

КОМИТЕТ ОБРАЗОВАНИЯ, НАУКИ И МОЛОДЕЖНОЙ ПОЛИТИКИ
ВОЛГОГРАДСКОЙ ОБЛАСТИ

государственное бюджетное профессиональное образовательное учреждение
«Волгоградский строительный техникум»
(ГБПОУ «Волгоградский строительный техникум»)

УТВЕРЖДАЮ

Директор ГБПОУ

«Волгоградский
строительный техникум»

Г.А. Голикова

31 марта 2022 г.



Основная профессиональная образовательная программа
подготовки специалистов среднего звена

Специальность

10.02.05 Обеспечение информационной безопасности автоматизированных
систем

уровень подготовки

базовый

квалификация

Техник по защите информации

форма обучения

очная

на базе основного общего образования

СОГЛАСОВАНО

ген. директор
ООО «Волга-Декор»

(должность,
наименование организации)

(личная подпись)

Зюбин В.И.

(расшифровка подписи)

«28» марта 2022 г.

(дата)

Директор ООО
«Волга-Декор»

(должность,
наименование организации)

(личная подпись)

Светличенкова Е.П.

(расшифровка подписи)

«29» марта 2022 г.

(дата)

Директор

(должность,
наименование организации)

(личная подпись)

Горюнова П.А.

(расшифровка подписи)

«29» марта 2022 г.

(дата)

Волгоград, 2022

Основная профессиональная образовательная программа подготовки специалистов среднего звена по специальности **10.02.05 Обеспечение информационной безопасности автоматизированных систем** разработана на основе федерального государственного образовательного стандарта среднего профессионального образования (ФГОС СПО) по специальности **10.02.05 Обеспечение информационной безопасности автоматизированных систем**, утвержденного приказом министерства образования и науки Российской Федерации от 9 декабря 2016 г. N 1553 (зарегистрированного в Минюсте РФ 26 декабря 2016 г., регистрационный N 44938), Положения об основной профессиональной образовательной программе, утвержденного директором ГБПОУ «Волгоградский строительный техникум» 30 августа 2019 г.

Организация-разработчик: государственное бюджетное профессиональное образовательное учреждение «Волгоградский строительный техникум» (ГБПОУ «Волгоградский строительный техникум»).

Разработчики:

Ломова М.Н. – заместитель директора по учебной работе ГБПОУ «Волгоградский строительный техникум».

Фарафонова Т.В. – заместитель директора по воспитательной работе ГБПОУ «Волгоградский строительный техникум».

Варжанцева Е.С. – методист ГБПОУ «Волгоградский строительный техникум».

Рекомендована педагогическим советом ГБПОУ «Волгоградский строительный техникум».

Протокол № 6 от 31 марта 2022 г.

СОДЕРЖАНИЕ

Раздел 1. Общие положения	4
Раздел 2. Общая характеристика образовательной программы.....	7
Раздел 3 Характеристика профессиональной деятельности	8
Раздел 4 Планируемые результаты освоения ППССЗ	9
4.1 Общие компетенции	9
4.2. Профессиональные компетенции	11
4.3. Личностные результаты	19
Раздел 5. Структура образовательной программы	21
5.1. Рабочий учебный план по программе подготовки специалистов среднего звена на базе основного общего образования (прилагается).....	21
5.2. Календарный учебный график по программе подготовки специалистов среднего звена (прилагается).....	21
5.3. Рабочая программа воспитания.....	21
5.4. Календарный план воспитательной работы (прилагается)	22
Раздел 6. Условия реализации образовательной программы	23
6.1. Требования к материально-техническому обеспечению образовательной программы	23
6.2. Требования к учебно-методическому обеспечению образовательной программы	26
6.3. Требования к организации воспитания обучающихся	27
6.4. Требования к кадровым условиям реализации образовательной программы.....	28
6.5. Требования к финансовым условиям реализации образовательной программы..	29
Раздел 7. Формирование фондов оценочных средств для проведения государственной итоговой аттестации.....	29
ПРИЛОЖЕНИЯ	
Приложение 1 Рабочий учебный план по программе подготовки специалистов среднего звена на базе основного общего образования	
Приложение 2 Календарный учебный график по программе подготовки специалистов среднего звена	
Приложение 3 Рабочая программа воспитания. Календарный график воспитательной работы	
Приложение 4 Рабочие программы профессиональных модулей	
Приложение 5 Рабочие программы учебных дисциплин	
Приложение 6 Рабочие программы общеобразовательных учебных дисциплин	
Приложение 7 Проект программы ГИА по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем	

Раздел 1. Общие положения

1.1. Основная образовательная программа среднего профессионального образования (далее – ООП СПО) по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем базовой подготовки, разработана на основе федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утвержденного приказом министерства образования и науки Российской Федерации от 9 декабря 2016 г. N 1553 (зарегистрированного в Минюсте РФ 26 декабря 2016 г., регистрационный N 44938), Положения об основной профессиональной образовательной программе, утвержденного директором ГБПОУ «Волгоградский строительный техникум» 30 августа 2019 г.

ООП СПО определяет объем и содержание среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, планируемые результаты освоения образовательной программы, условия образовательной деятельности.

ООП СПО разработана для реализации образовательной программы на базе основного общего образования

1.2. Нормативные основания для разработки ООП СПО:

– Федеральный закон от 29 декабря 2012 г. №273-ФЗ «Об образовании в Российской Федерации»;

– ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утвержденный приказом министерства образования и науки Российской Федерации от 9 декабря 2016 г. N 1553 (зарегистрированного в Минюсте РФ 26 декабря 2016 г., регистрационный N 44938);

– Приказ Минобрнауки России от 14 июня 2013 г. № 464 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам среднего профессионального образования»;

– Приказ Минпросвещения России от 28.08.2020 г. № 441 «О внесении изменений в Порядок организации и осуществления образовательной деятельности по образовательным программам среднего профессионального образования, утвержденный приказом Министерства образования и науки Российской Федерации от 14.06.2013 N 464;

– Приказ Минобрнауки России от 16 августа 2013 г. № 968 «Об утверждении Порядка проведения государственной итоговой аттестации по образовательным программам среднего профессионального образования»;

– Приказ Минобрнауки России № 885, Минпросвещения России № 390 от 5 августа 2020 г. «О практической подготовке обучающихся» (вместе с «Положением о практической подготовке обучающихся»);

- Приказ Министерства труда и социальной защиты Российской Федерации от 3 ноября 2016 г. № 608н «Об утверждении профессионального стандарта "Специалист по защите информации в телекоммуникационных системах и сетях" (зарегистрирован Министерством юстиции Российской Федерации 25 ноября 2016 г., регистрационный N 44449);

- Приказ Министерства труда и социальной защиты Российской Федерации от 1 ноября 2016 г. N 598н «Об утверждении профессионального стандарта "Специалист по безопасности компьютерных систем и сетей" (зарегистрирован Министерством юстиции Российской Федерации 28 ноября 2016 г., регистрационный N 44464);

- Приказ Министерства труда и социальной защиты Российской Федерации от 15 сентября 2016 г. N 522н «Об утверждении профессионального стандарта "Специалист по защите информации в автоматизированных системах" (зарегистрирован Министерством юстиции Российской Федерации 28 сентября 2016 г., регистрационный N 43857);

- Приказ Министерства труда и социальной защиты Российской Федерации от 1 ноября 2016 г. N 599н «Об утверждении профессионального стандарта "Специалист по технической защите информации" (зарегистрирован Министерством юстиции Российской Федерации 25 ноября 2016 г., регистрационный N 44443);

- Приказ Министерства труда и социальной защиты Российской Федерации от 29 декабря 2015 г. N 1179н «Об утверждении профессионального стандарта "Специалист по обнаружению, предупреждению и ликвидации последствий компьютерных атак" (зарегистрирован Министерством юстиции Российской Федерации 28 января 2016 г., N 40858);

- Приказ Министерства образования и науки РФ от 23 августа 2017 г. N 816 "Об утверждении Порядка применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ" (Зарегистрировано в Минюсте РФ 18 сентября 2017 г. Регистрационный N 48226);

- Приказ Минобрнауки России от 20.01.2014г. № 22 «Об утверждении перечней профессий и специальностей среднего профессионального образования, реализация образовательных программ по которым не допускается с применением исключительно электронного обучения, дистанционных образовательных технологий» (с изменениями и дополнениями от 10.12.2014);

– Письмо Министерства просвещения РФ от 19 марта 2020 г. № ГД-39/04 «О направлении методических рекомендаций по реализации образовательных программ начального общего, основного общего, среднего общего образования, образовательных программ среднего профессионального образования и дополнительных общеобразовательных программ с применением электронного обучения и дистанционных образовательных технологий»;

- Распоряжение Минпросвещения России от 01.04.2019 N P-42 (ред. от 01.04.2020) "Об утверждении методических рекомендаций о проведении аттестации с использованием механизма демонстрационного экзамена";

– Письмо Минпросвещения России от 08.04.2021 № 05-369 «О направлении рекомендаций" (вместе с "Рекомендациями, содержащие общие подходы к реализации образовательных программ среднего профессионального образования (отдельных их частей) в форме практической подготовки»);

– Приказ Комитета образования, науки и молодежной политики Волгоградской области №201 от 20.03.2020 «О введении временной реализации образовательных программ среднего профессионального образования с применением электронного обучения и дистанционных образовательных технологий в профессиональных образовательных организациях, расположенных на территории Волгоградской области»;

– Положение о порядке применения дистанционных образовательных технологий при реализации образовательных программ или их частей в ГБПОУ «Волгоградский строительный техникум», утвержденного приказом директора техникума от 20.03.2020 г. № 82-П».

– Устав государственного бюджетного профессионального образовательного учреждения «Волгоградский строительный техникум».

1.3. Согласно п.1.7 Федерального государственного образовательного стандарта СПО при реализации образовательной программы образовательная организация вправе применять электронное обучение и дистанционные образовательные технологии. При обучении инвалидов и лиц с ограниченными возможностями здоровья электронное обучение и дистанционные образовательные технологии предусматривает возможность приема-передачи информации в доступных для них формах.

1.4 Перечень сокращений, используемых в тексте ООП:

ФГОС СПО – Федеральный государственный образовательный стандарт среднего профессионального образования;

ПООП – примерная основная образовательная программа;

МДК – междисциплинарный курс;

ПМ – профессиональный модуль;

ОК – общие компетенции;

ПК – профессиональные компетенции;

ЛР – личностные результаты;

ГИА – государственная итоговая аттестация;

Цикл ОГСЭ – Общий гуманитарный и социально-экономический цикл

Цикл ЕН – Математический и общий естественнонаучный цикл

Раздел 2. Общая характеристика образовательной программы

Квалификация, присваиваемая выпускникам образовательной программы:
техник по защите информации.

Форма обучения: очная

Объем программы по освоению программы среднего профессионального образования на базе основного общего образования с одновременным получением среднего общего образования: 5940 академических часов, со сроком обучения 3 года 10 месяцев.

Раздел 3 Характеристика профессиональной деятельности

3.1 Область профессиональной деятельности, в которой выпускники, освоившие образовательную программу, могут осуществлять профессиональную деятельность: 06 Связь, информационные и коммуникационные технологии, 12 Обеспечение безопасности.

3.2 Соответствие профессиональных модулей присваиваемым квалификациям

Основные виды деятельности	Наименование профессиональных модулей осваиваемых в ППССЗ	Квалификация «Техник по защите информации»
Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	осваивается
Защита информации в автоматизированных системах программными и программно-аппаратными средствами	ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами	осваивается
Защита информации техническими средствами	ПМ.03 Защита информации техническими средствами	осваивается
Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих	ПМ.04 Выполнение работ по профессии 16199 Оператор электронно-вычислительных и вычислительных машин	осваивается

Раздел 4 Планируемые результаты освоения ППСЗ

Компетенции выпускника, формируемые в результате освоения ОПОП

4.1 Общие компетенции

Код компетенции	Формулировка компетенции	Знания, умения
ОК 01	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам	Умения: распознавать задачу и/или проблему в профессиональном и/или социальном контексте; анализировать задачу и/или проблему и выделять её составные части; определять этапы решения задачи; выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; составить план действия; определить необходимые ресурсы; владеть актуальными методами работы в профессиональной и смежных сферах; реализовать составленный план; оценивать результат и последствия своих действий (самостоятельно или с помощью наставника).
		Знания: актуальный профессиональный и социальный контекст, в котором приходится работать и жить; основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте. алгоритмы выполнения работ в профессиональной и смежных областях; методы работы в профессиональной и смежных сферах; структуру плана для решения задач; порядок оценки результатов решения задач профессиональной деятельности.
ОК 02	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности	Умения: определять задачи поиска информации; определять необходимые источники информации; планировать процесс поиска; структурировать получаемую информацию; выделять наиболее значимое в перечне информации; оценивать практическую значимость результатов поиска; оформлять результаты поиска.
		Знания номенклатура информационных источников применяемых в профессиональной деятельности; приемы структурирования информации; формат оформления результатов поиска информации
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие	Умения: определять актуальность нормативно-правовой документации в профессиональной деятельности; выстраивать траектории профессионального и личностного развития

		Знания: содержание актуальной нормативно-правовой документации; современная научная и профессиональная терминология; возможные траектории профессионального развития и самообразования
ОК 04	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами	Умения: организовывать работу коллектива и команды; взаимодействовать с коллегами, руководством, клиентами Знания: психология коллектива; психология личности; основы проектной деятельности
ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста	Умения: излагать свои мысли на государственном языке; оформлять документы. Знания: особенности социального и культурного контекста; правила оформления документов.
ОК 06	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей	Умения: описывать значимость своей профессии Презентовать структуру профессиональной деятельности по специальности Знания: сущность гражданско-патриотической позиции Общечеловеческие ценности Правила поведения в ходе выполнения профессиональной деятельности
ОК 07	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях	Умения: соблюдать нормы экологической безопасности; определять направления ресурсосбережения в рамках профессиональной деятельности по специальности. Знания: правила экологической безопасности при ведении профессиональной деятельности; основные ресурсы, задействованные в профессиональной деятельности; пути обеспечения ресурсосбережения.
ОК 08	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности	Умения: использовать физкультурно-оздоровительную деятельность для укрепления здоровья, достижения жизненных и профессиональных целей; применять рациональные приемы двигательных функций в профессиональной деятельности; пользоваться средствами профилактики перенапряжения характерными для данной специальности

		<p>Знания: роль физической культуры в общекультурном, профессиональном и социальном развитии человека; основы здорового образа жизни; условия профессиональной деятельности и зоны риска физического здоровья для специальности; средства профилактики перенапряжения.</p>
ОК 09	Использовать информационные технологии в профессиональной деятельности	<p>Умения: применять средства информационных технологий для решения профессиональных задач; использовать современное программное обеспечение</p> <p>Знания: современные средства и устройства информатизации; порядок их применения и программное обеспечение в профессиональной деятельности.</p>
ОК 10	Пользоваться профессиональной документацией на государственном и иностранном языках	<p>Умения: понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы; участвовать в диалогах на знакомые общие и профессиональные темы; строить простые высказывания о себе и о своей профессиональной деятельности; кратко обосновывать и объяснить свои действия (текущие и планируемые); писать простые связные сообщения на знакомые или интересующие профессиональные темы</p> <p>Знания: правила построения простых и сложных предложений на профессиональные темы; основные общеупотребительные глаголы (бытовая и профессиональная лексика); лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности; особенности произношения; правила чтения текстов профессиональной направленности</p>

