Государственное профессиональное образовательное учреждение
Ярославской области
Ярославский градостроительный колледж

ПРОГРАММА ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

специальности 10.02.05

«Обеспечение информационной безопасности автоматизированных систем»

Введено в действие с — 21.12.2022

Номер экземпляра: _____

Место хранения: _____

_____

Ярославль, 2022 г.

Лист утверждения и согласования

УТВЕРЖДАЮ
Директор колледжа
_____ М.Л Зуева
« 21 » декабря 2022 г.

.

ПРОГРАММА ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

по специальности

10.02.05 Обеспечение информационной безопасности автоматизированных систем

код и наименование

СОГЛАСОВАНО:

Педагогическим советом колледжа
название органа, подразделения и т.д.

« 21 » декабря 2022 г. Протокол № 6

Секретарь педагогического совета		Ковалева С.В.
должность	подпись	Фамилия И.О.

Председатель ГЭК Технический директор ГБУ ЯО Электронный регион
должность

	19.12.2022	Лукьяненко С.Ю.
подпись	дата	Фамилия И.О.

Заместитель директора по УВР
должность

	19.12.2022	Кулезнева И.Н.
подпись	дата	Фамилия И.О.

кафедра ИТ **Руководитель кафедры**

« 07 » декабря 2022 г. Протокол № 5 _____ Неделяева Н.А.
подпись Фамилия И.О.

Реестр рассылки

№ учтенного экземпляра	Подразделение	Количество копий
1.	Зам. директора по УВР	1
2.	кафедра	1
Размещено	Сайт колледжа / сведения об образовательной организации / Образование	

СОДЕРЖАНИЕ

1. Общие положения

Программа государственной итоговой аттестации разработана в соответствии с Федеральным законом от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации», ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утвержденного приказом Министерства образования и науки Российской Федерации от 09 декабря 2016 г №1547.

Настоящая Программа определяет совокупность требований к государственной итоговой аттестации по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, в части освоения профессиональных видов деятельности:

1. Эксплуатация автоматизированных (информационных) систем в защищенном исполнении

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

3. Защита информации техническими средствами

4. Выполнение работ по профессии "Наладчик технологического оборудования"

1.1. Результаты освоения ОПОП

ГИА позволяет оценить подготовку выпускников в трех направлениях: оценка уровня освоения дисциплин и компетенций, готовности к выполнению основных видов деятельности согласно получаемой квалификации специалиста среднего звена, освоению одной или нескольких профессий рабочих, должностей служащих.

При прохождении процедуры ГИА обучающиеся должны подтвердить освоение общих и профессиональных компетенций, достижения личностных результатов:

1.1.1 Перечень общих компетенций

Код	Наименование
ОК 1	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам
ОК 2	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности выполнения профессиональных задач, оценивать их эффективность и качество
ОК 3	Планировать и реализовывать собственное профессиональное и личностное развитие
ОК 4	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 5	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 6	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения
ОК 7	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях

ОК 8	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.
ОК 9	Использовать информационные технологии в профессиональной деятельности.
ОК 10	Пользоваться профессиональной документацией на государственном и иностранном языках.

1.1.2 Перечень личностных результатов

Код	***Наименование личностных результатов***
ЛР 1	Осознающий себя гражданином и защитником великой страны
ЛР 2	Проявляющий активную гражданскую позицию, демонстрирующий приверженность принципам честности, порядочности, открытости, экономически активный и участвующий в студенческом и территориальном самоуправлении, в том числе на условиях добровольчества, продуктивно взаимодействующий и участвующий в деятельности общественных организаций
ЛР 3	Соблюдающий нормы правопорядка, следующий идеалам гражданского общества, обеспечения безопасности, прав и свобод граждан России. Лояльный к установкам и проявлениям представителей субкультур, отличающий их от групп с деструктивным и девиантным поведением. Демонстрирующий неприятие и предупреждающий социально опасное поведение окружающих
ЛР 4	Проявляющий и демонстрирующий уважение к людям труда, осознающий ценность собственного труда. Стремящийся к формированию в сетевой среде личностно и профессионального конструктивного «цифрового следа»
ЛР 5	Демонстрирующий приверженность к родной культуре, исторической памяти на основе любви к Родине, родному народу, малой родине, принятию традиционных ценностей многонационального народа России
ЛР 6	Проявляющий уважение к людям старшего поколения и готовность к участию в социальной поддержке и волонтерских движениях
ЛР 7	Осознающий приоритетную ценность личности человека; уважающий собственную и чужую уникальность в различных ситуациях, во всех формах и видах деятельности.
ЛР 8	Проявляющий и демонстрирующий уважение к представителям различных этнокультурных, социальных, конфессиональных и иных групп. Сопричастный к сохранению, преумножению и трансляции культурных традиций и ценностей многонационального российского государства
ЛР 9	Соблюдающий и пропагандирующий правила здорового и безопасного образа жизни, спорта; предупреждающий либо преодолевающий зависимости от алкоголя, табака, психоактивных веществ, азартных игр и т.д. Сохраняющий психологическую устойчивость в ситуативно сложных или стремительно меняющихся ситуациях
ЛР 10	Заботящийся о защите окружающей среды, собственной и чужой безопасности, в том числе цифровой
ЛР 11	Проявляющий уважение к эстетическим ценностям, обладающий основами эстетической культуры
ЛР 12	Принимающий семейные ценности, готовый к созданию семьи и воспитанию детей; демонстрирующий неприятие насилия в семье, ухода от родительской ответственности, отказа от отношений со своими детьми и их финансового содержания
ЛР 13	Демонстрирующий умение эффективно взаимодействовать в команде, вести диалог, в том числе с использованием средств коммуникации
ЛР 14	Демонстрирующий навыки анализа и интерпретации информации из различных источников с учетом нормативно-правовых норм
ЛР 15	Демонстрирующий готовность и способность к образованию, в том числе самообразованию, на протяжении всей жизни; сознательное отношение к

	непрерывному образованию как условию успешной профессиональной и общественной деятельности.
ЛР 16	Сохраняющий психологическую устойчивость в ситуативно сложных или стремительно меняющихся ситуациях
ЛР 17	Экономически активный, предприимчивый, готовый к самозанятости
ЛР 18	Мотивированный к освоению функционально близких видов профессиональной деятельности, имеющих общие объекты (условия, цели) труда, либо иные схожие характеристики
ЛР 19	Проявляющий способность самостоятельно приобретать новые знание и умения по специальности, способность к своему постоянному профессиональному росту и повышению квалификации;

1.1.3 Перечень профессиональных компетенций

Код	Наименование
ВПД 1	**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
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
ВПД 2	**Защита информации в автоматизированных системах программными и программно-аппаратными средствами**
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
ВПД 3	**Защита информации техническими средствами**
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 34	Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации

Код	Наименование
ПК 3.5	Организовывать отдельные работы по физической защите объектов информатизации
ВПД 4	Выполнение работ по профессии "Наладчик технологического оборудования"
ПК 4.1	Осуществлять монтаж кабельной сети и оборудования локальных сетей различной топологии
ПК 4.2	Осуществлять настройку сетевых протоколов серверов и рабочих станций
ПК 4.3	Выполнять работы по эксплуатации и обслуживанию сетевого оборудования
ПК 4.4	Устанавливать и настраивать подключения к Интернету с помощью различных технологий и специализированного оборудования
ПК 4.5	Осуществлять выбор технологии подключения и тарифного плана у провайдера доступа в сеть Интернет.
ПК 4.6	Разрабатывать и использовать ресурсы сети Интернет, выполнять поиск данных с помощью поисковых систем

1.2 Форма государственной итоговой аттестации

В соответствии с Федеральным государственным образовательным стандартом среднего профессионального образования (далее ФГОС СПО) государственная итоговая аттестация включает проводится в форме защиты выпускной квалификационной работы и включает:

- дипломный проект и демонстрационный экзамен.

