствии с заданием. После создания всех политик может быть запущен автоматический «генератор трафика», который передаст поток данных, содержащих как утечки, так и легальную информацию.

При правильной настройке политики должны автоматически выявить (или блокировать) и маркировать инциденты безопасности. Не должно быть ложных срабатываний. Не должно быть неправильной маркировки. Должны быть выявлены все инциденты безопасности.

Для некоторых политик могут понадобиться дополнительные файлы, расположение которых можно узнать из карточки задания или у экспертов.

Выполнение отдельных заданий необходимо подтвердить скриншотом (это всегда указывается отдельно). Скриншоты необходимо сохранить в папке «Модуль 3».

Скриншоты необходимо называть в соответствии с номером задания и типом задания (Например, Политика 2, Задание 1–1 и т. д.)

Задания на разработку политик можно выполнять в любом порядке. Наиболее сложные политики находятся в конце.

При разработке политик стоит учитывать, что все политики трафика могут передаваться как через веб-сообщения, так и через почтовые сообщения. В случае, если данный пункт не соблюден, то проверка заданий может быть невозможной.

Списки сотрудников, занимаемые позиции и отделы сотрудников представлены в разделе «Персоны» по результатам LDAP-синхронизации.

Список тегов для политик:

Политика 1, Политика 2, Политика 3, …

При выполнении модуля С ставятся следующие цели:

1. Настроить систему предотвращения утечек для правильного функционирования политик безопасности.

2. Произвести настройку технологий, используемых в политиках безопасности, а именно: лингвистический анализ, регулярные выражения, эталонные документы, графические объекты, выгрузки из баз данных.

3. Произвести верную настройку объектов защиты, верно выстроить логику

срабатывания.

4. Разработать политики безопасности для корректного срабатывания политик, указать направления передачи, уровень нарушений, вердикты, теги.

5. Произвести проверку работоспособности политик.

При выполнении модуля С ставятся следующие задачи:

Задача 1.1

Необходимо выключить или удалить стандартные политики и отключить стандартные каталоги объектов защиты.

Задача 1.2

Создайте локальную группу пользователей и добавьте в нее пользователей.

Задача 1.3

Создать список веб-ресурсов. Добавить в список следующие сайты: Site.ru, domain.com,

Задача 1.4

Для работы системы необходимо настроить периметр компании: Почтовый домен, список веб ресурсов, группа персон, исключить из перехвата.

Задача 2

Для контроля за движением документов необходимо вести наблюдение за передачей шаблона документа за пределы компании. Стоит учесть, что содержимое документа может изменяться в пределах определенного уровня.

Вердикт: разрешить Уровень нарушения: низкий Тег: Задача 2

Задача 3

У генерального директора компании недавно появился котик и его фото утекло в сеть компании. Теперь сотрудники обмениваются смешными картинками с подписями и масками внутри компании и выкладывают их в социальные сети. Директор решил, что его котик вызвал снижение качества работы сотрудников из-за повышенной милоты картинок и хочет запретить обмен фотографией котика. Необходимо запретить обмен фотографией и немного измененной фотографией котика.

Вердикт: блокировать Уровень нарушения: низкий

Задача 4

Необходимо отслеживать документы, содержащие печать компании всем сотрудникам, кроме отдела (по вариантам) и определенного сотрудника. Они могут обмениваться документами внутри и за пределами компании без контроля.

Вердикт: разрешить Уровень нарушения: низкий

Задача 5

В последнее время возникла необходимость обработки текстовых данных, а также сканов и фото кредитных карт. Необходимо отслеживать передачу всех возможных данных кредитных карт (в том числе сканов) за пределы компании.

Вердикт: разрешить

Уровень нарушения: средний Тег: Задача 5

Задача 6

Сотрудники заподозрены в сливе баз данных клиентов. Необходимо настроить мониторинг выгрузок из БД для контроля движения данных из базы данных страховых компаний только при отправке из определенного отдела, для остальных контролировать не нужно.

Критичными данными в выгрузке являются определенные поля и в 1 документе присутствует более 1 строчки. Для настройки используйте файл примера.

Вердикт: разрешить

Уровень нарушения: средний Тег: Задача 6

Задача 7

Некая компания попросила обеспечить защиту от утечки важных данных.

Необходимо создать политику на контроль правила передачи содержащие слова «один», «два», «три» в 1 сообщении или документе одновременно. Если в документе встречается только по 1 слову из перечисленных —Задача срабатывать не должна.

Правило должно срабатывать на сообщения, которые отправляются за пределы компании всеми пользователями, кроме определенного отдела, который может отсылать информацию свободно.

Вердикт: разрешить

Уровень нарушения: средний Тег: Задача 7

Задача 8

Для мониторинга движения анкет необходимо вести наблюдение за анкетами компании за пределы компании, запрещая любую внешнюю передачу документов в пустых и заполненных бланках.