4.2. Профессиональные компетенции

Основные виды деятельности	Код и наименование компетенции	Показатели освоения компетенции
Эксплуатация автоматизированных (информационных)	ПК 1.1. Производить установку и настройку компонентов автоматизированных	Практический опыт: установка и настройка компонентов систем защиты информации автоматизированных (информационных) систем

систем защищенном исполнении	в	(информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации	Умения: осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении и компонент систем защиты информации автоматизированных систем
			Знания: состав и принципы работы автоматизированных систем, операционных систем и сред; принципы разработки алгоритмов программ, основных приемов программирования; модели баз данных; принципы построения, физические основы работы периферийных устройств
			Практический опыт: администрирование автоматизированных систем в защищенном исполнении
		ПК 1.2. Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении	Умения: организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней; осуществлять конфигурирование, настройку компонент систем защиты информации автоматизированных систем; производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы
		ПК 1.3. Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации	Практический опыт: эксплуатация компонентов систем защиты информации автоматизированных систем Умения: настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам Знания: порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях
		ПК 1.4. Осуществлять	Практический опыт: диагностика

	<p>проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении</p>	<p>компонентов систем защиты информации автоматизированных систем, устранение отказов и восстановление работоспособности автоматизированных (информационных) систем в защищенном исполнении</p> <p>Умения: обеспечивать работоспособность, обнаруживать и устранять неисправности</p> <p>Знания: принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации</p>
<p>Защита информации в автоматизированных системах программными и программно-аппаратными средствами</p>	<p>ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации</p> <p>ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.</p>	<p>Практический опыт: установка, настройка программных средств защиты информации в автоматизированной системе</p> <p>Умения: устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;</p> <p>Знания: особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных</p> <p>Практический опыт: обеспечение защиты автономных автоматизированных систем программными и программно-аппаратными средствами; использование программных и программно-аппаратных средств для защиты информации в сети</p> <p>Умения: устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями; устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;</p> <p>Знания: особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных</p>

	<p>ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации</p>	<p>Практический опыт: тестирование функций, диагностика, устранение отказов и восстановление работоспособности программных и программно-аппаратных средств защиты информации</p>
		<p>Умения: диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации;</p>
		<p>Знания: методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации</p>
	<p>ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа</p>	<p>Практический опыт: решение задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации; применение электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных</p>
		<p>Умения: применять программные и программно-аппаратные средства для защиты информации в базах данных; проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации; применять математический аппарат для выполнения криптографических преобразований; использовать типовые программные криптографические средства, в том числе электронную подпись</p>
		<p>Знания: особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных; типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации; основные понятия криптографии и типовых криптографических методов и средств защиты информации</p>

	<p>ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств</p>	<p>Практический опыт: учёт, обработка, хранение и передача информации, для которой установлен режим конфиденциальности</p> <p>Умения: применять средства гарантированного уничтожения информации</p> <p>Знания: особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации</p>
	<p>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</p>	<p>Практический опыт: работа с подсистемами регистрации событий; выявление событий и инцидентов безопасности в автоматизированной системе</p> <p>Умения: устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак</p> <p>Знания: типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа</p>
<p>Защита информации техническими средствами</p>	<p>ПК 3.1. Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации</p>	<p>Практический опыт: установка, монтаж и настройка технических средств защиты информации; техническое обслуживание технических средств защиты информации; применение основных типов технических средств защиты информации</p> <p>Умения: применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных</p> <p>Знания: порядок технического обслуживания технических средств защиты информации;</p>

		номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам
ПК 3.2. Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации	Практический опыт:	применение основных типов технических средств защиты информации; выявление технических каналов утечки информации; участие в мониторинге эффективности технических средств защиты информации; диагностика, устранение отказов и неисправностей, восстановление работоспособности технических средств защиты информации
	Умения:	применять технические средства для криптографической защиты информации конфиденциального характера; применять технические средства для уничтожения информации и носителей информации; применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами
	Знания:	физические основы, структуру и условия формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации; порядок устранения неисправностей технических средств защиты информации и организации ремонта технических средств защиты информации; методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации; номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам
ПК 3.3. Осуществлять	Практический опыт:	проведение

измерение параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа	измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов информатизации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации
	Умения: применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных
	Знания: номенклатуру и характеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации; структуру и условия формирования технических каналов утечки информации;
ПК 3.4. Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации	Практический опыт: проведение измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации; выявление технических каналов утечки информации
	Умения: применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных
	Знания: номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам
ПК 3.5. Организовывать отдельные работы по физической защите объектов информатизации	Практический опыт: установка, монтаж и настройка, техническое обслуживание, диагностика, устранение отказов и неисправностей, восстановление работоспособности инженерно-технических средств физической защиты
	Умения: применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом; применять инженерно-технические средства физической защиты объектов информатизации

		<p>Знания: основные принципы действия и характеристики технических средств физической защиты;</p> <p>основные способы физической защиты объектов информатизации;</p> <p>номенклатуру применяемых средств физической защиты объектов информатизации</p>
<p>ПМ.04 Выполнение работ по профессии 16199 Оператор электронно-вычислительных и вычислительных машин</p>	<p>ПК 4.1. Участвовать в разработке проектной документации компьютерных систем и комплексов с использованием современных пакетов прикладных программ в сфере профессиональной деятельности</p>	<p>Знания: профессионально важные качества и профессиональную характеристику оператора ЭВМ;</p> <p>- нормативные документы по установке, эксплуатации и охране труда при работе с компьютером, периферийным оборудованием и компьютерной оргтехникой;</p> <p>- состав мероприятий по защите персональных данных.</p> <p>Умения: создавать и редактировать графические объекты с помощью программ для обработки растровой и векторной графики, объекты мультимедиа;</p>
	<p>ПК 4.2. Участвовать в проектировании, монтаже, эксплуатации и диагностике компьютерных систем и комплексов</p>	<p>Знания: виды, назначение периферийных устройств, их принцип действия, интерфейсы подключения и правила эксплуатации;</p> <p>- порядок установки и настройки прикладного программного обеспечения;</p> <p>Умения: подключать, производить установку, использовать периферийные устройства и оргтехнику и диагностировать простейшие неисправности персонального компьютера;</p>
	<p>ПК 4.3. Проводить мероприятия по защите информации в компьютерных системах и комплексах</p>	<p>Знания: состав мероприятий по защите персональных данных.</p> <p>Умения: осуществлять мероприятия по защите персональных данных.</p>
	<p>ПК 4.4. Создавать и управлять на персональном компьютере текстовыми документами, таблицами, презентациями и содержанием баз данных</p>	<p>Знания: назначение, разновидности и функциональные возможности редакторов текстов, таблиц, презентаций, систем управления базами данных, программ обработки растровой и векторной графики, программ для создания объектов мультимедиа, Веб-страниц;</p> <p>Умения:- создавать и управлять содержимым документов с помощью редактора документов, таблиц, презентаций, HTML-редакторов;</p>
	<p>ПК 4.5. Осуществлять навигацию по ресурсам, поиск, ввод и передачу данных с</p>	<p>Знания: виды и характеристики носителей информации, файловые системы, форматы представления данных;</p> <p>- принципы функционирования локальных и</p>

	помощью технологий и сервисов Интернета	глобальных сетей; Умения: управлять файлами данных на локальных, съемных запоминающих устройствах, а также на дисках локальной компьютерной сети и в интернете;
	ПК 4.6. Создавать и обрабатывать цифровые изображения и объекты мультимедиа	Умения: выполнять настройку интерфейса ОС; - набирать алфавитно-цифровую информацию на клавиатуре пальцевым методом;
	ПК 4.7. Обеспечивать меры по информационной безопасности	Знания: состав мероприятий по защите персональных данных. Умения: осуществлять мероприятия по защите персональных данных.

4.3. Личностные результаты

Личностные результаты реализации программы воспитания (дескрипторы)	Код личностных результатов реализации программы воспитания
Осознающий себя гражданином и защитником великой страны.	ЛР 1
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 2
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 3
Проявляющий и демонстрирующий уважение к людям труда, осознающий ценность собственного труда. Стремящийся к формированию в сетевой среде лично и профессионального конструктивного «цифрового следа».	ЛР 4
Демонстрирующий приверженность к родной культуре, исторической памяти на основе любви к Родине, родному народу, малой родине, принятию традиционных ценностей многонационального народа России.	ЛР 5
Проявляющий уважение к людям старшего поколения и готовность к участию в социальной поддержке и волонтерских движениях.	ЛР 6
Осознающий приоритетную ценность личности человека; уважающий собственную и чужую уникальность в различных ситуациях, во всех формах и видах деятельности.	ЛР 7
Проявляющий и демонстрирующий уважение к представителям различных этнокультурных, социальных, конфессиональных и иных	ЛР 8

групп. Сопричастный к сохранению, преумножению и трансляции культурных традиций и ценностей многонационального российского государства.	
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 9
Заботящийся о защите окружающей среды, собственной и чужой безопасности, в том числе цифровой.	ЛР 10
Проявляющий уважение к эстетическим ценностям, обладающий основами эстетической культуры.	ЛР 11
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 12
Личностные результаты реализации программы воспитания, определенные отраслевыми требованиями к деловым качествам личности	
Соблюдающий в своей профессиональной деятельности этические принципы: честности, независимости, профессионального скептицизма, противодействия коррупции и экстремизму, обладающий системным мышлением и умением принимать решение в условиях риска и неопределенности	ЛР 13
Готовый соответствовать ожиданиям работодателей: проектно-мыслящий, эффективно взаимодействующий с членами команды и сотрудничающий с другими людьми, осознанно выполняющий профессиональные требования, ответственный, пунктуальный, дисциплинированный, трудолюбивый, критически мыслящий, нацеленный на достижение поставленных целей; демонстрирующий профессиональную жизнестойкость	ЛР 14
Открытый к текущим и перспективным изменениям в мире труда и профессий	ЛР 15
Личностные результаты реализации программы воспитания, определенные субъектом Российской Федерации¹ (при наличии)	
Осознающий культурное наследие Волгоградской области, готовый его сохранять, поддерживать и развивать для формирования положительного имиджа региона	ЛР 16
Жизнестойкий и адаптивный человек, готовый осуществлять свою профессиональную деятельность в интересах Волгоградской области вне зависимости от глобальной неопределенности и стремительных изменений в общественной жизни	ЛР 17
Личностные результаты реализации программы воспитания, определенные ключевыми работодателями² (при наличии)	

¹ Разрабатывается органами исполнительной власти субъекта Российской Федерации, переносится из Программы воспитания субъекта Российской Федерации. Заполняется при разработке рабочей программы воспитания профессиональной образовательной организации.

² Заполняется при разработке рабочей программы воспитания профессиональной образовательной организации.

Гармонично, разносторонне развитый, активно выражающий отношение к преобразованию общественных пространств, промышленной и технологической эстетике предприятия, корпоративному дизайну, товарным знакам	ЛР 18
Способный в цифровой среде искать нужные источники информации и данные, воспринимать, анализировать, запоминать и передавать информацию используя различные цифровые средства, позволяющие во взаимодействии с другими людьми достигать поставленных целей	ЛР19
Личностные результаты реализации программы воспитания, определенные субъектами образовательного процесса³ (при наличии)	
Принимающий роль наставляемого, который через взаимодействие с наставником и при его помощи и поддержке решает конкретные жизненные, личные и профессиональные задачи, приобретая новый опыт и развивая новые навыки и компетенции, а так же выступающий в роли наставника, имеющего успешный опыт в достижении жизненного, личного и профессионального результата, готового и компетентного поделиться опытом и навыками, необходимыми для стимуляции и поддержки процессов самореализации и самосовершенствования наставляемого	ЛР 20
Гордящийся прошлым, ценящий настоящее и смотрящий в будущее заботясь о ветеранах, помогающий в благоустройстве памятных мест, восстанавливающий историю семьи, популяризирующий современные достижения России с помощью интересных форматов и не дающий жителям всего мира забыть правдивую историю Победы	ЛР 21
Активный гражданин, чувствующий ответственность за свои действия и поступки, инициативный и самостоятельный, реализующий социально значимые проекты, умеющий находить пути решения проблем общества, окружающей среды.	ЛР 22

Раздел 5. Структура образовательной программы

5.1. Учебный план по программе подготовки специалистов среднего звена на базе основного общего образования (Приложение 3)

5.2. Календарный учебный график по программе подготовки специалистов среднего звена на базе основного общего образования (Приложение 3)

5.3. Рабочая программа воспитания

5.3.1. Цели и задачи воспитания обучающихся при освоении ими образовательной программы:

Цель рабочей программы воспитания – личностное развитие обучающихся и их социализация, проявляющиеся в развитии их позитивных отношений к общественным ценностям, приобретении опыта поведения и применения сформированных общих компетенций квалифицированных рабочих, служащих/специалистов среднего звена на практике.

Задачи:

³ Разрабатывается ПОО совместно с работодателями, родителями, педагогами и обучающимися. Заполняется при разработке рабочей программы воспитания профессиональной образовательной организации.

- формирование единого воспитательного пространства, создающего равные условия для развития обучающихся профессиональной образовательной организации;
- организация всех видов деятельности, вовлекающей обучающихся в общественно-ценностные социализирующие отношения;
- формирование у обучающихся профессиональной образовательной организации общих ценностей, моральных и нравственных ориентиров, необходимых для устойчивого развития государства;
- усиление воспитательного воздействия благодаря непрерывности процесса воспитания.

5.3.2. Рабочая программа воспитания (Приложение 3)

5.4. Календарный план воспитательной работы (Приложение 3)

Раздел 6. Условия реализации образовательной программы

6.1. Требования к материально-техническому обеспечению образовательной программы

6.1.1. Специальные помещения представляют собой учебные аудитории для проведения занятий всех видов, предусмотренных образовательной программой, в том числе групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы, мастерские и лаборатории, оснащенные оборудованием, техническими средствами обучения и материалами, учитывающими требования международных стандартов.

Перечень специальных помещений

Учебные аудитории:

социально-экономических дисциплин;
иностранного языка;
математики;
нормативного правового обеспечения информационной безопасности;
информатики;
компьютерный класс;
безопасности жизнедеятельности;
методический.

Лаборатории:

электроники и схемотехники;
информационных технологий, программирования и баз данных;
сетей и систем передачи информации;
программных и программно-аппаратных средств защиты информации;
технических средств защиты информации.