Демонстрационный экзамен проводится по двум уровням:

- базовый уровень;
- профильный уровень.

Демонстрационный экзамен базового уровня проводится, на базе колледжа (или другой организации) на основе требований к результатам освоения образовательных программ среднего профессионального образования, установленных ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем

Демонстрационный экзамен профильного уровня проводится по решению образовательной организации на основании заявлений выпускников, основывается на требованиях ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, а также квалификационных требований, заявленных организациями-работодателями, заинтересованными в подготовке кадров соответствующей квалификации, и проводится в центре проведения демонстрационного экзамена (в образовательной организации или на площадке организации-работодателя.

Объем времени на государственную итоговую аттестацию установлен ФГОС СПО – 6 недель, в том числе: 4 недели отведены на подготовку дипломного проекта и подготовку к демонстрационному экзамену и 2 недели на защиту дипломного проекта и проведение демонстрационного экзамена.

Сроки проведения государственной итоговой аттестации определены учебным планом и календарным учебным графиком по специальности.

2. Процедура проведения ГИА

2.1 Порядок проведения демоэкзамена базового уровня

Демонстрационный экзамен проводится с использованием КОД, включенных образовательными организациями в программу ГИА Задания для проведения демонстрационного экзамена для каждого студента определяется методом случайного выбора в начале демонстрационного экзамена.

КОД содержит:

Паспорт КОД с указанием:

- перечня знаний, умений и навыков и ПК в соответствии с ФГОС, проверяемых в рамках КОД базового уровня;
- обобщенной оценочной ведомости;
- количества экспертов, участвующих в оценке выполнения задания;
- списка оборудования и материалов, запрещенных на площадке (при наличии);
- время на выполнение – 3 часа
- Инструкцию по охране труда и технике безопасности для проведения демонстрационного экзамена;
- Образец задания для демонстрационного экзамена;
- Инфраструктурный лист;
- План застройки площадки для проведения демонстрационного экзамена.
- Инструкция по охране труда и технике безопасности для проведения демонстрационного экзамена по КОД базового уровня

Количество экспертов, участвующих в оценке выполнения задания

Количественный состав экспертной группы определяется образовательной организацией, исходя из числа сдающих одновременно демонстрационный экзамен выпускников. Один эксперт должен иметь возможность оценить результаты выполнения задания выпускников в полной мере согласно критериям оценивания.

Количество главных экспертов на демонстрационном экзамене 1

Минимальное (рекомендованное) количество экспертов на 1 выпускника 1

Минимальное (рекомендованное) количество экспертов на 5 выпускников 3

2.2 Порядок проведения демоэкзамена профильного уровня

Демонстрационный экзамен проводится по компетенции «Корпоративная защита от внутренних угроз информационной безопасности».

КОД 1.1 содержит:

Паспорт КОД с указанием:

- перечня знаний, умений и навыков из Спецификации стандарта компетенции «Корпоративная защита от внутренних угроз информационной безопасности», проверяемых в рамках КОД;
- обобщенной оценочной ведомости;
- количества экспертов, участвующих в оценке выполнения задания;
- списка оборудования и материалов, запрещенных на площадке (при наличии);
- Инструкцию по охране труда и технике безопасности для проведения демонстрационного экзамена;
- Образец задания для демонстрационного экзамена;
- Инфраструктурный лист;
- План проведения демонстрационного экзамена с указанием времени и продолжительности работы участников и экспертов;
- План застройки площадки для проведения демонстрационного экзамена.
- Инструкция по охране труда и технике безопасности для проведения демонстрационного экзамена по компетенции: «Корпоративная защита от внутренних угроз информационной безопасности»

Количество экспертов, участвующих в оценке выполнения задания

Минимальное количество экспертов, участвующих в оценке демонстрационного экзамена по компетенции «Корпоративная защита от внутренних угроз информационной безопасности» - 3 чел.

Дополнительное количество экспертов рассчитывается исходя из количества участников демонстрационного экзамена – 1 эксперт на 12 участников.

2.3 Порядок защиты дипломного проекта

На подготовку и проведение ГИА по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем в календарном учебном графике установлены следующие сроки:

- подготовка выпускной квалификационной работы – 4 недели;
- защита выпускной квалификационной работы – 2 недели.

Тематика дипломных проектов разрабатывается преподавателями колледжа. Студенту предоставляется право выбора темы выпускной квалификационной работы, в том числе предложения своей тематики с необходимым обоснованием целесообразности ее разработки для практического применения. При этом тематика выпускной квалификационной работы должна соответствовать содержанию одного или нескольких профессиональных модулей, входящих в образовательную программу среднего профессионального образования. Темы дипломных проектов должны отвечать

современным требованиям техники и технологиям в области разработки и сопровождения информационных систем.

Тематика дипломных проектов рассматривается на заседании кафедры. Примерная тематика дипломных проектов приведена в Приложении 1.

Закрепление за студентами тем выпускных квалификационных работ, назначение руководителей и консультантов осуществляется приказом

Заведующий отделением:

- готовит приказ о закреплении за студентами руководителей, консультантов и тем дипломных проектов;
- знакомит студентов с приказом о закреплении тем дипломных проектов не позднее, чем за две недели до начала преддипломной практики;
- оказывает помощь студентам в обеспечении техническими средствами для выполнения дипломного проекта;
- направляет студентов на рецензирование дипломных проектов.

Руководитель кафедры:

- знакомит студентов с программой ГИА не позднее, чем за 6 месяцев до начала выполнения дипломного проекта и составляет протокол ознакомления;
- готовит предложения о назначении руководителей и консультантов дипломных проектов;
- составляет график выполнения дипломного проектирования, который согласуется с заведующим отделением и утверждается заместителем директора по УВР (приложение 5);
- составляет расписание консультаций руководителей проектов и консультантов.

Руководители дипломных проектов:

- разрабатывают задание на дипломное проектирование для каждого студента, которые согласуются руководителем кафедры и утверждаются заведующим отделением;
- выдают студентам задания на дипломное проектирование перед выходом на преддипломную практику; выдача задания на дипломное проектирование сопровождается консультацией, в ходе которой разъясняется цель и задачи, структура и объём работы, принципы разработки и оформления, распределение времени на выполнение отдельных разделов дипломного проекта;
- проводят консультации по вопросам содержания и последовательности выполнения дипломного проекта;
- оказывают помощь в подборе необходимой литературы;
- осуществляют контроль выполнения дипломного проекта;
- оказывают помощь в оформлении дипломного проекта, подготовке выступления к защите проекта;
- дают заключение на выполненный студентом дипломный проект.