Генеральный директор и совет директоров могут обмениваться данной информацией совершенно свободно. Вердикт: разрешить Уровень нарушения: средний Тег: Задача 8

Задача 9

Пользователи стали часто обмениваться ссылками и файлами, в связи с этим необходимо блокировать передачу (а где это невозможно — просто контролировать) файлов, например, формата.mp4 и ссылок определенного формата (содержит уникальную последовательность, например, urlname). Ложных срабатываний быть не должно.

Вердикт: Заблокировать Уровень нарушения: средний Тег: Задача 9

Задача 10

Было замечено, что сотрудники компании стали получать множество рекламных сообщений электронной почты, из-за чего возникла необходимость отследить утечку баз email адресов сотрудников. В связи с этим необходимо детектировать сообщения, содержащие адреса электронной почты.

Важно, чтобы в одном сообщении содержалось минимум 2 адреса (т. к. в противном случае будут детектироваться все почтовые сообщения)!

Возможные домены первого уровня: ru, org и прочие. Детектирование только частей адресов (например, @mail.ru) недопустимо.

Вердикт: разрешить

Уровень нарушения: высокий Тег: Задача 10

Задача 11

В связи с разгильдяйством сотрудников, передающих свои пароли коллегам с помощью почты и сообщений, необходимо предотвратить передачу любых стандартизированных паролей для информационной системы в открытом виде любыми отправителями и получателями как внутри, так и за пределы компании.

Стоит учесть, что пароли могут передаваться любым указанным способом: социальные сети и прочие ресурсы (в браузере), мессенджеры, почта, флешки. Необходимо также контролировать наличие паролей в сетевых каталогах.

Стоит учесть, что отдел так как генерацией паролей занимается отдел ИТ, то пользователи отдела могут рассылать пароли пользователям совершенно свободно, но только внутри компании.

Стандартизированные форматы паролей (кириллица):

6 букв – 1 знак !?#$^/_& – 2-4 цифры – 4 буквы – 2-3 знака !?#$^/_& (например, ПаРолЬ#67рКнЕ!?)

Вердикт: разрешить

Уровень нарушения: средний Тег: Задача 11

Задача 12

Необходимо контролировать передачу определенных типов файлов только за пределы компании.

Вердикт: разрешить Уровень нарушения: низкий Тег: Задача 12

Задача 13

В связи с тем, что компания является оператором обработки персональных данных, необходимо запретить всем сотрудникам кроме отдела (по вариантам) отправлять документы, содержащие информацию о паспортных данных за пределы компании. Отдел (по вариантам) может отправлять файлы без ограничений.

Вердикт: разрешить Уровень нарушения: низкий Тег: Задача 13

Описание модуля F: «Предотвращение инцидентов и управление событиями информационной безопасности»

Необходимо настроить виджеты и отчеты в системе предотвращения утечек.

<u>При выполнении модуля F ставятся следующие цели:</u>

1. Настройка контроля доступа к системе.
2. Разработка виджетов и отчетов, отображающих определенные события и инциденты безопасности.

<u>При выполнении модуля F ставятся следующие задачи:</u>

Задача 1: Контроль доступа

Необходимо создать пользователя DLP системы с определенными правами просмотра и редактирования.

Задача 2: Сводки

Создайте новые вкладки сводки в разделе «Сводка»

Задача 3: Виджеты

Создайте в сводке 4 виджета:

9. Выборка по событиям за период
10. Выборка по политикам с технологиями за период
11. Статистика за период
12. По нарушителям за период

Задача 4

Необходимо создать виджет отображающий события определенного типа (с определенного устройства и т. п.) за период.

Зафиксировать скриншотом конструктора выборки.

Задача 5

Необходимо создать виджет отображающий события определенного уровня (определенных политик и т. п.) за период.

Оценивание ответа на демонстрационном экзамене

Перевод суммы полученных баллов в оценки «отлично», «хорошо», «удовлетворительно», «неудовлетворительно» осуществляется в соответствии с порядком, утвержденным Первым проректором по УР АлтГУ.

Оценивание выпускной квалификационной работы

4-балльная шкала	**Показатели**	**Критерии**
Отлично	1. Степень соответствия работы уровню квалификационных требований, предъявляемых к подготовке студентов, а также требованиям, предъявляемым к ВКР; 2. Соответствие темы ВКР специализации программы, актуальность, степень разработанности темы; 3. Качество	ВКР носит исследовательский характер, содержит грамотно изложенную теоретическую базу, содержательный анализ практического материала, характеризуется логичным изложением материала с соответствующими выводами и обоснованными предложениями; ВКР оценена на «отлично» рецензентом
Хорошо		ВКР носит исследовательский характер, содержит грамотно изложенную теоретическую базу, достаточно подробный анализ практического материала; характеризуется в целом последовательным изложением материала; выводы по работе носят правильный, но не вполне развернутый характер; при защите обучающийся в целом показывает знания в определенной области, умеет опираться на данные своего исследования, вносит свои рекомендации; во время доклада, обучающийся без особых затруднений отвечает на поставленные вопросы ВКР оценена рецензентом