Мастерские:

Лаборатория технических средств информатизации, или лаборатория информационных технологий и/или мастерская по наладке технологического оборудования по профилю выбираемой рабочей профессии.

Спортивный комплекс

Спортивный зал

Открытый стадион широкого профиля с элементами полосы препятствий

Стрелковый тир

Залы:

- библиотека,
- читальный зал с выходом в интернет;
- актовый зал;
- и др.

6.1.2. Материально-техническое оснащение лабораторий, мастерских и баз практики по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем

Образовательная организация, реализующая программу по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, располагает материально-технической базой, обеспечивающей проведение всех видов дисциплинарной и междисциплинарной подготовки, лабораторной, практической работы обучающихся, предусмотренных учебным планом, и соответствующей действующим санитарным и противопожарным правилам и нормам в разрезе выбранных траекторий. Минимально необходимый для реализации ООП перечень материально-технического обеспечения, включает в себя:

6.1.2.1. Оснащение лабораторий

Лаборатория «Электроники и схемотехники»:

- учебно-лабораторные стенды для освоения типовых схемотехнических решений;
- контрольно-измерительная аппаратура для измерения временных характеристик, амплитуды и формы сигналов (амперметр, вольтметр, осциллограф);
- генераторы сигналов с заданными параметрами;
- Logisim- бесплатная программа для создания и имитации логических схем, Multisim –конструктор электрических схем;
- EasyEDA – онлайн сервис для моделирования радиосхем.

Лаборатория «Информационных технологий, программирования и баз данных»:

- 12 рабочих мест на базе вычислительной техники, подключенных к локальной вычислительной сети и сети «Интернет» - 12;
- мультимедийное оборудование;
- программное обеспечение СУБД: Microsoft SQL, MySQL, Виртуальная машина: Oracle VM VirtualBox, Hyper-V

Лаборатория «Сетей и систем передачи информации»:

- рабочие места на базе вычислительной техники, подключенные к локальной вычислительной сети и информационно-телекоммуникационной сети Интернет;
- стенды сетей передачи данных;
- программное обеспечение сетевого оборудования Программный IP/MPLS-маршрутизатор EcoRouterOS.

Лаборатория «Программных и программно-аппаратных средств защиты информации»:

- рабочие места на базе вычислительной техники, подключенные к локальной вычислительной сети и информационно-телекоммуникационной сети Интернет;
- антивирусный программный комплекс;
- программно-аппаратные средства защиты информации от несанкционированного доступа (Secret Net Studio, ViPNet Client),
- Виртуальная машина: Oracle VM VirtualBox , встроенный Hyper-V
- программные средства криптозащиты информации КриптоПро CSP, VipNET CSP;
- DLP Traffic Monitor (система с широким спектром возможностей для защиты, анализа и контроля чувствительных данных организации).

Лаборатория «Технических средств защиты информации»:

- рабочие места обучающихся, оборудованные персональными компьютерами;
- лабораторные учебные макеты;
- аппаратные средства аутентификации пользователя (Рутокен KeyBox);
- стенд физической защиты объектов информатизации, оснащенными средствами контроля доступа, системами видеонаблюдения и охраны объектов;
- рабочее место преподавателя;
- учебно-методическое обеспечение модуля;
- интерактивная доска, комплект презентаций.

6.1.2.2. Оснащение мастерских:

Мастерская по наладке технологического оборудования по профилю выбираемой рабочей профессии.

Оборудование определяется образовательной организацией и соответствует профилю выбираемой рабочей профессии.

6.1.2.3. Оснащение баз практик

Реализация образовательной программы предполагает обязательную учебную и производственную практику.

Учебная практика проводится в кабинетах, лабораториях и учебно-производственных мастерских техникума.

Производственная практика реализуется в организациях: УФПС Волгоградской области – Филиал ФГПУ «Почта России», АО «Корпорация Красный Октябрь», направление деятельности которых соответствует профилю подготовки обучающихся

Оборудование организаций и технологическое оснащение рабочих мест производственной практики соответствует содержанию профессиональной деятельности и дает возможность обучающемуся овладеть профессиональными компетенциями по всем видам деятельности, предусмотренных программой, с использованием современных технологий, материалов и оборудования.

6.2. Требования к учебно-методическому обеспечению образовательной программы

6.2.1. Библиотечный фонд образовательной организации укомплектован печатными изданиями и (или) электронными изданиями по каждой дисциплине (модулю) из расчета не менее 0,25 экземпляра каждого из изданий, указанных в рабочих программах дисциплин (модулей) в качестве основной литературы, на одного обучающегося из числа лиц, одновременно осваивающих соответствующую дисциплину (модуль).

Техникум использует образовательную платформу «Юрайт» что позволяет заменить печатный библиотечный фонд предоставлением права одновременного доступа не менее 25 процентов обучающихся к электронной библиотечной системе образовательной платформы «Юрайт».

Обучающимся обеспечен доступ (удаленный доступ), в том числе в случае применения электронного обучения, дистанционных образовательных технологий, к современным профессиональным базам данных и информационным справочным системам, состав которых определяется в рабочих программах дисциплин (модулей) и подлежит обновлению (при необходимости).

Образовательная программа обеспечена учебно-методической документацией по всем учебным дисциплинам (модулям).

6.2.2. Обучающиеся инвалиды и лица с ограниченными возможностями здоровья обеспечиваются печатными и (или) электронными учебными изданиями, адаптированными при необходимости для обучения указанных обучающихся.

6.2.3. При реализации программы дисциплины с применением электронного обучения (далее - ЭО) и дистанционных образовательных технологий (далее – ДОТ) используется образовательная платформа «Сферум» и облачные технологии, доступные по адресу: VST34DZ@mail.ru.

Обучение по программе дисциплины с применением ЭО и ДОТ осуществляется на основе цифровых образовательных ресурсов:

- электронные учебники;
- образовательной платформы «Сферум»;
- облачная технология ВСТ;
- образовательная платформа Юрайт;
- интерактивные обучающие ресурсы;
- виртуальные среды учебно-практической деятельности;
- компьютерные демонстрации;
- электронные источники информации;
- электронно-библиотечная система «Юрайт»;
- электронные периодические издания;

- электронные коллекции.

Ресурсы, сопровождающие предметные дистанционные курсы:

- онлайн-поддержка обучения;
- тестирование on-line;
- конкурсы, консультации on-line;
- предоставление методических материалов;
- сопровождение off-line (проверка тестов, контрольных, различные виды аттестации).

Учебно-методические материалы для обучающихся также передаются посредством использования:

- систем обмена сообщениями (письмами) между абонентами компьютерных сетей — электронной почтой, включая использование VK-мессенджер;

При реализации образовательной программы или ее части с применением ЭО, ДОТ техникум оказывает учебно-методическую помощь обучающимся, в том числе в форме дистанционных индивидуальных консультаций, с использованием информационных и телекоммуникационных технологий.

Учебно-методические материалы для обучающихся также передаются посредством использования:

- систем обмена сообщениями (письмами) между абонентами компьютерных сетей — электронной почтой, вкл. использование облачных хранилищ данных;
- систем обмена мгновенными сообщениями между пользователями на компьютере или смартфоне/планшете — мессенджеры (Discord, Skype, WhatsApp, Viber и т.д.); – социальных сетей (Вконтакте).

При реализации образовательной программы или ее части с применением ЭО, ДОТ техникум оказывает учебно-методическую помощь обучающимся, в том числе в форме дистанционных индивидуальных консультаций, с использованием информационных и телекоммуникационных технологий.

6.3. Требования к организации воспитания обучающихся

6.3.1. Условия организации воспитания определяются образовательной организацией.

Выбор форм организации воспитательной работы основывается на анализе эффективности и практическом опыте.

Для реализации Программы определены следующие формы воспитательной работы с обучающимися:

- информационно-просветительские занятия (лекции, встречи, совещания, собрания и т.д.)
- массовые и социокультурные мероприятия;
- спортивно-массовые и оздоровительные мероприятия;

- деятельность творческих объединений, студенческих организаций;
- психолого-педагогические тренинги и индивидуальные консультации;
- научно-практические мероприятия (конференции, форумы, олимпиады, чемпионаты и др.);
- профориентационные мероприятия (конкурсы, фестивали, мастер-классы, квесты, экскурсии и др.);
- опросы, анкетирование, социологические исследования среди обучающихся.

6.4. Требования к кадровым условиям реализации образовательной программы

6.4.1. Реализация образовательной программы обеспечивается педагогическими работниками образовательной организации, а также лицами, привлекаемыми к реализации образовательной программы на условиях гражданско-правового договора, в том числе из числа руководителей и работников организаций, направление деятельности которых соответствует области профессиональной деятельности 06 Связь, информационные и коммуникационные технологии, 12 Обеспечение безопасности, и имеющих стаж работы в данной профессиональной области не менее 3 лет.

Квалификация педагогических работников образовательной организации отвечает квалификационным требованиям, указанным в Едином квалификационном справочнике должностей руководителей, специалистов и служащих (далее - ЕКС), а также профессиональном стандарте «Педагог профессионального обучения, профессионального образования и дополнительного профессионального образования», утвержденном приказом Министерства труда и социальной защиты Российской Федерации от 8 сентября 2015 г. № 608н.

Педагогические работники, привлекаемые к реализации образовательной программы, получают дополнительное профессиональное образование по программам повышения квалификации, в том числе в форме стажировки в организациях, направление деятельности которых соответствует области профессиональной деятельности 06 Связь, информационные и коммуникационные технологии, 12 Обеспечение безопасности, не реже 1 раза в 3 года с учетом расширения спектра профессиональных компетенций.

Доля педагогических работников (в приведенных к целочисленным значениям ставок), обеспечивающих освоение обучающимися профессиональных модулей, имеющих опыт деятельности не менее 3 лет в организациях, направление деятельности которых соответствует области профессиональной деятельности 06 Связь, информационные и коммуникационные технологии, 12 Обеспечение безопасности, в общем числе педагогических работников, реализующих образовательную программу, составляет не менее 25 процентов.

6.5. Требования к финансовым условиям реализации образовательной программы

6.5.1. Примерные расчеты нормативных затрат оказания государственных услуг по реализации образовательной программы⁴

Расчеты нормативных затрат оказания государственных услуг по реализации образовательной программы осуществляются в соответствии с Методикой определения нормативных затрат на оказание государственных услуг по реализации образовательных программ среднего профессионального образования по профессиям (специальностям) и укрупненным группам профессий (специальностей), утвержденной Минобрнауки России 27 ноября 2015 г. № АП-114/18вн.

Нормативные затраты на оказание государственных услуг в сфере образования по реализации образовательной программы включают в себя затраты на оплату труда преподавателей и мастеров производственного обучения с учетом обеспечения уровня средней заработной платы педагогических работников за выполняемую ими учебную (преподавательскую) работу и другую работу в соответствии с Указом Президента Российской Федерации от 7 мая 2012 г. № 597 «О мероприятиях по реализации государственной социальной политики».

Раздел 7. Формирование фондов оценочных средств для проведения государственной итоговой аттестации

7.1. Государственная итоговая аттестация (далее – ГИА) является обязательной для образовательных организаций СПО. Она проводится по завершении всего курса обучения по направлению подготовки. В ходе ГИА оценивается степень соответствия сформированных компетенций выпускников требованиям ФГОС.

ГИА проходит в форме защиты ВКР в виде дипломного проекта и демонстрационного экзамена.

7.2. Выпускники, освоившие программы подготовки специалистов среднего звена, выполняют выпускную квалификационную работу (дипломный проект) и сдают демонстрационный экзамен.

7.3. Для государственной итоговой аттестации цикловой методической комиссией общих математических и естественнонаучных дисциплин (ЕН) совместно с заместителем директора по учебной работе разработана программа государственной итоговой аттестации и фонды оценочных средств.

7.4. Задания для демонстрационного экзамена разработаны на основе профессиональных стандартов и с учетом оценочных материалов, разработанных АНО «Агентство развития профессиональных сообществ и рабочих кадров «Молодые профессионалы (Ворлдскиллс Россия)», при условии наличия соответствующих профессиональных стандартов и материалов.

⁴ Образовательная организация приводит расчетную величину стоимости услуги в соответствии с рекомендациями федеральных и региональных нормативных документов.

7.5. Фонды оценочных средств для проведения ГИА включают типовые задания для демонстрационного экзамена, примерные темы дипломных проектов, описание процедур и условий проведения государственной итоговой аттестации, критерии оценки (Приложение 7).

ПРИЛОЖЕНИЕ 1

Учебный план по программе подготовки специалистов среднего звена на базе основного общего образования

<https://r1.nubex.ru/s138456->

[053/f3751_73/%D0%A3%D1%87%D0%B5%D0%B1%D0%BD%D1%8B%D0%B9%20%D0%BF%D0%BB%D0%B0%D0%BD%2010.02.05%20%D0%9E%D0%98%D0%91%209%20%D0%BA%D0%BB.%202022.pdf](https://r1.nubex.ru/s138456-053/f3751_73/%D0%A3%D1%87%D0%B5%D0%B1%D0%BD%D1%8B%D0%B9%20%D0%BF%D0%BB%D0%B0%D0%BD%2010.02.05%20%D0%9E%D0%98%D0%91%209%20%D0%BA%D0%BB.%202022.pdf)

Комитет образования, науки и молодежной политики Волгоградской области

Утверждаю

Директор

Голикова Галина Артуровна



31.03.2022

Рассмотрено на заседании учебно-методического совета.