За каждым руководителем дипломного проекта может быть закреплено не более 8 студентов.

Консультанты дипломных проектов оказывают квалифицированную помощь в выполнении проектов по соответствующим направлениям.

Комиссия в составе: зав. отделением, руководитель проекта, руководитель кафедры, производит контрольные проверки (процентовки) в ходе выполнения дипломного проекта в соответствии со сроками, установленными графиком выполнения разделов дипломного проекта.

По итогам последней контрольной проверки составляется график защиты дипломных проектов.

На последней неделе выполнения ДП проводятся предзащиты дипломных проектов. Организуется предзащита дипломных проектов в присутствии руководителя проекта и руководителя кафедры. По результатам предзащиты ДП осуществляется допуск студентов к защите дипломных проектов.

Общее руководство и контроль за ходом выполнения дипломного проекта осуществляет зам. директора по УВР.

Государственная итоговая аттестация выпускников осуществляется государственной экзаменационной комиссией (ГЭК).

Состав ГЭК утверждается приказом директора по колледжу. Численность ГЭК не менее 5 человек. Состав ГЭК:

- **председатель** – ведущий специалист - представитель работодателя по профилю подготовки выпускников; руководитель или заместитель руководителя организации, осуществляющей образовательную деятельность по профилю подготовки выпускников, имеющий ученую степень и (или) ученое звание или высшую квалификационную категорию;
- **заместитель председателя** – директор, заместитель директора колледжа или педагогические работники, имеющие высшую квалификационную категорию;
- **члены комиссии** – руководитель кафедры, преподаватели, имеющие высшую или первую квалификационную категорию;
- **секретарь** – назначается из числа членов комиссии.

Основные функции ГЭК:

- определение соответствия результатов освоения студентами программы подготовки специалистов среднего звена соответствующим требованиям федерального государственного образовательного стандарта среднего профессионального образования;
- решение вопроса о присвоении квалификации по результатам ГИА и выдаче выпускнику соответствующего диплома о среднем профессиональном образовании, решение оформляется протоколом (приложение 1);

- вносить предложения по дальнейшему совершенствованию подготовки выпускников.

Председатель ГЭК:

- участвует в обсуждении положения и программы ГИА;
- организует и контролирует деятельность ГЭК;
- обеспечивает единство требований, предъявляемых к выпускникам.

Решение ГЭК принимается на закрытом заседании большинством голосов членов комиссии при обязательном присутствии председателя комиссии или его заместителя (при равном числе голосов голос председательствующего на заседании ГЭК является решающим).

Заседания ГЭК протоколируются. Протокол подписывается председателем и секретарём комиссии. Книга протоколов должна быть прошнурована, пронумерована и скреплена печатью. Книга протоколов хранится в архиве.

Решение ГЭК о присвоении квалификации выпускникам, прошедшим ГИА, и выдаче соответствующего документа об образовании, объявляется приказом директора колледжа.

По результатам работы в недельный срок председатель ГЭК составляет отчёт установленной формы, который обсуждается на заседании кафедры, педагогическом совете и представляется учредителю.

3. Требования к ВКР и методика их оценивания

3.1 Описание задания демонстрационного экзамена базового уровня и критериев его оценки

№ п/п	Модуль задания (вид деятельности, вид профессиональной деятельности)	Критерий оценивания[5]	Баллы
1	2	3	4
1	Эксплуатация автоматизированных (информационных) систем в 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 защищенном 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**

Максимальное количество баллов, которое возможно получить за выполнение задания демонстрационного экзамена, принимается за 100%. Перевод баллов в оценку может быть осуществлен на основе Таблицы 2

Таблица 2

Оценка ГИА	«2»	«3»	«4»	«5»
Отношение полученного количества баллов к максимально возможному (в процентах)	0,0% - 19,99%	20,0% - 39,99%	40% - 69,99%	70% - 100,00%

3.2 Описание задания демонстрационного экзамена профильного уровня и критериев его оценки

Модуль 1: Исследование (аудит) организации с целью защиты от внутренних угроз.

обследование и анализ структуры организации (как главного объекта защиты) на основании представленных материалов и стенда, её вычислительно-сетевой инфраструктуры, определить потоки данных, потенциальные угрозы и каналы утечек.

Модуль 2: Разработка политик информационной безопасности.

разработать политики информационной безопасности, используя инструментарий автоматизированной системы, а также, по средствам имитации процесса утечки конфиденциальной информации, протестировать факт перехвата системой, в соответствии с объектами защиты разработанной политики ИБ, удостовериться что перехват работает..

Модуль 3 Настройка и тестирование системы защиты от внутренних угроз

функциональность и соответствие настроек целевой сетевой инфраструктуре

- Провести имитацию процесса утечки конфиденциальной информации в системе;

Модуль 4: Контроль информационных потоков и применение политик

Политики информационной безопасности в системе, выполнить поиск инцидентов информационной безопасности

Модуль 5: Анализ выявленных инцидентов

Использование аналитического функционала и фильтров системы для детализированного поиска инцидентов безопасности и работы с ними.

Критерии оценки

В данном разделе определены критерии оценки и количество начисляемых баллов (субъективные и объективные) в Таблице 1.

Таблица 1.

№ п/п	Модуль задания, где проверяется критерий	Критерий	Разделы WSSS	Судейские баллы	Объективные баллы	Общие баллы
1	2	3	4	5	6	7
1.	Модуль A. Установка, конфигурирование и устранение неисправностей в системе систем корпоративной защиты от внутренних угроз	B.Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз	2	0,00	14,00	14,00
2.	Модуль E. Технологии защиты узла и агентского мониторинга	F.Технологии защиты узла и агентского мониторинга	6	0,00	18,00	18,00
3.	Модуль C. Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз	D.Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз	4	0,00	18,00	18,00
4.	Модуль F. Предотвращение инцидентов и управление событиями информационной безопасности	G.Предотвращение инцидентов и управление событиями информационной безопасности	7	0,00	4,00	4,00
Итог	-	-	-	0,00	54,00	54,00

Максимальное количество баллов, которое возможно получить за выполнение задания демонстрационного экзамена, принимается за 100%. Перевод баллов в оценку может быть осуществлен на основе Таблицы 2

Таблица 2

Оценка ГИА	«2»	«3»	«4»	«5»
Отношение полученного количества баллов к максимально возможному (в процентах)	0,0% - 19,99%	20,0% - 39,99%	40% - 69,99%	70% - 100,00%

3.3 Требования к дипломным проектам

Для обеспечения единства требований к выпускной квалификационной работе студентов устанавливаются общие требования к структуре и объему дипломного проекта.

Требования к структуре и оформлению дипломного проекта

В состав дипломного проекта входит пояснительная записка и файлы, а также схемы, макеты на CD, DVD, Flash-накопителях.

Все приложенные файлы должны открываться в режиме offline, как запускаемые файлы или с помощью установленных приложений.

Объём пояснительной записки – не менее 70 страниц рукописного или 40 страниц печатного текста. Пояснительная записка должна быть переплетена и подписана дипломником с указанием даты окончания работы над проектом.

В пояснительной записке к дипломному проекту должна быть четко выдержана структура.