Удовлетворительно	и самостоятельность проведенного исследования/выполненного проекта, в том числе	ВКР носит исследовательский характер, содержит теоретическую главу и базируется на практическом материале, но отличается поверхностным анализом и недостаточно критическим разбором; в работе просматривается непоследовательность изложения материала, представлены недостаточно обоснованные утверждения; в отзыве рецензента имеются замечания по содержанию работы и методики анализа; при защите обучающийся проявляет неуверенность,показывает слабое знание вопросов определенной области, не дает полного, аргументированного ответа на заданные вопросы
Неудовлетворительно		ВКР не носит исследовательского характера, не содержит практического разбора; не отвечает требованиям, изложенным в методических указаниях АлтГУ; не имеет выводов либо они носят декларативный характер; в отзыве рецензента имеются замечания по содержанию работы и методики анализа; при защите обучающийся затрудняется отвечать на поставленные вопросы по теме, не знает теории вопроса, при ответе допускает существенные ошибки

Типовые контрольные задания или иные материалы, необходимые для оценки результатов освоения образовательной программы

Рекомендуемая тематика выпускных квалификационных работ

1. Проект обеспечения инженерно-технической защиты объекта офиса для усиления его информационной безопасности
2. Разработка комплексной системы защиты информации объекта защиты
3. Разработка комплексной системы защиты информации (КСЗИ) предприятия.
4. Разработка основных направлений совершенствования КСЗИ предприятия.
5. Разработка сценария инженерно-технической защиты информации в кабинете/подразделении (указать название) руководителя организации
6. Совершенствование системы информационной безопасности в помещениях название организации.
7. Организация безопасности сети предприятия с использованием операционной системы Linux
8. Автоматизация обеспечения информационной безопасности группы компаний на базе ОС Unix/Linux.
9. Организация безопасного удаленного доступа к ЛВС предприятия.
10. Построение защищенной виртуальной сети на базе специализированного программного обеспечения на предприятии.
11. Автоматизация учета конфиденциальных документов на предприятии.
12. Организация процессов мониторинга конфиденциального документооборота на предприятии.
13. Автоматизация процесса проверок наличия конфиденциальных документов на

предприятии.
14. Организация системы планирования и контроля функционирования КСЗИ на предприятии.
15. Организация подсистемы, обеспечивающей управление КСЗИ в условиях чрезвычайной ситуации на предприятии.

Методические материалы, определяющие процедуры оценивания результатовосвоения программы подготовки специалистов среднего звена

Формой государственной итоговой аттестации по программе подготовки специалистов среднего звена по специальности 10.02.05. Обеспечение информационной безопасности автоматизированных систем является защита выпускной квалификационной работы / проекта в виде дипломной работы и демонстрационного экзамена (ДЭ).

Демонстрационный экзамен проводится на основе требований к результатам освоения образовательной программы среднего профессионального образования, установленных ФГОС СПО по специальности 10.02.05. Обеспечение информационной безопасности автоматизированных систем. Процедура оценивания результатов выполнения заданий демонстрационного экзамена осуществляется в соответствии с требованиями комплекта оценочной документации.

Методические материалы, определяющие процедуры оценивания результатов освоения программы подготовки специалистов среднего звена по специальности 10.02.05. Обеспечение информационной безопасности автоматизированных систем.

План работы Центра проведения демонстрационного экзамена
по специальности 10.02.05. Обеспечение информационной безопасности автоматизированных систем
Адрес ЦПДЭ: г. Барнаул, проспект Комсомольский 100

День (00.00.0000)	**Начало мероприятия (укажите в формате ЧЧ:ММ)**	**Окончание мероприятия (укажите в формате ЧЧ:ММ)**	**Длительность мероприятия (расчет производится автоматически)**	**Мероприятие**
Подготовительный				Проверка готовности проведения демонстрационного экзамена
Подготовительный				Распределение обязанностей по проведению экзамена между членами Экспертной группы
Подготовительный				Инструктаж Экспертной группы по охране труда и технике безопасности, сбор подписей
Подготовительный				Регистрация участников демонстрационного экзамена
Подготовительный				Инструктаж участников по охране труда и технике безопасности
Подготовительный				Распределение рабочих мест(жеребьевка) и ознакомление участников с рабочими местами, оборудованием, графиком работы, иной документацией
Подготовительный				Получение главным экспертом

				задания демонстрационного экзамена

День (00.00.0000)	**Начало мероприятия(укажите в формате ЧЧ:ММ)**	**Окончание мероприятия(укажите в формате ЧЧ:ММ)**	**Длительность мероприятия (расчет производится автоматически)**	**Мероприятие**
День ДЭ				Ознакомление с заданием и правилами
День ДЭ				Брифинг экспертов
День ДЭ				Выдача задания
День ДЭ				Обед
День ДЭ				Выдача задания
День ДЭ				Работа экспертов