Протокол № 8 от 30.03.2022

УЧЕБНЫЙ ПЛАН

программы подготовки специалистов среднего звена

государственное бюджетное профессиональное образовательное учреждение «Волгоградский строительный техникум»

наименование образовательного учреждения (организации)

по специальности среднего профессионального образования

10.02.05

Обеспечение информационной безопасности автоматизированных систем

код

наименование специальности

по программе базовой подготовки

основное общее образование

Уровень образования, необходимый для приема на обучение

квалификация:

техник по защите информации

форма обучения

Очная

Нормативный срок освоения ОПОП

3г 10м

год начала подготовки по УП 2022

профиль получаемого профессионального образования

технический

при реализации программы среднего общего образования

Приказ об утверждении ФГОС

от 09.12.2016 № 1553

Виды деятельности
Эксплуатация автоматизированных (информационных) систем в защищенном исполнении
Защита информации в автоматизированных системах программными и программно-аппаратными средствами
Защита информации техническими средствами
Выполнение работ по профессии 16199 Оператор электронно-вычислительных и вычислительных машин

ПРИЛОЖЕНИЕ 3**Рабочая программа воспитания. Календарный план воспитательной работы**

https://r1.nubex.ru/s138456-053/f6416_e5/Рабочая%20программа%20воспитания%202022%20год.pdf

<https://r1.nubex.ru/s138456->

[053/f4012_b3/Календарный%20план%20воспитательной%20работы%2010.02.05%20ОИБ%209%20на%202022-2023г.pdf](https://r1.nubex.ru/s138456-053/f4012_b3/Календарный%20план%20воспитательной%20работы%2010.02.05%20ОИБ%209%20на%202022-2023г.pdf)

ПРИЛОЖЕНИЕ 4

Рабочие программы профессиональных модулей

<https://cloud.mail.ru/public/B3s5/1S7ywnzTT> - ПМ

Рабочие программы учебных дисциплин

<https://cloud.mail.ru/public/2NjS/EzuUi1jhG> - ОГСЭ

<https://cloud.mail.ru/public/XzDr/YY1MPmewH> - ЕН

<https://cloud.mail.ru/public/BRmb/s4PSG87uJ> - ОП

ПРИЛОЖЕНИЕ 6

Рабочие программы общеобразовательных учебных дисциплин

<https://cloud.mail.ru/public/7Bq9/wQDqstX1X>

ПРИЛОЖЕНИЕ 7

**ПРОЕКТ ПРОГРАММЫ ГИА ПО СПЕЦИАЛЬНОСТИ 10.02.05 ОБЕСПЕЧЕНИЕ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ
СИСТЕМ**

КОМИТЕТ ОБРАЗОВАНИЯ, НАУКИ И МОЛОДЕЖНОЙ ПОЛИТИКИ
ВОЛГОГРАДСКОЙ ОБЛАСТИ

государственное бюджетное профессиональное образовательное учреждение
«Волгоградский строительный техникум»
(ГБПОУ «Волгоградский строительный техникум»)

УТВЕРЖДАЮ

Директор ГБПОУ «Волгоградский
строительный техникум»

_____ Г.А. Голикова
«__» _____ 202__ г.

**Программа
государственной итоговой аттестации
обучающихся по специальности
10.02.05 Обеспечение информационной безопасности
автоматизированных систем
на 202__ год**

СОГЛАСОВАНО

_____ «__» _____ 20__ г.
(должность, (личная подпись) (расшифровка подписи) (дата)
наименование организации)

_____ «__» _____ 20__ г.
(должность, (личная подпись) (расшифровка подписи) (дата)
наименование организации)

_____ «__» _____ 20__ г.
(должность, (личная подпись) (расшифровка подписи) (дата)
наименование организации)

_____ «__» _____ 20__ г.
(должность, (личная подпись) (расшифровка подписи) (дата)
наименование организации)

Волгоград, 202__

СОГЛАСОВАНО

Зам. директора по учебной работе

_____ М.Н. Ломова
« ____ » _____ 202_ г.

РАССМОТРЕНО

Протокол заседания педагогического совета ГБПОУ «Волгоградский строительный техникум» № __ от «__» _____ 202_ г.

РАССМОТРЕНО

Протокол заседания учебно-методического совета ГБПОУ «Волгоградский строительный техникум» № __ от «__» _____ 202_ г.

РАССМОТРЕНО

Протокол заседания ЦМК _____

№ __ от «__» _____ 202_ г.

Председатель ЦМК

Зав. кафедрой технического профиля
подготовки очной формы обучения

_____ Н.Г. Титова

Структура программы государственной итоговой аттестации

1. ОБЩИЕ ПОЛОЖЕНИЯ
2. ЦЕЛИ И ЗАДАЧИ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ
3. ФОРМЫ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ И УСЛОВИЯ ЕЕ ПРОВЕДЕНИЯ
 - 3.1 Формы государственной итоговой аттестации
 - 3.2 Объем времени и сроки проведения государственной итоговой аттестации
 - 3.3 Условия допуска обучающихся к государственной итоговой аттестации
 - 3.4 Процедура проведения государственной итоговой аттестации
 - 3.5 Особенности проведения государственной итоговой аттестации для лиц с ограниченными возможностями, детей-инвалидов
 - 3.6 Документация по итогам государственной итоговой аттестации
4. ТРЕБОВАНИЯ К ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ В ФОРМЕ ЗАЩИТЫ ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЫ (ДИПЛОМНЫЙ ПРОЕКТ)
 - 4.1 Материалы необходимые для подготовки выпускной квалификационной работы (дипломный проект)
 - 4.2 Тематика выпускной квалификационной работы (дипломный проект)
 - 4.3 Объем и структура выпускной квалификационной работы (дипломный проект)
 - 4.4 Руководство подготовкой и защитой выпускной квалификационной работы (дипломный проект)
 - 4.5 Рецензирование выпускной квалификационной работы (дипломный проект)
 - 4.6 Указания по подготовке к защите выпускной квалификационной работы (дипломный проект)
 - 4.7 Условия защиты выпускной квалификационной работы (дипломный проект)
 - 4.8 Критерии оценки и защиты выпускной квалификационной работы (дипломный проект)
1. ТРЕБОВАНИЯ К ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ В ФОРМЕ ЗАЩИТЫ ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЫ, ВЫПОЛНЯЕМОЙ В ВИДЕ ДЕМОНСТРАЦИОННОГО ЭКЗАМЕНА
 - 5.1 Подготовка к процедуре проведению выпускной квалификационной работы, которая выполняется в виде демонстрационного экзамена
 - 5.2 Процедура проведения выпускной квалификационной работы, которая выполняется в виде демонстрационного экзамена
 - 5.3 Оценка выпускной квалификационной работы, которая выполняется в виде демонстрационного экзамена
2. ПОРЯДОК ПОДАЧИ И РАССМОТРЕНИЯ АПЕЛЯЦИЙ
3. ХРАНЕНИЕ ВЫПУСКНЫХ КВАЛИФИЦИРОВАННЫХ РАБОТ
 - Приложение А
 - Приложение Б
 - Приложение В

Приложение Г
Приложение Д
Приложение Е
Приложение Ж
Приложение З
Приложение И
Приложение К
Приложение Л
Приложение М
Приложение Н
Приложение О
Приложение П

1. Общие положения

Настоящая Программа государственной итоговой аттестации обучающихся по специальности 10.02.05 Обеспечение автоматизированных систем информационной безопасности на 2023 год (далее - программа ГИА) определяет совокупность требований к ГИА обучающихся (далее – ГИА) государственного бюджетного профессионального образовательного учреждения «Волгоградский строительный техникум» (далее – техникум) специальности 10.02.05 Обеспечение автоматизированных систем информационной безопасности.

Программа ГИА разработана в соответствии с действующей нормативно-правовой документацией и локальными актами техникума:

- Федеральный закон «Об образовании в РФ» от 29.12.2012 г. № 273;
- Приказ Министерства образования и науки Российской Федерации от 14.06.2013 года №464 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам среднего профессионального образования»;
- Федеральный государственный образовательный стандарт среднего профессионального образования (далее - ФГОС СПО) по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утвержденным приказом Министерства образования и науки Российской Федерации от 09 декабря 2016 г. № 1553,
- Порядок проведения государственной итоговой аттестации по образовательным программам среднего профессионального образования, утвержденный приказом Министерства просвещения 8 ноября 2021 г. №800 (далее – Порядок);
- Устав государственного бюджетного профессионального образовательного учреждения «Волгоградский строительный техникум»;
- Положение о государственной итоговой аттестации выпускников ГБПОУ «Волгоградский строительный техникум», утвержденного приказом директора техникума от 01.09.2022 г. № 279-П (далее – Положение).

В соответствии с ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем ГИА обучающихся техникума проводится в форме защиты выпускной квалификационной работы (дипломный проект) (далее – ВКР(ДП)) и демонстрационного экзамена.

Программа ГИА определяет требования к защите ВКР(ДП), методике его оценивания, а также уровень ДЭ, конкретные комплекты оценочной документации (далее- КОД), выбранные техникумом, исходя из содержания

реализуемой образовательной программы 10.02.05 Обеспечение информационной безопасности автоматизированных систем (далее – ОП), из размещенных на официальном сайте оператора в сети «Интернет» единых оценочных материалов, включающихся в программу ГИА.

ГИА является обязательной процедурой для обучающихся техникума, завершающих освоение программы подготовки специалистов среднего звена (далее – ППССЗ) по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

ГИА обучающихся не может быть заменена на оценку уровня их подготовки на основе текущего контроля успеваемости и результатов промежуточной аттестации, за исключением случая если по решению государственной экзаменационной комиссии (ГЭК) результаты ДЭ, проведенного при участии оператора в рамках промежуточной аттестации по итогам освоения профессионального модуля по заявлению обучающихся, а могут быть учтены при выставлении оценки по итогам ГИА в форме ДЭ.

Программа ГИА ежегодно утверждается директором техникума после обсуждения на заседаниях учебно-методического совета, педагогического совета с участием председателя ГЭК.

Программа ГИА доводится до сведения обучающихся не позднее, чем за шесть месяцев до начала ГИА.

2. Цели и задачи государственной итоговой аттестации

Целью ГИА является комплексная оценка качества и уровня подготовки обучающихся, а также соответствие результатов освоения образовательной программы требованиям ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, требованиям работодателей. Требования к профессиональной подготовленности обучающихся, необходимые для выполнения им профессиональных функций. ВКР(ДП) – это комплексная самостоятельная работа обучающегося, главной целью и содержанием которой является всесторонний анализ, исследование и разработка некоторых актуальных задач как теоретического, так и прикладного характера по профилю специальности.

Успешное прохождение обучающимся ГИА, является завершающим этапом получения среднего профессионального образования и необходимым условием присуждения обучающемуся квалификации «техник по защите информации» по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Целевым назначением ГИА является комплексная оценка компетенций обучающегося на соответствие требованиям к результатам освоения основной профессиональной образовательной программы по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, отражающей объекты и виды будущей профессиональной деятельности.

Ориентируясь на достижение общих целей образования в целом – формирование и развитие креативного (созидательного, инновационного) типа мышления и целей среднего профессионального образования в частности – ГИА направлена на выполнение основных требований к результатам освоения основной профессиональной образовательной программы, по которым производится оценка уровня профессиональной подготовленности обучающегося. Интегрально эти основные требования сводятся к следующему:

Общие компетенции:

ОК 01. Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам;

ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности;

ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие;

ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами;

ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста;

ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей;

ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях;

ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности;

ОК 09. Использовать информационные технологии в профессиональной деятельности;

ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках;

ОК 11. Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере.

Профессиональные компетенции:

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.

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.

ПК 3.1. Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации.

ПК 3.2. Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации.

ПК 3.3. Осуществлять измерение параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа.

ПК 3.4. Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.

ПК 3.5. Организовывать отдельные работы по физической защите объектов информатизации.

3. Формы государственной итоговой аттестации, условия ее проведения

3.1 Формы государственной итоговой аттестации

В соответствии с ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем ГИА проводится в форме защиты выпускной квалификационной работы (дипломная работа (дипломный проект) (далее - ВКР(ДП)). По усмотрению образовательной организации демонстрационный экзамен включается в выпускную квалификационную работу или проводится в виде государственного экзамена.

Обучающимися техникума специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем в 202__ году проходят ГИА в форме ВКР (ДП) и ДЭ.

По решению техникума, с учетом заявлений обучающихся на основе требований к результатам освоения ОП СПО по специальности, установленных ФГОС СПО 10.02.05 Обеспечение информационной безопасности автоматизированных систем, с учетом положений стандартов «Ворлдскиллс», устанавливаемых автономной некоммерческой организацией «Агентство развития профессионального мастерства (Ворлдскиллс Россия) (далее - Агентство), а также квалификационных требований (далее - организации-партнеры) обучающиеся сдают ДЭ базового ли профильного уровней.

3.2 Объем времени и сроки проведения государственной итоговой аттестации

Объем времени на подготовку и проведение ГИА в форме ВКР (ДП) установлен учебным планом в соответствии с ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

На ГИА отводиться – 216 часов, что соответствует 6 неделям, из них:

4 недели (144 ч) - на подготовку к ГИА,

2 недели (72 часа) - на проведение ГИА (защита ВКР(ДП) и сдача

ДЭ).

Сроки проведения ГИА для обучающихся очной формы обучения установлены в соответствии с календарным учебным графиком на 2022-2023 учебный год:

- с __.05.2023 по __.06.2023 – подготовка к ГИА,

- с __.06.2022 по __.06.2022 – проведение ГИА

3.3 Условия допуска обучающихся к государственной итоговой аттестации

К ГИА допускаются обучающиеся и специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем (далее – обучающиеся), не имеющие академической задолженности и в полном объеме

выполнившие учебный план или индивидуальный учебный план, о чем свидетельствуют:

- документы, подтверждающие освоение обучающимся компетенций при изучении теоретического материала и прохождении практики по каждому из основных видов деятельности;
- наличие зачетной книжки, подтверждающей отсутствие у обучающегося академических задолженностей и выполнение учебного плана или индивидуального учебного плана.

Необходимым условием допуска к защите ВКР(ДП) является:

- наличие ВКР(ДП), выполненной в соответствии с индивидуальным заданием, в сроки, установленные графиком;
- наличие отзыва руководителя ВКР на ВКР(ДП);
- наличие рецензии специалиста отраслевой организации (предприятия) или другой образовательной организации.

Решение о допуске обучающихся к ГИА утверждается приказом директора техникума.

Обучающиеся и в рамках ГИА имеют право представить портфолио обучающегося, в котором представлены отчеты о ранее достигнутых результатах в своей учебной и общественной деятельности, полученные дополнительные сертификаты, свидетельства (дипломы) олимпиад, конкурсов, творческие работы по специальности, характеристики с мест прохождения производственной и/или преддипломной практики.

3.4 Процедура проведения государственной итоговой аттестации

Обучающиеся проходят процедуру ГИА в форме ВКР (ДП) и ВКР в виде ДЭ.

В целях определения соответствия результатов освоения обучающимися имеющих государственную аккредитацию образовательных программ СПО соответствующим требованиям ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем ГИА проводится государственными экзаменационными комиссиями (далее - ГЭК), создаваемыми в техникуме.

Защита ВКР(ДП) проводится на открытых заседаниях ГЭК с участием не менее двух третей ее состава.

Результаты проведения ГИА оцениваются с проставлением одной из отметок: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно» - и объявляются в тот же день после оформления протоколов заседаний ГЭК (Приложение А).

Выполнение ВКР в виде ДЭ профильного или базового уровня **по стандартам Ворлдскиллс Россия** проводится с использованием единых оценочных материалов, включающих в себя конкретные КОД, варианты заданий

и критерии оценивания, разрабатываемых оператором с участием организаций-партнеров, отраслевых и профессиональных сообществ.

Результаты проведения ГИА оцениваются с проставлением одной из отметок: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно» - и объявляются в тот же день после оформления протоколов заседаний ГЭК.

Процедура оценивания результатов выполнения заданий ДЭ осуществляется членами экспертной группы по 100-балльной системе в соответствии с требованиями КОД.

Баллы выставляются в протоколе проведения ДЭ (Приложение Б), который подписывается каждым членом экспертной группы и утверждается главным экспертом после завершения экзамена для экзаменационной группы.

При выставлении баллов присутствует член ГЭК, не входящий в экспертную группу, присутствие других лиц запрещено.