Титульный лист является первой страницей, оформляется на типовом бланке.

Задание на дипломный проект является второй страницей и оформляется на бланке установленной формы с указанием даты выдачи задания, сроков выполнения и даты сдачи законченной работы.

Заключение руководителя оформляется на типовом бланке.

Рецензия оформляется на типовом бланке.

Содержание ДП включает названия глав и параграфов с указанием страниц, с которых они начинаются. Пункты содержания соответствуют заголовкам глав и параграфов в тексте работы, представление их в тексте в другой редакции не допускается.

Введение должно содержать общие сведения о работе, ее краткую характеристику. В нем необходимо отразить актуальность выбранной темы, цель и задачи, решаемые в работе, используемые методики и средства разработки, практическую значимость полученных результатов.

Во введении необходимо также перечислить вопросы, которые будут рассмотрены в проекте, выделив вопросы, которые предполагается решить практически.

Основная часть содержит несколько глав, каждая из которых может делиться на необходимое количество разделов.

Содержание глав основной части должно точно соответствовать теме дипломного проекта и полностью его раскрывать. Главы целесообразно завершать краткими выводами.

Первая глава посвящена рассмотрению теоретических аспектов исследуемой темы и служит основой для дальнейшего изложения материала.

В этой главе рассматривается сущность, содержание, организация исследуемого процесса, его составные элементы.

Полученные в результате рассмотрения первой главы выводы должны раскрыть новизну работы, которая формулируется во введении. Приводимые факты и числовой материал должны быть достоверными.

При написании дипломной работы собранный во время прохождения студентами производственной и преддипломной практики по исследуемой теме материал дополняется и обновляется.

Предлагается примерное содержание **первой главы**:

Постановка задачи

Методы и средства решения задачи

В данном подразделе следует раскрыть современное состояние технологий в области информационной безопасности, а также более подробно описать поставленные задачи, которые должны быть реализованы в проекте.

В зависимости от темы дипломного проекта (применение программно-аппаратных средств или инженерно - технических средств обеспечения информационной безопасности) рассматриваются различные современные технологии, методы и средства защиты информации в автоматизированных системах (АС), например:

для ВКР, посвященных совершенствованию системы безопасности автоматизированных систем необходимо провести исследование текущего состояния информационной безопасности организации по направлениям:

методы и средства организационно-правовой защиты информации;

методы и средства инженерно-технической защиты информации;

аппаратные методы и средства защиты информации.

Содержание и структура глав дипломного проекта могут быть изменены дипломником совместно с руководителем в соответствии с темой дипломного проекта и поставленными задачами.

Глава 2. Практическая часть (наименование главы определяется тематикой дипломной работы, например, Проектирование системы инженерно-технических для защиты).

В данной главе должно содержаться пошаговое описание процесса практических мероприятий при решении поставленных задач по защите информации автоматизированных систем. На основе моделирования угроз рассчитывается структура комплекса по защите информации автоматизированных систем. Разрабатывается схема комплексной системы защиты безопасности с расчётом возможностей применяемых инженерно-технических или программно-аппаратных средств

В **заключении** могут быть освещены следующие моменты:

В заключении кратко и логически последовательно излагаются теоретические и практические выводы и предложения, они должны вытекать из содержания работы и носить обобщающий характер. Из текста заключения должно быть ясно, что цель и задачи дипломного проекта полностью выполнены. Последовательность изложения выводов должна соответствовать порядку представления материалов в тексте работы.

Следует также указать пути внедрения работы (если таковое имеет место), сформулировать перспективные направления развития темы диплома. Заключение представляет собой связный, четкий, компактный текст. Заключение завершается оценкой перспектив исследуемой проблемы в целом.

Объем заключения занимает 2 – 3 страницы.

Материалы дипломного проекта должны излагаться четко, ясно, последовательно, соблюдая логичность перехода от одной главы к другой и от одного параграфа к другому. Законченную мысль в тексте необходимо выделять в самостоятельный абзац, применяя для этого «красную строку».

Следует использовать принятую научную терминологию, избегать повторений общеизвестных положений, имеющихся в учебниках и учебных пособиях. Уточнять необходимо только понятия малоизвестные или противоречивые, делая ссылку на авторов, высказывающих разные мнения по одному и тому же вопросу.

Особое внимание должно быть уделено языку и стилю написания пояснительной записки, свидетельствующей об общем уровне подготовки будущего специалиста, его профессиональной культуре.

Стиль написания – безличный монолог, т.е. изложение, ведется от второго лица, множественного числа. Не употребляется форма первого и второго лица местоимений единственного числа.

Во всем дипломном проекте должно быть достигнуто единообразие терминов, обозначений и условных сокращений.

Список литературы (библиографический список) содержит не менее 10 наименований литературных источников, оформляется в соответствии с принятым стандартом (ГОСТ 7.1-2016).

В список включаются только те источники, которые использовались при подготовке дипломного проекта и на которые имеются ссылки в основной части работы.

Приложение содержит файлы со всеми компонентами АИС и вспомогательный материал, не включенный в основную часть пояснительной записки (таблицы, схемы, заполненные формы отчетности, инструкции, распечатки, фрагменты нормативных документов и т.д.). Указанный материал включается в приложение с целью сокращения объема основной части, страницы его не входят в подсчет общего объема работы.

Конкретный состав приложений, их объем, включая иллюстрационный материал, определяются по согласованию с руководителем дипломного проекта. Объем приложений не ограничивается и не учитывается при определении общего объема работы.

Связь приложений с текстом осуществляется с помощью ссылок со словами «смотри», которое сокращается и заключается в круглые скобки

Файлы с компонентами АИС на CD, DVD, Flash-накопителях.

Пояснительная записка дипломного проекта должна быть выполнена машинописным способом с помощью компьютера на одной стороне листа белой бумаги формата А4 (210*297 мм) через полтора межстрочных интервала. Шрифт – 14. Размер полей составляет: левое – 30 мм; правое – 20 мм; верхнее – 20 мм, нижнее – 20 мм. Вписывать в текст отдельные слова, условные знаки допускается только черного цвета, причем плотность вписанного текста должна соответствовать плотности основного текста. Опечатки или графические неточности допускается исправлять путем применения специальных корректирующих средств с последующим внесением исправлений черным цветом. На странице не должно быть более пяти исправлений.

Необходимые сноски и подстрочные примечания помещаются в нижней части соответствующей страницы и заканчиваются до границы нижнего поля.

Номера страниц проставляются в правом верхнем углу листа, соблюдая сквозную нумерацию по всему тексту работы. Точка в номере страницы не ставится. Титульный лист и задание на дипломное проектирование включаются в общую нумерацию страниц, но номер страницы на них не проставляется. Нумерация начинается с 3-ей страницы – «Содержание».

Каждая новая глава и другие структурные элементы работы – введение, заключение, список литературы, приложения, кроме параграфов, входящих в состав глав, начинаются с новой страницы. Фразы, начинающиеся с «красной строки», выделяют абзацным отступом, равным 15 мм (5 печатных знаков).

Расстояние между заголовком главы и последующим текстом должно быть равно трем межстрочным интервалом (т.е. следует пропустить одну строку).