Статус победителя, призера чемпионатов профессионального мастерства, проведенных Агентством (Союзом «Агентство развития профессиональных сообществ и рабочих кадров «Молодые профессионалы (Ворлдскиллс Россия)») либо международной организацией «WorldSkills International», в том числе «WorldSkills Europe» и «WorldSkills Asia», и участника национальной сборной России по профессиональному мастерству по стандартам «Ворлдскиллс» обучающегося а по профилю осваиваемой образовательной программы СПО засчитывается в качестве оценки «отлично» по демонстрационному экзамену в рамках проведения ГИА по данной образовательной программе СПО.

Подписанный членами экспертной группы и утвержденный главным экспертом протокол проведения ДЭ далее передается в ГЭК для выставления оценок по итогам ГИА (Приложение В).

Оригинал протокола проведения ДЭ передается на хранение в техникуме в составе архивных документов.

В случае досрочного завершения ГИА обучающим по независящим от него причинам результаты ГИА оцениваются по фактически выполненной работе, или по заявлению такого обучающегося, а ГЭК принимается решение об аннулировании результатов ГИА, а такой обучающийся признается ГЭК не прошедшим ГИА по уважительной причине.

Решения ГЭК принимаются на закрытых заседаниях простым большинством голосов членов ГЭК, участвующих в заседании, при обязательном присутствии председателя комиссии или его заместителя. При равном числе голосов голос председательствующего на заседании ГЭК является решающим.

Решение ГЭК оформляется протоколом, который подписывается председателем ГЭК, в случае его отсутствия заместителем ГЭК и секретарем ГЭК и хранится в архиве техникума.

Обучающимся, не прошедшим ГИА по уважительной причине, в том числе не явившимся для прохождения ГИА по уважительной причине (далее - обучающиеся и, не прошедшие ГИА по уважительной причине), предоставляется возможность пройти ГИА без отчисления из техникума.

Обучающиеся не прошедшие ГИА по неуважительной причине, в том числе не явившиеся для прохождения ГИА без уважительных причин (далее - обучающиеся и, не прошедшие ГИА по неуважительной причине) и

обучающиеся и, получившие на ГИА неудовлетворительные результаты, могут быть допущены техникумом для повторного участия в ГИА не более двух раз.

Дополнительные заседания ГЭК организуются в установленные техникумом сроки, но не позднее четырех месяцев после подачи заявления обучающимся, не прошедшим ГИА по уважительной причине.

Обучающиеся, не прошедшие ГИА по неуважительной причине, и обучающиеся, получившие на ГИА неудовлетворительные результаты, отчисляются из техникума и проходят ГИА не ранее чем через шесть месяцев после прохождения ГИА впервые.

3.5 Особенности проведения государственной итоговой аттестации для лиц с ограниченными возможностями здоровья, детей-инвалидов

Для обучающихся из числа лиц с ограниченными возможностями здоровья и обучающихся из числа детей-инвалидов и инвалидов проводится ГИА с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся (далее - индивидуальные особенности).

При проведении ГИА в техникуме обеспечивается соблюдение следующих общих требований:

- проведение ГИА для обучающихся с ограниченными возможностями здоровья, обучающихся из числа детей-инвалидов и инвалидов в одной аудитории совместно с обучающимися, не имеющими ограниченных возможностей здоровья, если это не создает трудностей для обучающихся при прохождении ГИА;
- присутствие в аудитории, центре проведения экзамена тьютора, ассистента, оказывающих обучающимся необходимую техническую помощь с учетом их индивидуальных особенностей (занять рабочее место, передвигаться, прочесть и оформить задание, общаться с членами ГЭК, членами экспертной группы);
- пользование необходимыми обучающимся техническими средствами при прохождении ГИА с учетом их индивидуальных особенностей;
- обеспечение возможности беспрепятственного доступа обучающихся в аудитории, туалетные и другие помещения, а также их пребывания в указанных помещениях (наличие пандусов, поручней, расширенных дверных проемов, лифтов, при отсутствии лифтов аудитория располагается на первом этаже, наличие специальных кресел и других приспособлений).

Дополнительно при проведении ГИА обеспечивается соблюдение следующих требований в зависимости от категорий обучающихся с ограниченными возможностями здоровья, обучающихся из числа детей-инвалидов и инвалидов:

Для слепых:

- задания для выполнения, а также инструкция о порядке ГИА, КОД, задания ДЭ оформляются рельефно-точечным шрифтом по системе Брайля или в виде электронного документа, доступного с помощью

компьютера со специализированным программным обеспечением для слепых, или зачитываются ассистентом;

- письменные задания выполняются на бумаге рельефно-точечным шрифтом по системе Брайля или на компьютере со специализированным программным обеспечением для слепых, или надиктовываются ассистенту;
- обучающимся для выполнения задания при необходимости предоставляется комплект письменных принадлежностей и бумага для письма рельефно-точечным шрифтом Брайля, компьютер со специализированным программным обеспечением для слепых.

Для слабовидящих:

- обеспечивается индивидуальное равномерное освещение не менее 300 люкс;
- обучающимся для выполнения задания при необходимости предоставляется увеличивающее устройство;
- задания для выполнения, а также инструкция о порядке проведения ГИА оформляются увеличенным шрифтом.

Для глухих и слабослышащих, с тяжелыми нарушениями речи:

- обеспечивается наличие звукоусиливающей аппаратуры коллективного пользования, при необходимости предоставляется звукоусиливающая аппаратура индивидуального пользования;
- по их желанию государственный экзамен может проводиться в письменной форме.

Для лиц с нарушениями опорно-двигательного аппарата (с тяжелыми нарушениями двигательных функций верхних конечностей или отсутствием верхних конечностей):

- письменные задания выполняются на компьютере со специализированным программным обеспечением или надиктовываются ассистенту;
- по их желанию государственный экзамен может проводиться в устной форме.

Также для обучающихся из числа лиц с ограниченными возможностями здоровья и обучающихся из числа детей-инвалидов и инвалидов создаются иные специальные условия проведения ГИА в соответствии с рекомендациями психолого-медико-педагогической комиссии (далее - ПМПК), справкой, подтверждающей факт установления инвалидности, выданной федеральным государственным учреждением медико-социальной экспертизы (далее - справка).

Обучающиеся или родители (законные представители) несовершеннолетних обучающихся не позднее чем за 3 месяца до начала ГИА подают в образовательную организацию письменное заявление о необходимости создания для них специальных условий при проведении ГИА с приложением копии рекомендаций психолого-медико-педагогической комиссии, а дети-инвалиды, инвалиды - оригинала или заверенной копии справки, а также копии рекомендаций психолого-медико-педагогической комиссии при наличии.

3.6 Документация по итогам государственной итоговой аттестации

Решение ГЭК о присвоении квалификации «Техник по защите информации» по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем и о выдаче диплома обучающимся, прошедшим ГИА оформляется протоколом ГЭК и приказом директора техникума.

По окончании ГИА председатель ГЭК составляет отчет о работе комиссии.

4. Требования к государственной итоговой аттестации в форме выпускной квалификационной работы (дипломного проекта)

Прохождение ГИА в форме защиты ВКР(ДП) направлено на систематизацию и закрепление знаний обучающимися по специальности, а также определение уровня готовности обучающихся к самостоятельной профессиональной деятельности. Защита ВКР(ДП) предполагает самостоятельную подготовку обучающимся проекта, демонстрирующего уровень знаний обучающегося в рамках выбранной темы, а также сформированности его профессиональных умений и навыков.

4.1 Материалы необходимые для подготовки защиты выпускной квалификационной работы (дипломный проект)

Для подготовки ВКР (ДП) необходимы следующие материалы:

- тематика ВКР(ДП) (Приложение Д);
- критерии оценки содержания ВКР (ДП);
- критерии оценки защиты ВКР(ДП);
- перечень учебной литературы, нормативно-правовых актов;
- образцы оформления ВКР(ДП);
- титульный лист ВКР(ДП) (Приложение Ж);
- форма бланка индивидуального задания на ВКР(ДП) (Приложение З);
- список использованных источников.

4.2 Тематика выпускной квалификационной работы (дипломный проект)

Тематика ВКР(ДП) определяется техникумом. Обучающемуся предоставляется право выбора темы ВКР(ДП), в том числе предложения своей темы с необходимым обоснованием целесообразности ее разработки для практического применения.

Темы ВКР(ДП) на 202__ год представлены в Приложении Г.

В случае если студент в установленные сроки не выбрал тему ВКР(ДП), цикловая методическая комиссия вправе определить ее по собственному усмотрению.

Для подготовки ВКР(ДП) обучающемуся назначается руководитель и при необходимости консультанты, оказывающие обучающемуся методическую поддержку.

После получения темы ВКР(ДП) обучающийся пишет заявление на имя заместителя директора по учебной работе, в котором указывает выбранную тему и руководителя ВКР(ДП) (форма заявления - Приложение Д).

Окончательное закрепление тем ВКР(ДП) и руководителей оформляется приказом директора.

Подготовка к защите ВКР(ДП) осуществляется обучающимся в течение 4 недель при участии руководителя ВКР(ДП).

4.3 Объем и структура, распределение объёма выпускной квалификационной работы (дипломный проект)

ВКР(ДП) (70-90 страниц рукописного или 50-80 страниц печатного текста формата А4) состоит из Пояснительной записки, проектной (практической) части и презентационного материала.

Пояснительная записка имеет следующее содержание:

1 Теоретический раздел - дается обзор и теоретические основы рассматриваемой проблемы, динамика развития исследуемой темы, анализ отечественного и международного опыта, накопленного в данной области.

2 Аналитический раздел выполняется с учетом данных, полученных в результате анализа теоретического раздела, включает в себя исследования, расчёты, выводы и обоснования, предложения по улучшению и т.д.

3 Практический раздел включает в себя выполнение практического задания, написание исходного кода программы, сборку модели или устройства, выполнение практических действий по сборке, ремонту, установке и модификации материальных и программных комплексов и т.д.

4 Экономический раздел, включающий в себя расчёт экономической эффективности проекта.

5 Безопасность жизнедеятельности.

В проектной (практической) части выделяются три направления: - разработка проекта по модернизации программно-аппаратных и инженерно-технических средств защиты информации; - разработка проекта по организации защиты информации на предприятии; - разработка программ для шифрования, дешифрования на основе различных алгоритмов; - проектирование стендов согласно профилю специальности.

Иногда в тематике дипломного проектирования невозможно провести четкую грань между разработкой аппаратных и программных средств, так как задача, поставленная перед дипломником, может быть решена только за счет их совместного применения. Дипломные проекты такого типа ориентированы на комплексную разработку аппаратных и программных средств. Обоснование решения в виде наглядного представления (схемы алгоритма, диаграммы, циклограммы, информационной или иной модели, блок-схемы и т.д.) должно быть представлено в раздаточном материале.

Программные документы, разработанные в ВКР (ДП) различных проблемных областей, должны быть оформлены в соответствии с требованиями стандартов Единой системы программной документации.

Графическая часть ВКР (ДП) должна иллюстрировать постановку задачи, формализацию методов ее решения, реализацию, полученные результаты. Под презентационной частью ВКР (ДП) понимают готовые форматные слайды, в одном из общеупотребительных форматах их представления – электронном (ppt, pptx, pdf и т.д.), графическом (плакаты и чертежи), мультимедийные (видеоролики), содержащие конкретную, чётко структурируемую информацию. Презентация представляется в электронном

виде, на одном из установленных типов носителей (CD/DVD диск, флэш карта, переносной жёсткий диск и т.д.). Допускается использование обучающимся своих средств представления презентаций (ноутбуков).

4.4 Руководство подготовкой и защитой выпускной квалификационной работы(дипломный проект)

Основные функции руководителя ВКР(ДП) следующие:

- разработка индивидуальных заданий;
- проведение консультаций по вопросам содержания, последовательности и сроков выполнения ВКР(ДП) согласно графику, утвержденному директором техникума;
- оказание помощи обучающемуся в подборе необходимой литературы, в использовании фактических данных, презентационных материалов, в формулировании четких выводов;
- подготовка письменного отзыва на ВКР(ДП);
- составление графика проверки хода выполнения ВКР(ДП), который утверждается директором техникума (Приложение К).

По завершении работы над ВКР(ДП) руководитель проверяет ее содержание и оформление, подписывает и составляет отзыв на ВКР(ДП).

Отзыв на ВКР(ДП) составляется руководителем в соответствии с установленной формой (Приложение Л).

Отзыв руководителя должен содержать:

- а) оценку степени качественного решения поставленных цели и задач;
- б) оценку уровня профессионализма и самостоятельности в проведении исследования, в практических рекомендациях;
- в) указание на степень соответствия оформления ВКР(ДП) установленным требованиям.

Заведующий кафедрой после получения отзыва направляет обучающегося на внешнюю рецензию.

Готовый ВКР(ДП) подписывает заместитель директора по учебной работе, дает допуск к его защите и передает ВКР(ДП) в ГЭК.

4.5 Рецензирование дипломного проекта

ВКР(ДП) подлежит рецензированию ведущими преподавателями техникума, специалистами из числа работников образовательных учреждений СПО, ВПО, предприятий строительной отрасли г. Волгограда и Волгоградской области, деятельность которых связана с профилем подготовки обучающихся близка к тематике ВКР(ДП).

Рецензенты ВКР (ДП) назначаются приказом директора техникума.

Рецензия внешняя (Приложение М) должна включать:

- заключение о соответствии выполненной ВКР(ДП) заданию;
- оценку качества содержания каждого раздела ВКР(ДП);
- оценку степени новизны в разработке вопросов, оригинальности решений (предложений), теоретической и практической значимости работы;
- общую оценку ВКР(ДП) (отлично, хорошо, удовлетворительно, неудовлетворительно).

Содержание рецензии доводится до сведения обучающегося не позднее, чем за день до защиты ВКР(ДП).

Внесение изменений в ВКР(ДП) после получения рецензии не допускается.

Заместитель директора по учебной работе после ознакомления с отзывом и рецензией решает вопрос о допуске обучающегося к защите и передает ВКР(ДП) в ГЭК.

4.6 Указания по подготовке к защите дипломного проекта

Чтобы успешно защитить дипломный проект, обучающийся должен ориентироваться в ее теоретической части, разбираться в методах исследования и подготовить речь для выступления перед членами аттестационной комиссии.

Подготовительный этап

Первое, что необходимо сделать перед защитой дипломного проекта, — обсудить с руководителем дипломного проекта затруднительные моменты, возникшие в ходе учебно-исследовательской деятельности, а также досконально проработать все полученные замечания.

Текст выступления целесообразно заранее обсудить с руководителем дипломного проекта, чтобы в случае чего иметь возможность внести поправки. К докладу рекомендуется подготовить мультимедийную презентацию и раздаточный материал (если возникает необходимость), которые помогут раскрыть цели и задачи дипломного проекта.

Продумать ответы на примерные вопросы членов комиссии.

4.7 Условия защиты дипломного проекта

Защита ВКР(ДП) проводится на открытых заседаниях ГЭК с участием не менее двух третей ее состава согласно расписанию, утверждаемому директором техникума.