Критерии оценки дипломных проектов

Для определения качества выполнения и защиты дипломных проектов предлагаются следующие основные показатели ее оценки:

- соответствие темы исследования сформулированным целям и задачам;
- умение систематизировать и обобщать факты, самостоятельно решать поставленные задачи (в том числе нестандартные) с использованием передовых научных технологий;
- структура дипломной работы и культура ее оформления; последовательность и логичность, завершенность изложения, наличие научно-справочного аппарата, стиль изложения;
- использование в работе научных достижений отечественных и зарубежных исследователей и реального опыта; апробация в среде специалистов-практиков;
- использование современных технологий, применение в работе методов исследования;
- возможность использования результатов в профессиональной практике для решения образовательных задач.

Оценка качества дипломного проекта является комплексной. Государственная экзаменационная комиссия при оценке дипломного проекта обращает внимание на содержание и качество проведенного исследования (проектирования), оформление работы, содержательность ответов студентов на вопросы комиссии, оценку рецензента и отзыв руководителя.

Подготовка и защита дипломного проекта студентом позволяет оценить освоение общих и профессиональных компетенций, сформированности личностных результатов.

Оценка по результатам защиты дипломного проекта определяется баллами «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

«отлично»	1. Студент своевременно отчитывался по всем этапам выполнения дипломного проекта 2. Текстовое описание дипломного проекта составлено в полном объеме и аккуратно. 3. Во время защиты студент показал свободное владение темой проекта, знание используемых терминов. Для защиты студент использовал презентацию. 4. Выпускная квалификационная работа соответствует

	утвержденной теме и в полной мере отражает профессиональные знания выпускника
«хорошо»	1. Студент своевременно отчитывался по всем этапам выполнения дипломного проекта 2.Текстовое описание дипломного проекта составлено не в полном объеме. 3. Во время защиты студент показал свободное владение темой проекта, знание используемых терминов. Для защиты студент использовал презентацию. 4. Выпускная квалификационная работа соответствует утвержденной теме
«удовлетвори-тельно»	1. Студент несвоевременно отчитывался по всем этапам выполнения дипломного проекта 2. Текстовое описание дипломного проекта составлено не в полном объеме и недостаточно аккуратно. 3. Во время защиты студент показал слабые знания по теме проекта. Для защиты студент не использовал презентацию или презентация выполнена на слабом уровне 4. Выпускная квалификационная работа соответствует утвержденной теме
«неудовлетворительно»	1. Студент не выполнил дипломный проект. 2. Студент не владеет темой проекта и не ответил на дополнительные вопросы. 3. Пояснительная записка или выступление студента или приложенные файлы не соответствуют теме проекта.

4. Порядок проведения ГИА для выпускников из числа лиц с ограниченными возможностями здоровья и инвалидов

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 (далее - индивидуальные особенности) таких обучающихся.

При проведении демонстрационного экзамена обеспечивается соблюдение требований, закрепленных в статье 79 «Организация получения образования обучающимися с ограниченными возможностями здоровья» Закона об образовании и разделе V Порядка проведения государственной итоговой аттестации по образовательным программам среднего профессионального образования приказа Министерства образования и науки Российской Федерации от 16 августа 2013 г. № 968, определяющих Порядок проведения государственной итоговой аттестации для выпускников из числа лиц с ОВЗ и инвалидов.

При проведении демонстрационного экзамена для лиц с ОВЗ и инвалидов при необходимости надо предусмотреть возможность увеличения времени, отведенного на

выполнение задания и организацию дополнительных перерывов, с учетом индивидуальных особенностей таких обучающихся.

Перечень оборудования, необходимого для выполнения задания демонстрационного экзамена, может корректироваться, исходя из требований к условиям труда лиц с ОВЗ и инвалидов.

Рабочие места при необходимости должны быть оборудованы специальными приспособлениями.

Для сопровождения лиц с ограниченными возможностями здоровья и инвалидов на площадку проведения демонстрационного экзамена могут привлекаться ассистенты или волонтеры.

5. Порядок апелляции и пересдачи ГИА

ГИА выпускников осуществляется государственной экзаменационной комиссией.

По результатам государственной аттестации выпускник, участвовавший в ГИА, имеет право подать в апелляционную комиссию (АК) письменное апелляционное заявление о нарушении, по его мнению, установленного порядка проведения ГИА и (или) несогласии с ее результатами (далее - апелляция).

Апелляция подается лично выпускником или родителями (законными представителями) несовершеннолетнего выпускника в АК образовательной организации.

Апелляция о нарушении порядка проведения ГИА подается непосредственно в день проведения ГИА.

Апелляция о несогласии с результатами ГИА подается не позднее следующего рабочего дня после объявления результатов ГИА.

Апелляция рассматривается АК не позднее трех рабочих дней с момента ее поступления.

Состав АК утверждается образовательной организацией одновременно с утверждением состава ГЭК.

АК формируется в количестве не менее пяти человек из числа преподавателей образовательной организации, имеющих высшую или первую квалификационную категорию, не входящих в данном учебном году в состав ГЭК. Председателем АК является руководитель образовательной организации либо лицо, исполняющее обязанности руководителя на основании распорядительного акта образовательной организации.

Апелляция рассматривается на заседании АК с участием не менее двух третей ее состава.

На заседание АК приглашается председатель соответствующей ГЭК.

Выпускник, подавший апелляцию, имеет право присутствовать при рассмотрении апелляции. С несовершеннолетним выпускником имеет право присутствовать один из

родителей (законных представителей). Указанные лица должны иметь при себе документы, удостоверяющие личность.

Рассмотрение апелляции не является пересдачей ГИА.

При рассмотрении апелляции о нарушении порядка проведения ГИА апелляционная комиссия устанавливает достоверность изложенных в ней сведений и выносит одно из решений:

- об отклонении апелляции, если изложенные в ней сведения о нарушениях порядка проведения ГИА выпускника не подтвердились и/или не повлияли на результат ГИА;
- об удовлетворении апелляции, если изложенные в ней сведения о допущенных нарушениях порядка проведения ГИА выпускника подтвердились и повлияли на результат ГИА.

В последнем случае результат проведения ГИА подлежит аннулированию, в связи с чем протокол о рассмотрении апелляции не позднее следующего рабочего дня передается в ГЭК для реализации решения комиссии. Выпускнику предоставляется возможность пройти ГИА в дополнительные сроки, установленные образовательной организацией.

Для рассмотрения апелляции о несогласии с результатами ГИА, полученными при защите выпускной квалификационной работы, секретарь ГЭК не позднее следующего рабочего дня с момента поступления апелляции направляет в АК выпускную квалификационную работу, протокол заседания ГЭК и заключение председателя ГЭК о соблюдении процедурных вопросов при защите подавшего апелляцию выпускника.

В результате рассмотрения апелляции о несогласии с результатами ГИА АК принимает решение об отклонении апелляции и сохранении результата ГИА либо об удовлетворении апелляции и выставлении иного результата ГИА. Решение АК не позднее следующего рабочего дня передается в ГЭК. Решение АК является основанием для аннулирования ранее выставленных результатов ГИА выпускника и выставления новых.

Решение АК принимается простым большинством голосов. При равном числе голосов голос председательствующего на заседании АК является решающим.