На защиту ВКР(ДП) каждому обучающемуся отводится не более 45 мин.

Процедура защиты ВКР(ДП):

- представление работы секретарем комиссии;
- доклад обучающегося (10-15 мин);
- представление отзыва и рецензии;
- ответы обучающегося на вопросы членов комиссии.

Примерная структура доклада на защите ВКР(ДП):

- представление темы ВКР(ДП);
- актуальность выбранной темы ВКР(ДП);

- цель, задачи работы, предмет, объект и методы исследования;
- краткий обзор основного содержания ВКР(ДП);
- основные выводы и рекомендации по исследуемой проблеме.

Защита ВКР(ДП) является публичной. Обучающемуся рекомендуется подготовить презентацию, выполненную с применением информационных технологий.

Члены ГЭК могут задавать вопросы, как по теме дипломного проекта, так и для выявления общей профессиональной подготовленности обучающегося (Приложение Н).

4.8 Критерии оценки и защиты дипломного проекта

ГЭК коллегиально оценивает содержание ВКР(ДП), форму его защиты, оценивает уровень знаний и соответствие подготовки обучающегося требованиям ФГОС СПО специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Критерии оценки текста ВКР(ДП):

- актуальность и новизна темы;
- практическая значимость ВКР(ДП);
- соответствие целей и задач, поставленных в дипломном проекте, полученным результатам и выводам;
- уровень профессиональной компетентности обучающегося;
- умение анализировать и обобщать факты, самостоятельно решать поставленные задачи, в том числе и нестандартные;
- умение работать с современными научно-правовыми источниками, разрабатывать рекомендации по улучшению финансово-хозяйственной деятельности организации;
- структура работы, последовательность и логичность, завершенность изложения, стиль изложения, культура оформления;
- достоверность и объективность результатов ВКР(ДП), выполненной в форме ВКР(ДП), использование в работе современных научных достижений в сфере отечественной и зарубежной экономики, наличие обобщений, логических аргументов специалистов-практиков;
- достаточность и актуальность использованных учебных и нормативно-правовых документов;
- обоснованность привлечения тех или иных методов решения поставленных задач;
- глубина и обоснованность анализа и полученных результатов;
- соответствие оформления дипломного проекта требованиям ФГОС СПО специальности 10.02.05 Обеспечение

информационной безопасности автоматизированных систем методическим рекомендациям по оформлению ВКР (ДП).

При оценке ВКР(ДП) дополнительно учитывается качество сообщения, отражающего основное содержание ВКР(ДП), и ответы обучающегося а на вопросы, заданные как по теме ВКР(ДП), так и из сферы его будущей профессиональной деятельности.

Критерии оценки графической части ВКР(ДП):

- соответствие чертежей выданному заданию;
- полное насыщение проекта необходимыми чертежами;
- использование информационных технологий при выполнении графической части;
- рациональное размещение материала на листах с точки зрения компактности;
- соответствие оформления проекта требованиям ГОСТ и СПДС;
- четкая графика, аккуратность;

При оценке дипломного проекта дополнительно учитывается качество сообщения, отражающего основное содержание ВКР(ДП), и ответы обучающегося а на вопросы, заданные как по теме ВКР(ДП), так и из сферы его будущей профессиональной деятельности.

Критерии оценки защиты ВКР(ДП):

- четкость и внятность доклада, отражающего актуальность, новизну, цель, задачи, краткое содержание, основные выводы и результаты работы;
- четкость, внятность, глубина ответов на вопросы членов ГЭК и присутствующих на защите;
- обоснованность, логичность, глубина ответов на замечания, содержащиеся в рецензии;
- качество выполнения и оформления графического материала;
- использование технических средств, сопровождающих доклад.

При определении окончательной оценки учитываются материалы портфолио обучающегося, характеризующие уровень освоенности профессиональных и общих компетенций.

Итоговая оценка определяются оценками ***«отлично»***, ***«хорошо»***, ***«удовлетворительно»***, ***«неудовлетворительно»***.

Оценка ***«Отлично»*** выставляется за ВКР(ДП), которая соответствует следующим требованиям:

- работа по тематике актуальна и соответствует одному из профессиональных модулей, выполнена обучающимся самостоятельно;

- по своему стилистическому содержанию, форме и объему дипломный проект соответствует требованиям методических рекомендаций;
- наличие презентации по материалам ВКР(ДП) с использованием информационных технологий;
- свободное оперирование данными исследования;
- полное насыщение проекта необходимыми чертежами;
- использование информационных технологий при выполнении графической части;
- рациональное размещение материала на листах с точки зрения компактности;
- соответствие оформления проекта требованиям ГОСТ и СПДС;
- четкая графика, аккуратность;
- грамотное выступление по содержанию, при ответах на вопросы и критические замечания;
- рецензия на выпускную квалификационную работу содержит минимальные замечания;
- обучающийся демонстрирует высокий уровень освоения общих и профессиональных компетенций.

Оценка «*Хорошо*» выставляется в случае, если:

- работа актуальна, выполнена обучающийся самостоятельно;
- по своему стилистическому содержанию, форме и объему работа соответствует требованиям методических рекомендаций;
- обучающийся показывает знания основных проблем темы, оперирует данными проведенных исследований;
- наличие презентации с использованием информационных технологий;
- насыщение ВКР(ДП) необходимыми чертежами;
- рациональное размещение материала на листах с точки зрения компактности;
- соответствие оформления проекта требованиям ГОСТ и СПДС;
- четкая графика, аккуратность;
- отзыв руководителя на ВКР(ДП) содержит незначительные замечания;
- рецензент, высказывает несущественные замечания;
- выступление обучающегося при защите, ответы на вопросы и критические замечания проведены в недостаточно полном объеме;
- при защите обучающийся демонстрирует хороший уровень освоения общих и профессиональных компетенции.

Оценка **«Удовлетворительно»** выставляется в случае, если:

- работа соответствует заявленной теме;
- по своему стилистическому содержанию, объему и форме работа не во всем соответствует требованиям методических рекомендаций;
- чертежи соответствуют выданному заданию;
- соответствие оформления ВКР(ДП) требованиям ГОСТ и СПДС;
- аккуратность;
- выступление студента при защите, ответы на вопросы и критические замечания не имеют глубины, не раскрывают тему в полном объеме;
- отзыв руководителя на ВКР(ДП) содержит значительные замечания;
- рецензент высказывает серьезные замечания;
- при защите обучающийся демонстрирует поверхностный уровень освоения общих и профессиональных компетенций.

Оценка **«Неудовлетворительно»** выставляется в том случае, если:

- содержание работы не соответствует теме;
- отсутствуют аналитические материалы;
- предложения не имеют четкости в содержании и оформлении;
- в отзывах руководителя и рецензента имеются существенные критические замечания;
- при защите дипломного проекта студент не смог сделать убедительный доклад по теме работы, не ответил на поставленные вопросы, не знает теории вопроса, при ответе допустил существенные ошибки

5. Требования к государственной итоговой аттестации в форме выпускной квалификационной работы, которая выполняется в виде демонстрационного экзамена

ВКР в виде демонстрационного экзамена базового или профильного уровней (далее – ДЭ) направлены на определение уровня освоения обучающимися материала, предусмотренного ОП по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, и степени форсированности профессиональных умений и навыков путём проведения независимой экспертной оценки выполненных обучающимся практических заданий в условиях реальных или смоделированных производственных процессов.

5.1. Подготовка к процедуре проведения демонстрационного экзамена

ДЭ базового или профильного уровней проводится с использованием единых оценочных материалов, варианты заданий и критерии оценивания, разрабатываемых оператором с участием организаций-партнеров, отраслевых и профессиональных сообществ (Приложение И).

Техникум заимствует КОД для проведения ДЭ, разработанный Министерством просвещения Российской Федерации и размещенный на официальном сайте оператора в информационно-телекоммуникационной сети «Интернет» (далее - сеть «Интернет») не позднее 1 октября 202__ года, предшествующего проведению ГИА.

КОД включает комплекс требований для проведения ДЭ, перечень оборудования и оснащения, расходных материалов, средств обучения и воспитания, план застройки площадки ДЭ, требования к составу экспертных групп, инструкции по технике безопасности, а также образцы заданий.

Задание ДЭ включает комплексную практическую задачу, моделирующую профессиональную деятельность и выполняемую в режиме реального времени.

Задания ДЭ доводятся до главного эксперта в день, предшествующий дню начала ДЭ.

Техникум обеспечивает необходимые технические условия для обеспечения заданиями во время ДЭ обучающихся, членов ГЭК, членов экспертной группы.

ДЭ проводится в центре проведения демонстрационного экзамена (далее - центр проведения экзамена), представляющем собой площадку на территории техникума, оборудованную и оснащенную в соответствии с КОД.

Место расположения центра проведения экзамена, дата и время начала проведения ДЭ, расписание сдачи экзаменов в составе экзаменационных групп, планируемая продолжительность проведения ДЭ, технические перерывы в проведении ДЭ определяются планом проведения ДЭ,

утверждаемым ГЭК совместно с техникумом не позднее чем за двадцать календарных дней до даты проведения ДЭ. (Приложение П)

Техникум знакомит с планом проведения ДЭ обучающихся, сдающих ДЭ, и лиц, обеспечивающих проведение ДЭ, в срок не позднее чем за пять рабочих дней до даты проведения экзамена.

Количество, общая площадь и состояние помещений, предоставляемых для проведения ДЭ, должны обеспечивать проведение ДЭ в соответствии с КОД.

Центр проведения экзамена соответствует условиям, установленным КОД, в том числе в части наличия расходных материалов, что подтверждает статус «обследование» оператора.

Не позднее чем за один рабочий день до даты проведения ДЭ главным экспертом проводится проверка готовности центра проведения экзамена в присутствии членов экспертной группы, обучающихся, а также технического эксперта, назначаемого организацией, на территории которой расположен центр проведения экзамена, ответственного за соблюдение установленных норм и правил охраны труда и техники безопасности.

Главным экспертом осуществляется осмотр центра проведения экзамена, распределение обязанностей между членами экспертной группы по оценке выполнения заданий ДЭ, а также распределение рабочих мест между обучающимися с использованием способа случайной выборки. Результаты распределения обязанностей между членами экспертной группы и распределения рабочих мест между обучающимися фиксируются главным экспертом в соответствующих протоколах.

5.2 Права и обязанности участников демонстрационного экзамена

5.2.1 Центр проведения экзамена располагается на территории техникума, обладающей необходимыми ресурсами для организации центра проведения экзамена.

Обучающиеся проходят ГИА в форме ДЭ в центре проведения экзамена в составе экзаменационных групп.

Обучающиеся знакомятся со своими рабочими местами, под руководством главного эксперта также повторно знакомятся с планом проведения ДЭ, условиями оказания первичной медицинской помощи в центре проведения экзамена. Факт ознакомления отражается главным экспертом в протоколе распределения рабочих мест.

5.2.2 Технический эксперт под подпись знакомит главного эксперта, членов экспертной группы, обучающихся, проходящих ГИА в форме ДЭ с требованиями охраны труда и безопасности производства.

5.2.3 В день проведения ДЭ в центре проведения экзамена присутствуют:

- руководитель (уполномоченный представитель) организации, на базе которой организован центр проведения экзамена;
- не менее одного члена ГЭК, не считая членов экспертной группы;
- члены экспертной группы;
- главный эксперт;
- представители организаций-партнеров (по согласованию с техникумом);
- обучающиеся, проходящие ГИА в форме ДЭ;
- технический эксперт;
- представитель техникума, ответственный за сопровождение обучающихся к центру проведения экзамена (при необходимости);
- тьютор (ассистент), оказывающий необходимую помощь обучающемуся из числа лиц с ограниченными возможностями здоровья, детей-инвалидов, инвалидов (далее - тьютор (ассистент));
- организаторы, назначенные техникумом из числа педагогических работников, оказывающие содействие главному эксперту в обеспечении соблюдения всех требований к проведению ДЭ.

5.2.4 В случае отсутствия в день проведения ДЭ в центре проведения экзамена лиц, указанных в настоящем пункте, решение о проведении ДЭ принимается главным экспертом, о чем главным экспертом вносится соответствующая запись в протокол проведения ДЭ.

Допуск обучающихся к ГИА в форме ДЭ в центр проведения экзамена осуществляется главным экспертом на основании документов, удостоверяющих личность.

В день проведения ДЭ в центре проведения экзамена могут присутствовать:

- должностные лица Комитета образования, науки и молодежной политики Волгоградской области (по решению последнего);
- представители оператора (по согласованию с техникумом);
- медицинские работники (по решению техникума);
- представители организаций-партнеров (по решению таких организаций по согласованию с техникумом).

Указанные в пунктах 4.2.3 и 4.2.4 лица присутствуют в центре проведения экзамена в день проведения ДЭ на основании документов, удостоверяющих личность.

Лица, указанные в пунктах 4.2.3 и 4.2.4, обязаны:

- соблюдать установленные требования по охране труда и производственной безопасности, выполнять указания технического эксперта по соблюдению указанных требований;
- пользоваться средствами связи исключительно по вопросам служебной необходимости, в том числе в рамках оказания необходимого содействия главному эксперту;

- не мешать и не взаимодействовать с обучающимися проходящими ГИА в форме ДЭ при выполнении ими заданий, не передавать им средства связи и хранения информации, иные предметы и материалы.

5.2.5 Члены ГЭК, не входящие в состав экспертной группы, наблюдают за ходом проведения ДЭ и вправе сообщать главному эксперту о выявленных фактах нарушения процедуры проведения ДЭ.

5.2.6 Члены экспертной группы осуществляют оценку выполнения заданий ДЭ самостоятельно.

5.2.7 Главный эксперт вправе давать указания по организации и проведению ДЭ, обязательные для выполнения лицами, привлеченными к проведению ДЭ, и обучающимся проходящим ГИА в форме ДЭ, удалять из центра проведения экзамена лиц, допустивших грубое нарушение процедуры проведения ДЭ, требований охраны труда и безопасности производства, а также останавливать, приостанавливать и возобновлять проведение ДЭ при возникновении необходимости устранения грубых нарушений порядка проведения ДЭ, требований охраны труда и производственной безопасности.

5.2.8 Главный эксперт может делать заметки о ходе демонстрационного экзамена.

5.2.9 Главный эксперт обязан находиться в центре проведения экзамена до окончания ДЭ, осуществлять контроль за соблюдением лицами, привлеченными к проведению ДЭ, обучающимися требований процедуры проведения ДЭ.

5.2.10 При привлечении медицинского работника техникум на базе которого будет организован центр проведения экзамена, обязан организовать помещение, оборудованное для оказания первой помощи и первичной медико-санитарной помощи.