Решение АК доводится до сведения подавшего апелляцию выпускника (под роспись) в течение трех рабочих дней со дня заседания АК.

Решение АК является окончательным и пересмотру не подлежит.

Решение АК оформляется протоколом, который подписывается председателем и секретарем АК и хранится в архиве образовательной организации.

Приложение 1

Примерные темы дипломных проектов для специальности

10.02.05 Обеспечение информационной безопасности автоматизированных систем

1.	Разработка информационно-поисковой системы, приложения баз данных: складской учет, библиотечные системы кадровый состав, системы хранения и обработки информации, создание комментариев, руководств пользователей для новых программных средств, адаптация их для конкретной организации, разработка программных средств защиты информационных систем
2.	Программирование расчетных задач: задачи моделирования и расчета производственных процессов, разработка программных модулей для бухгалтерских пакетов, корпоративных систем
3.	Создание WEB-сайтов, средств дистанционного обучения: создание сайтов организации, создание тематических сайтов, разработка электронных учебников, разработка обучающих игр
4.	Проектирование компьютерной сети в соответствии с заданными параметрами
5.	Разработка программных средств по защите информации

Приложение 2

Пример задания демонстрационного экзамена базового уровня

Описание общих требований
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 DLP-сервером 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 веб-сервер 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 6С 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
Настроить политику паролей и блокировки:
- Максимальный срок действия пароля: 47 дней
- Минимальная длина пароля: 8 символов
- Блокировка пользователя при неправильном вводе пароля: 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

Приложение 2

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 срабатываниевсеми 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 DLP-сервером 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 E 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 E 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 сессии для 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 черезпочтовые сообщения. Вслучае, 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 документевстречаетсятолько по 1 словуиз 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

Задача 9

Пользователи стали часто обмениваться ссылками и файлами, в связис 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.

При выполнении модуля F ставятся следующие цели: 1. Настройка контроля доступа к системе.

2. Разработка виджетов и отчетов, отображающих определенные события и инциденты безопасности.

При выполнении модуля F ставятся следующие задачи: 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.

Приложение 4

Инструкция по охране труда и технике безопасности для проведения демонстрационного экзамена

1.1. Программа инструктажа по охране труда и технике безопасности

Инструктаж по охране труда и технике безопасности должен включать: – Общие сведения о месте проведения экзамена, расположении компетенции, времени трансфера до места проживания, расположении транспорта для площадки, особенности питания участников и экспертов, месторасположении санитарно-бытовых помещений, питьевой воды, медицинского пункта, аптечки первой помощи, средств первичного пожаротушения.

– Время начала и окончания проведения экзаменационных заданий, нахождение посторонних лиц на площадке.

– Контроль требований охраны труда участниками и экспертами.

– Вредные и опасные факторы во время выполнения экзаменационных заданий и нахождение на территории проведения экзамена.

– Общие обязанности участника и экспертов по охране труда, общие правила поведения во время выполнения экзаменационных заданий и на территории.

– Основные требования санитарии и личной гигиены.

– Средства индивидуальной и коллективной защиты, необходимость их использования.

– Порядок действий при плохом самочувствии или получении травмы. Правила оказания первой помощи.

– Действия при возникновении чрезвычайной ситуации, ознакомление со схемой эвакуации и пожарными выходами.

1.2. Инструкция по охране труда для участников

1.2.1. Общие требования охраны труда

• К самостоятельному выполнению заданий экзамена по стандартам «WorldSkills» допускаются участники:

• прошедшие инструктаж по охране труда по «Программе инструктажа по охране труда и технике безопасности»;

• ознакомленные с инструкцией по охране труда;

• имеющие необходимые навыки по эксплуатации инструмента, приспособлений совместной работы на оборудовании;

• не имеющие противопоказаний к выполнению заданий по состоянию здоровья.

• При работе с ПК рекомендуется организация перерывов на через каждые 45 минут работы.

• При работе на ПК могут воздействовать опасные и вредные производственные факторы:

• физические: повышенный уровень электромагнитного излучения; повышенный уровень статического электричества; повышенная яркость светового изображения; повышенный уровень пульсации светового потока; повышенное значение напряжения в электрической цепи, замыкание которой может произойти через тело человека; повышенный или пониженный уровень освещенности; повышенный уровень прямой и отраженной блескости;

• психофизиологические: напряжение зрения и внимания; интеллектуальные и эмоциональные нагрузки; длительные статические нагрузки; монотонность труда.

• Запрещается находиться возле ПК в верхней одежде, принимать пищу и курить, употреблять во время выполнения задания алкогольные напитки, а также приходить на площадку в состоянии алкогольного, наркотического или другого опьянения.

• Участник экзамена должен знать месторасположение первичных средств пожаротушения.

• О каждом несчастном случае пострадавший или очевидец несчастного случая немедленно должен известить ближайшего эксперта. • В помещении экспертов находится аптечка первой помощи, укомплектованная изделиями медицинского назначения, ее необходимо использовать для оказания первой помощи, самопомощи в случаях получения травмы.

• В случае возникновения несчастного случая или болезни участника, об этом немедленно уведомляются Главный эксперт и линейные Эксперты. Главный эксперт принимает решение о назначении дополнительного времени для участия. В случае отстранения участника от дальнейшего участия в экзамене ввиду болезни или несчастного случая, он получит баллы за любую завершенную работу.

• Вышеуказанные случаи подлежат обязательной регистрации в Форме регистрации несчастных случаев и в Форме регистрации перерывов в работе. Знаки безопасности, используемые на рабочем месте, для обозначения присутствующих опасностей:

• F 04 Огнетушитель

• E 22 Указатель выхода

• E 23 Указатель запасного выхода

• EC 01 Аптечка первой медицинской помощи

• При работе с ПК участники экзамена должны соблюдать правила личной гигиены.

• Работа на площадке разрешается исключительно в присутствии эксперта. Запрещается присутствие на площадке посторонних лиц. • По всем вопросам, связанным с работой компьютера, следует обращаться к техническому эксперту.

• Участники, допустившие невыполнение или нарушение инструкции по охране труда, привлекаются к ответственности в соответствии с Регламентом.

• Несоблюдение норм безопасности может привести к временному или перманентному отстранению аналогично апелляции

1.2.2. Требования охраны труда перед началом выполнения работ

• В подготовительный день все участники должны ознакомиться с инструкцией по технике безопасности, с планами эвакуации при возникновении пожара, местами расположения санитарно-бытовых помещений, медицинскими кабинетами, питьевой воды, подготовить рабочее место в соответствии с Техническим описанием компетенции

• По окончании ознакомительного периода, участники подтверждают свое ознакомление со всеми процессами, подписав лист прохождения инструктажа по работе на оборудовании по форме, определенной Оргкомитетом.

• Подготовить рабочее место:

• Осмотреть и привести в порядок рабочее место, убрать все посторонние предметы, которые могут отвлекать внимание и затруднять работу.

• Проверить правильность установки стола, стула, подставки под ноги, угол наклона экрана монитора, положения клавиатуры в целях исключения неудобных поз и длительных напряжений тела. Особо обратить внимание на то, что дисплей должен находиться на расстоянии не менее 50 см от глаз (оптимально 60-70 см).