5.2.11 Технический эксперт вправе:

- наблюдать за ходом проведения ДЭ;
- давать разъяснения и указания лицам, привлеченным к проведению ДЭ, обучающимся по вопросам соблюдения требований охраны труда и производственной безопасности;
- сообщать главному эксперту о выявленных случаях нарушений лицами, привлеченными к проведению ДЭ, обучающимися проходящими ГИА в форме ДЭ требований охраны труда и требований производственной безопасности, а также невыполнения такими лицами указаний технического эксперта, направленных на обеспечение соблюдения требований охраны труда и производственной безопасности;
- останавливать в случаях, требующих немедленного решения, в целях охраны жизни и здоровья лиц, привлеченных к проведению ДЭ, обучающихся проходящих ГИА в форме ДЭ действия обучающихся по

выполнению заданий, действия других лиц, находящихся в центре проведения экзамена с уведомлением главного эксперта.

5.2.12 Образовательная организация обязана не позднее чем за один рабочий день до дня проведения ДЭ уведомить главного эксперта об участии в проведении ДЭ тьютора (ассистента).

5.2.14 Обучающийся проходящий ГИА в форме ДЭ вправе:

- пользоваться оборудованием центра проведения экзамена, необходимыми материалами, средствами обучения и воспитания в соответствии с требованиями КОД, задания ДЭ;

- получать разъяснения технического эксперта по вопросам безопасной и бесперебойной эксплуатации оборудования центра проведения экзамена;

- получить копию задания ДЭ на бумажном носителе;

5.2.15. Обучающийся проходящий ГИА в форме ДЭ обязаны:

- во время проведения ДЭ не пользоваться и не иметь при себе средства связи, носители информации, средства ее передачи и хранения, если это прямо не предусмотрено КОД;

- во время проведения ДЭ использовать только средства обучения и воспитания, разрешенные КОД;

- во время проведения ДЭ не взаимодействовать с другими обучающимися, экспертами, иными лицами, находящимися в центре проведения экзамена, если это не предусмотрено КОД.

5.2.16. Обучающийся проходящий ГИА в форме ДЭ могут иметь при себе лекарственные средства и питание, прием которых осуществляется в специально отведенном для этого помещении согласно плану проведения ДЭ за пределами центра проведения экзамена.

5.2.17. Допуск обучающихся проходящих ГИА в форме ДЭ к выполнению заданий осуществляется при условии обязательного их ознакомления с требованиями охраны труда и производственной безопасности.

5.3 Процедура проведения демонстрационного экзамена

5.3.1. В соответствии с планом проведения ДЭ главный эксперт ознакомливает обучающихся с заданиями, передает им копии заданий ДЭ.

5.3.2 После ознакомления с заданиями ДЭ обучающиеся занимают свои рабочие места в соответствии с протоколом распределения рабочих мест.

5.3.3 После того, как все обучающиеся и лица, привлеченные к проведению ДЭ, займут свои рабочие места в соответствии с требованиями охраны труда и производственной безопасности, главный эксперт объявляет о начале ДЭ.

Время начала ДЭ фиксируется в протоколе проведения ДЭ, составляемом главным экспертом по каждой экзаменационной группе.

После объявления главным экспертом начала ДЭ обучающиеся приступают к выполнению заданий ДЭ.

5.3.4 ДЭ проводится при неукоснительном соблюдении обучающимися, лицами, привлеченными к проведению ДЭ, требований охраны труда и производственной безопасности, а также с соблюдением принципов объективности, открытости и равенства обучающихся.

5.3.5 Центры проведения экзамена могут быть оборудованы средствами видеонаблюдения, позволяющими осуществлять видеозапись хода проведения ДЭ.

5.3.6 Видеоматериалы о проведении ДЭ в случае осуществления видеозаписи подлежат хранению в техникуме не менее одного года с момента завершения ДЭ.

5.3.7 Явка обучающегося, его рабочее место, время завершения выполнения задания ДЭ подлежат фиксации главным экспертом в протоколе проведения ДЭ.

5.3.8 В случае удаления из центра проведения экзамена обучающегося, лица, привлеченного к проведению ДЭ, или присутствующего в центре проведения экзамена, главным экспертом составляется акт об удалении. Результаты ГИА обучающегося, удаленного из центра проведения экзамена, аннулируются ГЭК, и такой обучающийся признается ГЭК не прошедшим ГИА по неуважительной причине.

5.3.9 Главный эксперт сообщает обучающемуся о течении времени выполнения задания ДЭ каждые 60 минут, а также за 30 и 5 минут до окончания времени выполнения задания.

5.3.10 После объявления главным экспертом окончания времени выполнения заданий обучающиеся прекращают любые действия по выполнению заданий ДЭ.

Технический эксперт обеспечивает контроль за безопасным завершением работ обучающихся в соответствии с требованиями производственной безопасности и требованиями охраны труда.

5.3.11 Обучающийся по собственному желанию может завершить выполнение задания досрочно, уведомив об этом главного эксперта.

5.3.12 Результаты выполнения обучающимися заданий ДЭ подлежат фиксации экспертами экспертной группы в соответствии с требованиями КОД задания ДЭ.

5.3 Оценка результатов выполнения демонстрационного экзамена

5.3.1 Результаты проведения ГИА в форме защиты ВКР в виде ДЭ оцениваются с проставлением одной из отметок: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно» - и объявляются в тот же день после оформления протоколов заседаний ГЭК.

Таблица «Схема перевода результатов демонстрационного экзамена из стобалльной шкалы в пятибалльную»: КОД

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

5.3.2 Процедура оценивания результатов выполнения заданий ДЭ осуществляется членами экспертной группы по 100-балльной системе в соответствии с требованиями комплекта оценочной документации.

5.3.3 Баллы выставляются в протоколе проведения ДЭ, который подписывается каждым членом экспертной группы и утверждается главным экспертом после завершения экзамена для экзаменационной группы.

При выставлении баллов присутствует член ГЭК, не входящий в экспертную группу, присутствие других лиц запрещено.

Подписанный членами экспертной группы и утвержденный главным экспертом протокол проведения ДЭ далее передается в ГЭК для выставления оценок по итогам ГИА.

Оригинал протокола проведения ДЭ передается на хранение в техникуме в составе архивных документов.

5.3.4 Статус победителя, призера чемпионатов профессионального мастерства, проведенных Агентством (Союзом «Агентство развития профессиональных сообществ и рабочих кадров «Молодые профессионалы (Ворлдскиллс Россия)» либо международной организацией «WorldSkills International», в том числе «WorldSkills Europe» и «WorldSkills Asia», и участника национальной сборной России по профессиональному мастерству по стандартам «Ворлдскиллс» обучающийся а по профилю осваиваемой образовательной программы СПО засчитывается в качестве оценки «отлично» по демонстрационному экзамену в рамках проведения ГИА по данной образовательной программе СПО.

6 Порядок подачи и рассмотрения апелляций

6.1 По результатам ГИА обучающийся имеет право подать в апелляционную комиссию письменную апелляцию о нарушении, по его мнению, порядка проведения и (или) несогласии с результатами ГИА (далее - апелляция).

6.2. Апелляция подается лично обучающимся или родителями (законными представителями) несовершеннолетнего обучающегося в апелляционную комиссию техникума.

Апелляция о нарушении Порядка подается непосредственно в день проведения ГИА, в том числе до выхода из центра проведения экзамена.

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

6.3. Апелляция рассматривается апелляционной комиссией не позднее трех рабочих дней с момента ее поступления.

6.4. Состав апелляционной комиссии утверждается техникумом одновременно с утверждением состава ГЭК.

Апелляционная комиссия состоит из председателя апелляционной комиссии, не менее пяти членов апелляционной комиссии и секретаря апелляционной комиссии из числа педагогических работников техникума, не входящих в данный учебный год в состав ГЭК. Председателем апелляционной комиссии может быть назначено лицо из числа руководителей или заместителей руководителей организаций, осуществляющих образовательную деятельность, соответствующую области профессиональной деятельности, к которой готовятся обучающиеся, представителей организаций-партнеров или их объединений, включая экспертов, при условии, что направление деятельности данных представителей соответствует области профессиональной деятельности, к которой готовятся обучающиеся, при условии, что такое лицо не входит в состав ГЭК.

6.5. Апелляция рассматривается на заседании апелляционной комиссии с участием не менее двух третей ее состава.

На заседание апелляционной комиссии приглашается председатель соответствующей ГЭК, а также главный эксперт при проведении ГИА в форме ДЭ.

При проведении ГИА в форме ДЭ по решению председателя апелляционной комиссии к участию в заседании комиссии могут быть также привлечены члены экспертной группы, технический эксперт.

По решению председателя апелляционной комиссии заседание апелляционной комиссии может пройти с применением средств видео, конференц-связи, а равно посредством предоставления письменных пояснений по поставленным апелляционной комиссией вопросам.

Обучающийся, подавший апелляцию, имеет право присутствовать при рассмотрении апелляции.

С несовершеннолетним обучающимся имеет право присутствовать один из родителей (законных представителей).

Указанные лица должны при себе иметь документы, удостоверяющие личность.

6.6. Рассмотрение апелляции не является передачей ГИА.

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

– об отклонении апелляции, если изложенные в ней сведения о нарушениях не подтвердились и (или) не повлияли на результат ГИА;

– об удовлетворении апелляции, если изложенные в ней сведения о допущенных нарушениях подтвердились и повлияли на результат ГИА.

В последнем случае результаты проведения ГИА подлежат аннулированию, в связи с чем протокол о рассмотрении апелляции не позднее следующего рабочего дня передается в ГЭК для реализации решения апелляционной комиссии. Обучающемуся предоставляется возможность пройти ГИА в дополнительные сроки, установленные техникумом без отчисления такого обучающегося из образовательной организации в срок не более четырех месяцев после подачи апелляции.

6.8. В случае рассмотрения апелляции о несогласии с результатами ГИА, полученными при прохождении демонстрационного экзамена, секретарь ГЭК не позднее следующего рабочего дня с момента поступления апелляции направляет в апелляционную комиссию протокол заседания ГЭК, протокол проведения ДЭ, письменные ответы обучающегося (при их наличии), результаты работ обучающегося, подавшего апелляцию, видеозаписи хода проведения ДЭ (при наличии).

6.9. В случае рассмотрения апелляции о несогласии с результатами ГИА, полученными при защите ДП, секретарь ГЭК не позднее следующего рабочего дня с момента поступления апелляции направляет в апелляционную комиссию ДП, протокол заседания ГЭК.

6.10. В случае рассмотрения апелляции о несогласии с результатами ГИА, полученными при сдаче государственного экзамена, секретарь ГЭК не позднее следующего рабочего дня с момента поступления апелляции направляет в апелляционную комиссию протокол заседания ГЭК, письменные ответы обучающегося (при их наличии).

6.11. В результате рассмотрения апелляции о несогласии с результатами ГИА апелляционная комиссия принимает решение об отклонении апелляции и сохранении результата ГИА либо об удовлетворении апелляции и выставлении иного результата ГИА. Решение апелляционной комиссии не позднее следующего рабочего дня передается в ГЭК. Решение апелляционной комиссии является основанием для аннулирования ранее выставленных результатов ГИА обучающегося и выставления новых результатов в соответствии с мнением апелляционной комиссии.

6.12. Решение апелляционной комиссии принимается простым большинством голосов. При равном числе голосов голос председательствующего на заседании апелляционной комиссии является решающим.

Решение апелляционной комиссии доводится до сведения подавшего апелляцию обучающегося в течение трех рабочих дней со дня заседания апелляционной комиссии.

6.13. Решение апелляционной комиссии является окончательным и пересмотру не подлежит.

6.14. Решение апелляционной комиссии оформляется протоколом, который подписывается председателем (заместителем председателя) и секретарем апелляционной комиссии и хранится в архиве техникума.

7 Хранение выпускных квалификационных работ

Выполненные студентами ВКР(ДП) хранятся после их защиты в техникуме не менее пяти лет. По истечении указанного срока вопрос о дальнейшем хранении решается организуемой по приказу директора техникума комиссией, которая представляет предложения о списании ВКР(ДП).

Списание ВКР(ДП) оформляется соответствующим актом.

Лучшие ВКР(ДП), представляющие учебно-методическую ценность, могут быть использованы в качестве учебных пособий в кабинетах техникума.

По запросу предприятия, учреждения, организации директор техникума имеет право разрешить снимать копии дипломных проектов студентов. При наличии в ВКР изобретения или рационализаторского предложения разрешение на копию выдается только после оформления (в установленном порядке) заявки на авторские права обучающегося.

Изделия и результаты творческой деятельности по решению государственной экзаменационной комиссии могут не подлежать хранению в течение пяти лет. Они могут быть использованы в качестве учебных пособий, реализованы через выставки-продажи и т.п.

**КОМИТЕТ ОБРАЗОВАНИЯ, НАУКИ И МОЛОДЕЖНОЙ ПОЛИТИКИ
ВОЛГОГРАДСКОЙ ОБЛАСТИ**

**государственное бюджетное профессиональное образовательное учреждение
«Волгоградский строительный техникум»
(ГБПОУ «Волгоградский строительный техникум»)**

ПРОТОКОЛ № _____

Заседания государственной экзаменационной комиссии

от 2__ июня 202__ г.

Председатель ГЭК: _____

Заместитель председателя ГЭК: _____

Члены ГЭК:

Член ГЭК _____

Член ГЭК _____

Секретарь ГЭК _____

СЛУШАЛИ:

1. _____ обучающегося

ФИО

специальности _____

с защитой выпускной квалификационной работы(дипломный проект)

на тему: _____,

соответствующей содержанию _____ профессиональных модулей, входящих в образовательную программу среднего профессионального образования по специальности _____

ПМ. 0 _____:

ПМ. 0 _____

Руководитель - _____

Консультанты:

_____	—	_____
_____	—	_____
_____	—	_____
_____	—	_____

Нормоконтроль – _____

В ГЭК представлены следующие материалы:

а) сводные ведомости итогов обучения обучающихся группы _____;

б) сводные ведомости экзаменов (квалификационных) группы _____;

в) пояснительная записка на _____ листах;

г) графическая часть на _____ листах;

д) объемный макет, наглядное пособие, выполненное задание по оборудованию учебного кабинета (необходимое подчеркнуть) по теме

2. Секретарь ГЭК зачитал отзыв и рецензию на выпускную квалификационную работу, (дипломный проект)

Оценка руководителя _____

Оценка рецензента _____

3. Вопросы, заданные обучающемуся после доклада:

№ п/п	Содержание вопроса	Автор вопроса

Общая характеристика ответов обучающегося на вопросы членов ГЭК

1. Учитывая уровень самостоятельной подготовки (написание) обучающимся выпускной квалификационной работы (дипломный проект), его защиту, ответы на вопросы членов ГЭК, члены ГЭК сделали вывод об уровне знаний обучающегося в рамках выбранной темы, а также сформированности его профессиональных умений и навыков, ГЭК постановила:

оценить защиту выпускной квалификационной работы(дипломный проект) на оценку _____.

Результаты голосования: «за»_____, «против»_____, «воздержались»_____.