• Проверить правильность расположения оборудования.

• Кабели электропитания, удлинители, сетевые фильтры должны находиться с тыльной стороны рабочего места, сетевые фильтры не должны лежать на полу.

• Убедиться в отсутствии засветок, отражений и бликов на экране монитора.

• Убедиться в том, что на устройствах ПК (системный блок, монитор, клавиатура) не располагаются сосуды с жидкостями, сыпучими материалами (чай, кофе, сок, вода и пр.).

• Включить электропитание в последовательности, установленной инструкцией по эксплуатации на оборудование; убедиться в правильном выполнении процедуры загрузки оборудования, правильных настройках. Участнику запрещается приступать к выполнению задания при обнаружении неисправности оборудования. О замеченных недостатках и

неисправностях немедленно сообщить Эксперту и до устранения неполадок к заданию не приступать.

1.2.3. Требования охраны труда во время выполнения работ

• В течение всего времени выполнения задания со средствами компьютерной и оргтехники участник экзамена обязан: • содержать в порядке и чистоте рабочее место;

• следить за тем, чтобы вентиляционные отверстия устройств ничем не были закрыты;

• выполнять требования инструкции по эксплуатации оборудования;

• соблюдать, установленные расписанием, перерывы в выполнении задания, выполнять рекомендованные физические упражнения.

• Участнику запрещается во время выполнения задания:

• отключать и подключать интерфейсные кабели периферийных устройств если это не указано в задании;

• класть на устройства средств компьютерной и оргтехники бумаги, папки и прочие посторонние предметы;

• прикасаться к задней панели системного блока (процессора) при включенном питании;

• отключать электропитание во время выполнения программы, процесса;

• допускать попадание влаги, грязи, сыпучих веществ на устройства средств компьютерной и оргтехники;

• производить самостоятельно вскрытие и ремонт оборудования;

• работать со снятыми кожухами устройств компьютерной и оргтехники;

• располагаться при работе на расстоянии менее 50 см от экрана монитора.

• При работе с текстами на бумаге, листы надо располагать как можно ближе к экрану, чтобы избежать частых движений головой и глазами при переводе взгляда.

• Рабочие столы следует размещать таким образом, чтобы экран монитора был ориентирован боковой стороной к световым проемам, чтобы естественный свет падал преимущественно слева.

• Освещение не должно создавать бликов на поверхности экрана.

• Продолжительность работы на ПК без регламентированных перерывов не должна превышать 1-го часа. Во время регламентированного перерыва с целью снижения нервно-эмоционального напряжения, утомления зрительного аппарата, необходимо выполнять комплексы физических упражнений.

• При неисправности инструмента и оборудования – прекратить выполнение задания и сообщить об этом Эксперту, а в его отсутствие заместителю главного Эксперта.

1.2.4. Требования охраны труда в аварийных ситуациях

• При обнаружении неисправности в работе электрических устройств, находящихся под напряжением (повышенном их нагреве, появления искрения, запаха гари, задымления и т. д.), участнику следует немедленно сообщить о случившемся Экспертам. Выполнение задания продолжить только после устранения возникшей неисправности.

• В случае возникновения у участника плохого самочувствия или получения травмы сообщить об этом эксперту.

• При поражении участника электрическим током немедленно отключить электросеть, оказать первую помощь (самопомощь) пострадавшему, сообщить Эксперту, при необходимости обратиться к врачу.

• При несчастном случае или внезапном заболевании необходимо в первую очередь отключить питание электрооборудования, сообщить о случившемся Экспертам, которые должны принять мероприятия по оказанию первой помощи пострадавшим, вызвать скорую медицинскую помощь, при необходимости отправить пострадавшего в ближайшее лечебное учреждение.

• При возникновении пожара необходимо немедленно оповестить Главного эксперта и экспертов. При последующем развитии событий следует руководствоваться указаниями Главного эксперта или эксперта, заменяющего его. Приложить усилия для исключения состояния страха и паники.

• При обнаружении очага возгорания на площадке необходимо любым возможным способом постараться загасить пламя в "зародыше" с обязательным соблюдением мер личной безопасности.

• При возгорании одежды попытаться сбросить ее. Если это сделать не удается, упасть на пол и, перекатываясь, сбить пламя; необходимо накрыть горящую одежду куском плотной ткани, облиться водой, запрещается бежать – бег только усилит интенсивность горения.

• В загоревшемся помещении не следует дожидаться, пока приблизится пламя. Основная опасность пожара для человека – дым. При наступлении признаков удушья лечь на пол и как можно быстрее ползти в сторону эвакуационного выхода.

• При обнаружении взрывоопасного или подозрительного предмета не подходите близко к нему, предупредите о возможной опасности находящихся поблизости экспертов или обслуживающий персонал. • При происшествии взрыва необходимо спокойно уточнить обстановку и действовать по указанию экспертов, при необходимости эвакуации возьмите с собой документы и предметы первой необходимости, при передвижении соблюдайте осторожность, не трогайте поврежденные конструкции, оголившиеся электрические провода.

В разрушенном или поврежденном помещении не следует пользоваться открытым огнем (спичками, зажигалками и т. п.). 1.2.5. Требование охраны труда по окончании работ

• По окончании работы участник экзамена обязан соблюдать следующую последовательность отключения оборудования:

• произвести завершение всех выполняемых на ПК задач; • отключить питание в последовательности, установленной инструкцией по эксплуатации данного оборудования.

• Убрать со стола рабочие материалы и привести в порядок рабочее место. • Обо всех замеченных неполадках сообщить эксперту. • Сообщить эксперту о выявленных во время выполнения заданий неполадках и неисправностях оборудования, и других факторах, влияющих на безопасность выполнения задания.

1.3. Инструкция по охране труда для экспертов

1.3.1. Общие требования охраны труда

• К работе в качестве эксперта Компетенции «Корпоративная защита от внутренних угроз информационной безопасности» допускаются Эксперты, прошедшие специальное обучение и не имеющие противопоказаний по состоянию здоровья.

• Эксперт с особыми полномочиями, на которого возложена обязанность за проведение инструктажа по охране труда, должен иметь действующие удостоверение «О проверке знаний требований охраны труда».

• В процессе контроля выполнения заданий и нахождения на площадке Эксперт обязан четко соблюдать:

• инструкции по охране труда и технике безопасности;

• правила пожарной безопасности, знать места расположения первичных средств пожаротушения и планов эвакуации.

• расписание и график проведения задания, установленные режимы труда и отдыха.

• При работе на персональном компьютере и копировально множительной технике на Эксперта могут воздействовать следующие вредные и (или) опасные производственные факторы:

• электрический ток;

• статическое электричество, образующееся в результате трения движущейся бумаги с рабочими механизмами, а также при некачественном заземлении аппаратов;

• шум, обусловленный конструкцией оргтехники;

• химические вещества, выделяющиеся при работе оргтехники;

• зрительное перенапряжение при работе с ПК.

• При несчастном случае пострадавший или очевидец несчастного случая обязан немедленно сообщить о случившемся Главному Эксперту. В помещении Экспертов Компетенции «Корпоративная защита от внутренних угроз информационной безопасности» находится аптечка первой помощи, укомплектованная изделиями медицинского назначения, ее необходимо использовать для оказания первой помощи, самопомощи в случаях получения травмы. В случае возникновения несчастного случая или болезни Эксперта, об этом немедленно уведомляется Главный эксперт.

• Эксперты, допустившие невыполнение или нарушение инструкции по охране труда, привлекаются к ответственности в соответствии с Регламентом, а при необходимости согласно действующему законодательству.

1.3.2. Требования охраны труда перед началом работы

• Перед началом работы Эксперты должны выполнить следующее:

• В подготовительный день, Эксперт с особыми полномочиями, ответственный за охрану труда, обязан провести подробный инструктаж по «Программе инструктажа по охране труда и технике безопасности», ознакомить экспертов и участников с инструкцией по технике безопасности, с планами эвакуации при возникновении пожара, с местами расположения санитарно-бытовых помещений, медицинскими кабинетами, питьевой воды, проконтролировать подготовку рабочих мест участников в соответствии с Техническим описанием компетенции.

• Ежедневно, перед началом работ на площадке и в помещении экспертов необходимо:

• осмотреть рабочие места экспертов и участников;

• привести в порядок рабочее место эксперта;

• проверить правильность подключения оборудования в электросеть;

• Эксперту запрещается приступать к работе при обнаружении неисправности оборудования. О замеченных недостатках и неисправностях немедленно сообщить Техническому Эксперту и до устранения неполадок к работе не приступать.

1.3.3. Требования охраны труда во время работы

• Изображение на экранах видеомониторов должно быть стабильным, ясным и предельно четким, не иметь мерцаний символов и фона, на экранах не должно быть бликов и отражений светильников, окон и окружающих предметов.

• Суммарное время непосредственной работы с персональным компьютером и другой оргтехникой в течение дня должно быть не более 6 часов. Продолжительность непрерывной работы с персональным компьютером и другой оргтехникой без регламентированного

перерыва не должна превышать 2-х часов. Через каждый час работы следует делать регламентированный перерыв продолжительностью 15 мин.

• Во избежание поражения током запрещается:

• прикасаться к задней панели персонального компьютера и другой оргтехники, монитора при включенном питании;

• допускать попадания влаги на поверхность монитора, рабочую поверхность клавиатуры, дисководов, принтеров и других устройств;

• производить самостоятельно вскрытие и ремонт оборудования;

• переключать разъемы интерфейсных кабелей периферийных устройств при включенном питании;

• загромождать верхние панели устройств бумагами и посторонними предметами;

• допускать попадание влаги на поверхность системного блока, монитора, рабочую поверхность клавиатуры, дисководов, принтеров и др. устройств;

• При выполнении модулей задания участниками, Эксперту необходимо быть внимательным, не отвлекаться посторонними разговорами и делами без необходимости, не отвлекать других Экспертов и участников.

• Эксперту во время работы с оргтехникой:

• обращать внимание на символы, высвечивающиеся на панели оборудования, не игнорировать их;

• не снимать крышки и панели, жестко закрепленные на устройстве. В некоторых компонентах устройств используется высокое напряжение или лазерное излучение, что может привести к поражению электрическим током или вызвать слепоту;

• не производить включение/выключение аппаратов мокрыми руками;

• не ставить на устройство емкости с водой, не класть металлические предметы;

• не эксплуатировать аппарат, если он перегрелся, стал дымиться, появился посторонний запах или звук;

• не эксплуатировать аппарат, если его уронили или корпус был поврежден;

• вынимать застрявшие листы можно только после отключения устройства из сети;

• запрещается перемещать аппараты включенными в сеть;

• все работы по замене картриджей, бумаги можно производить только после отключения аппарата от сети;

• обязательно мыть руки теплой водой с мылом после каждой чистки картриджей, узлов и т. д.;

• просыпанный тонер, носитель немедленно собрать пылесосом или влажной ветошью.

• Включение и выключение персонального компьютера и оргтехники должно проводиться в соответствии с требованиями инструкции по эксплуатации.

• Запрещается:

• устанавливать неизвестные системы паролирования и самостоятельно проводить переформатирование диска;

• иметь при себе любые средства связи;

• пользоваться любой документацией кроме предусмотренной заданием. • При неисправности оборудования – прекратить работу и сообщить об этом Техническому эксперту, а в его отсутствие заместителю главного Эксперта.

• При нахождении на площадке Эксперту:

• одеть необходимые средства индивидуальной защиты;

• передвигаться по площадке не спеша, не делая резких движений, смотря под ноги.

1.3.4. Требования охраны труда в аварийных ситуациях

• При обнаружении неисправности в работе электрических устройств, находящихся под напряжением (повышенном их нагреве, появления искрения, запаха гари, задымления и т.д.), Эксперту следует немедленно отключить источник электропитания и принять меры к устранению неисправностей, а также сообщить о случившемся Техническому Эксперту. Выполнение задания продолжать только после устранения возникшей неисправности.

• В случае возникновения зрительного дискомфорта и других неблагоприятных субъективных ощущений следует ограничить время работы с персональным компьютером и другой оргтехникой, провести коррекцию длительности перерывов для отдыха или провести смену деятельности на другую, не связанную с использованием персонального компьютера и другой оргтехники.

• При поражении электрическим током немедленно отключить электросеть, оказать первую помощь (самопомощь) пострадавшему, сообщить Главному Эксперту, при необходимости обратиться к врачу.

• При возникновении пожара необходимо немедленно оповестить Главного эксперта. При последующем развитии событий следует руководствоваться указаниями Главного эксперта или должностного лица, 20 заменяющего его. Приложить усилия для исключения состояния страха и паники.

• При обнаружении очага возгорания на площадке необходимо любым возможным способом постараться загасить пламя в «зародыше» с обязательным соблюдением мер личной безопасности.

• При возгорании одежды попытаться сбросить ее. Если это сделать не удается, упасть на пол и, перекатываясь, сбить пламя; необходимо накрыть горящую одежду куском плотной ткани, облиться водой, запрещается бежать – бег только усилит интенсивность горения.

• В загоревшемся помещении не следует дожидаться, пока приблизится пламя. Основная опасность пожара для человека – дым. При наступлении признаков удушья лечь на пол и как можно быстрее ползти в сторону эвакуационного выхода.

• При обнаружении взрывоопасного или подозрительного предмета не подходить близко к нему, предупредить о возможной опасности находящихся поблизости ответственных лиц.

• При происшествии взрыва необходимо спокойно уточнить обстановку и действовать по указанию должностных лиц, при необходимости эвакуации, эвакуировать участников и других экспертов и площадки, взять те с собой документы и предметы первой необходимости, при передвижении соблюдать осторожность, не трогать поврежденные конструкции, оголившиеся электрические провода. В разрушенном или поврежденном помещении не следует пользоваться открытым огнем (спичками, зажигалками и т. п.).

1.3.5. Требование охраны труда по окончании выполнения работы

• После окончания дня Эксперт обязан:

• Отключить электрические приборы, оборудование, инструмент и устройства от источника питания.

• Привести в порядок рабочее место Эксперта и проверить рабочие места участников.

• Сообщить Техническому эксперту о выявленных во время выполнения заданий неполадках и неисправностях оборудования, и других факторах, влияющих на безопасность труда