Председатель ГЭК _____
(Подпись) (Инициалы, фамилия)

Заместитель председателя ГЭК _____
(Подпись) (Инициалы, фамилия)

Члены ГЭК:

Член ГЭК _____
(Подпись) (Инициалы, фамилия)

Секретарь ГЭК _____
(Подпись) (Инициалы, фамилия)

ОЦЕНКИ

за защиту выпускной квалификационной работы (дипломный проект)

Член ГЭК _____
(фамилия, инициалы)

Дата « ____ » _____ 202__г

№ п/п	Фамилия, имя, отчество обучающихся	Оценка

Член ГЭК _____
(подпись)

СВОДНАЯ ВЕДОМОСТЬ

оценок защиты выпускной квалификационной работы (дипломный проект)
обучающихся ГБПОУ «Волгоградский строительный техникум» по специальности

_____ (код, наименование)

« _____ » _____ 202_____ г.

№ п/п	Фамилия, имя, отчество обучающихся	Оценки					Общая оценка
1							
2							
3							
4							
5							
6							
7							
8							

Председатель ГЭК _____

(Подпись)

_____ (Инициалы, фамилия)

Заместитель председателя ГЭК _____

(Подпись)

_____ (Инициалы, фамилия)

Члены ГЭК:

Член ГЭК _____

(Подпись)

_____ (Инициалы, фамилия)

Секретарь ГЭК _____

(Подпись)

_____ (Инициалы, фамилия)

ПРОТОКОЛ
проведения демонстрационного экзамена

Вид аттестации: _____

Уровень ДЭ (при проведении ДЭ как формы ГИА): _____

Образовательная организация: _____

Профессия/специальность: _____

Главный эксперт: _____

ID _____

КОД _____

Вариант _____

Смена _____

Мы, нижеподписавшиеся, подтверждаем корректность выставленных оценок.

№ п.п.	ФИО участников	Рабочее место	Время начала выполнения задания	Время завершения выполнения задания	Итоговый балл
1					
2					
3					
4					
5					

Выставление баллов осуществлено в присутствии члена ГЭК

_____ (ФИО) _____ (подпись)

Экспертная группа:

_____ (ФИО) _____ (подпись)

_____ (ФИО) _____ (подпись)

_____ (ФИО) _____ (подпись)

Дата: _____

Утверждаю:
Главный эксперт: _____ (подпись)

Документ сформирован: _____

**КОМИТЕТ ОБРАЗОВАНИЯ, НАУКИ И МОЛОДЕЖНОЙ ПОЛИТИКИ
ВОЛГОГРАДСКОЙ ОБЛАСТИ**

**государственное бюджетное профессиональное образовательное учреждение
«Волгоградский строительный техникум»
(ГБПОУ «Волгоградский строительный техникум»)**

**ИТОГОВЫЙ ПРОТОКОЛ ГИА № _____
(КНИГА ПРОТОКОЛОВ № __)**

Заседания государственной экзаменационной комиссии в целях определения в рамках ГИА соответствия результатов освоения обучающимися имеющей государственную аккредитацию образовательной программы среднего профессионального образования по специальности _____ соответствующим требованиям ФГОС СПО по специальности _____ и присвоению квалификации и выдаче дипломов о среднем профессиональном образовании обучающимся группы _____.

«__» _____ 202__ г.

Присутствовали: Председатель ГЭК _____
Заместитель председателя ГЭК _____

Члены ГЭК:

Член ГЭК _____
Секретарь ГЭК _____

1. Утвердить результаты демонстрационного экзамена _____ уровня по компетенции _____ в рамках ГИА, полученные переводом баллов обучающегося за выполнение практического задания в условиях смоделированных производственных процессов в оценки по пятибалльной шкале, в соответствии с Таблицей «Схема перевода результатов демонстрационного экзамена из стобалльной шкалы в пятибалльную», утвержденной новой редакцией программы ГИА по специальности _____ (приказ директора ГБПОУ «Волгоградский строительный техникум» от _____ № _____)

№ п /п	Фамилия, имя, отчество обучающихся	Итоговый балл согласно протоколу проведения демонстрационного экзамена	Отношение полученного количества баллов к максимально	Оценка ГИА в форме защиты выпускной квалификационной работы в виде

		ID____ КОД ____	возможному (в процентах)	демонстрационного экзамена
1				
2				
3				
4				
5				
6				
7				
8				
9				
0	1			
1	1			
2	1			

Особое мнение: _____

Результаты голосования: «за» _____, «против» _____,
«воздержались» _____.

2. Рассмотрев итоговые оценки успеваемости за курс обучения, оценки ГИА в форме защиты выпускной квалификационной работы, которая выполнялась в виде демонстрационного экзамена; оценки обучающихся за защиту выпускной квалификационной работы, которая выполнялась в виде дипломного проекта ГЭК определила соответствие результатов освоения обучающимися имеющей государственную аккредитацию образовательной программы среднего профессионального образования по специальности _____ требованиям ФГОС СПО по специальности _____ и постановила и утвердить следующие оценки за ГИА:

2. 1. Присвоить квалификацию « _____ » и выдать дипломы о среднем профессиональном образовании с отличием следующим обучающимся:

№ п/п	Фамилия, имя, отчество обучающихся	Оценка за ГИА в форме защиты выпускной квалификационной работы		Итоговая оценка за ГИА в форме защиты выпускной квалифика ционной	Присвоен ная квалифика ция
		Демонстраци онный экзамен	Дипломный проект		

				работы	
1					
2					
3					
4					
5					

Результаты голосования: «за» _____, «против» _____, «воздержались» _____.

2.2. Присвоить квалификацию « _____ » и выдать дипломы о среднем профессиональном образовании следующим обучающимся:

№ п/п	Фамилия, имя, отчество обучающихся	Оценка за ГИА в форме защиты выпускной квалификационной работы		Итоговая оценка за ГИА в форме защиты выпускной квалификационной работы	Присвоенная квалификация
		Демонстрационный экзамен	Дипломный проект		
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					

Результаты голосования: «за» _____, «против» _____, «воздержались» _____.

Председатель ГЭК _____

(Подпись)

(Инициалы, фамилия)

Члены ГЭК:

Секретарь ГЭК _____

(Подпись)

(Инициалы, фамилия)

РЕШЕНИЕ

Государственной экзаменационной комиссии
ГБПОУ «Волгоградский строительный техникум»
от «2_» _____ 202_ г.

1. Присвоить квалификацию «_____» по специальности _____ обучающимся группы _____ формы обучения ГБПОУ «Волгоградский строительный техникум», прошедшим ГИА и показавшим соответствие результатов освоения имеющей государственную аккредитацию образовательной программы среднего профессионального образования по специальности _____ требованиям ФГОС СПО по специальности _____

Присвоить квалификацию «_____» и выдать дипломы о среднем профессиональном образовании с отличием следующим обучающимся:

№ п/п	Фамилия, имя, отчество обучающихся	Оценка за ГИА в форме защиты выпускной квалификационной работы		Итоговая оценка за ГИА в форме защиты выпускной квалификационной работы	Присвоенная квалификация
		Демонстрационный экзамен	Дипломный проект		
1					
2					
3					
4					
5					

2. Присвоить квалификацию «_____» и выдать дипломы о среднем профессиональном образовании следующим обучающимся:

№ п/п	Фамилия, имя, отчество обучающихся	Оценка за ГИА в форме защиты выпускной квалификационной работы		Итоговая оценка за ГИА в форме защиты выпускной квалификационной работы	Присвоенная квалификация
		Демонстрационный экзамен	Дипломный проект		
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					

Председатель ГЭК _____

(Подпись)

(Инициалы, фамилия)

Члены ГЭК:

Секретарь ГЭК

(Подпись)

(Инициалы, фамилия)

**ПРИМЕРНАЯ ТЕМАТИКА ДИПЛОМНЫХ ПРОЕКТОВ
на 202__ год**

- 1 Проектирование системы защиты компьютерной информации организации.
- 2 Организация программной защиты информации учета кадров на предприятии.
- 3 Защита информации в локальной вычислительной сети организации при использовании сервисов и ресурсов сетей общего пользования.
- 4 Защита информации в локальной вычислительной сети предприятия.
- 5 Организация режима защиты конфиденциальной информации в экономическом отделе предприятия. 6 Анализ системы защиты электронного документооборота предприятия.
- 7 Разработка защищённой автоматизированной информационной системы.
- 8 Разработка политики информационной безопасности организации.
- 9 Проектирование системы видеонаблюдения для магазина.
- 10 Защита информации в локальной вычислительной сети предприятия на основе контроллера домена.
- 11 Организация программной защиты информации предприятия в приложении «1С: Предприятие»
- 12 Защита информации в локальной вычислительной сети предприятия при использовании сети Интернет.
- 13 Разработка системы защиты информации АИС «Пропуск» для администрации г. Ливны.
- 14 Анализ системы обеспечения информационной безопасности АИС «Кадры» и разработка предложений по её совершенствованию.
- 15 Анализ системы обеспечения информационной безопасности рабочих станций локальной вычислительной сети предприятия.
- 16 Организация программной защиты информации организации в приложении «1С: Бухгалтерия»
- 17 Анализ системы обеспечения информационной безопасности учёта продукции для организации товародвижения готовой продукции.
- 18 Организация системы защиты автоматизированного учёта движения продукции.
- 19 Организация системы защиты автоматизированной системы пропускконтроля администрации Ливенского района.
- 20 Организация системы защиты локальной вычислительной сети организации с модулем Wi-Fi.
- 21 Анализ системы обеспечения информационной безопасности автоматизированного заполнения первичной документации.
- 22 Обеспечение безопасности информационной системы тестирования уровня знаний
- 23 Обеспечение безопасности информационной системы АПС предприятия
- 24 Обеспечение безопасности информационной системы образовательного учреждения
- 25 Обеспечение безопасности информационной системы учета средств компьютерной техники

Перечень учебной литературы, нормативно-правовых актов**Основная литература:**

1. Беленький, В. Г. Беспроводные сети передачи данных: учебное пособие для СПО / В. Г. Беленький, А. В. Лошкарев. — Саратов: Профобразование, 2022. — 98 с. — ISBN 978-5-4488-1499-0. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/125572.html>
2. Внуков, А. А. Основы информационной безопасности: защита информации: учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2023. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/518006>
3. Гостев, И. М. Операционные системы: учебник и практикум для среднего профессионального образования / И. М. Гостев. — 2-е изд., испр. И доп. — Москва: Издательство Юрайт, 2023. — 164 с. — (Профессиональное образование). — ISBN 978-5-534-04951-0. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/514426>
4. Зиангирова, Л. Ф. Инфокоммуникационные системы и сети: учебное пособие для СПО / Л. Ф. Зиангирова. — Саратов: Профобразование, Ай Пи Ар Медиа, 2019. — 128 с. — ISBN 978-5-4488-0302-4, 978-5-4497-0183-1. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/85806.html>
5. Извозчикова, В. В. Эксплуатация информационных систем : учебное пособие для СПО / В. В. Извозчикова. — Саратов: Профобразование, 2019. — 136 с. — ISBN 978-5-4488-0355-0. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/86210.html>
6. Ильин, М. Е. Криптографическая защита информации в объектах информационной инфраструктуры: учеб. для студ. учреждений сред. проф. образования / М. Е. Ильин, Т. И. Калинин, В. Н. Пржегорлинский ; под ред. В. Н. Пржегорлинского. — Москва: Академия, 2020. — 288 с. — URL: <https://www.academia-moscow.ru/catalogue/4831/444518/>
7. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва: Издательство Юрайт, 2023. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/519364>
8. Мэйволд, Э. Безопасность сетей: учебное пособие для СПО / Э. Мэйволд. — Саратов: Профобразование, 2021. — 571 с. — ISBN 978-5-4488-0990-3. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/102183.html>
9. Организационное и правовое обеспечение информационной безопасности: учебник и практикум для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов; ответственные редакторы Т. А. Полякова, А. А. Стрельцов. — Москва : Издательство Юрайт, 2023. — 325 с. — (Профессиональное образование). — ISBN 978-5-534-00843-2.

- Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/512861>
10. Скрипник, Д. А. Общие вопросы технической защиты информации: учебное пособие / Д. А. Скрипник. — 3-е изд. — Москва, Саратов: Интернет Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 424 с. — ISBN 978-5-4497-0336-1. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/89451.html>
 11. Советов, Б. Я. Базы данных: учебник для среднего профессионального образования / Б. Я. Советов, В. В. Цехановский, В. Д. Чертовской. — 3-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2023. — 420 с. — (Профессиональное образование). — ISBN 978-5-534-09324-7. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/514585>
 12. Солонская, О. И. Средства защиты информации: учебное пособие для СПО / О. И. Солонская. — Саратов: Профобразование, 2022. — 88 с. — ISBN 978-5-4488-1504-1. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/125578.html>
 13. Технологии защиты информации в компьютерных сетях: учебное пособие для СПО / Н. А. Руденков, А. В. Пролетарский, Е. В. Смирнова, А. М. Суровов. — Саратов: Профобразование, 2021. — 368 с. — ISBN 978-5-4488-1014-5. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/102207.html>
 14. Фороузан, Б. А. Криптография и безопасность сетей: учебное пособие для СПО / Б. А. Фороузан; под редакцией А. Н. Берлина. — Саратов: Профобразование, 2021. — 776 с. — ISBN 978-5-4488-0999-6. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/102192.html> Дополнительная литература:
 15. Конституция Российской Федерации (с гимном России). Новая редакция. - Москва: Проспект, 2021. - 64 с. 16. О безопасности. Федеральный закон от 28.12.2010 N 390-ФЗ (ред. От 09.11.2020) // СПС КонсультантПлюс.
 16. О персональных данных. Федеральный закон от 27.07.2006 N 152-ФЗ 2. (ред. от 14.07.2022) // СПС КонсультантПлюс.
 17. О техническом регулировании. Федеральный закон от 27.12.2002 N 184-ФЗ (ред. от 02.07.2021) (с изм. и доп., вступ. в силу с 23.12.2021) // СПС КонсультантПлюс.
 18. Об информации, информационных технологиях и о защите информации. Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 29.12.2022) (с 30 изм. и доп., вступ. в силу с 09.01.2023) // СПС КонсультантПлюс.
 19. Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну. Приказ ФАПСИ от 13.06.2001 N 152 (Зарегистрировано в Минюсте РФ 06.08.2001 N 2848) // СПС КонсультантПлюс.
 20. Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005). Приказ ФСБ РФ от 09.02.2005 N 66 (ред. от 12.04.2010) (Зарегистрировано в Минюсте РФ 03.03.2005 N 6382) // СПС КонсультантПлюс.

21. ГОСТ Р 52447-2005. Защита информации. Техника защиты информации. Номенклатура показателей качества (утв. Приказом Ростехрегулирования от 29.12.2005 N 448-ст) // СПС КонсультантПлюс
22. ГОСТ Р ИСО/МЭК 13335-1-2006. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий" (утв. и введен в действие Приказом Ростехрегулирования от 19.12.2006 N 317-ст) // СПС КонсультантПлюс.
23. ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования (принят и введен в действие Постановлением Госстандарта РФ от 09.02.1995 N 49) // СПС КонсультантПлюс.
24. Меры защиты информации в государственных информационных системах. Методический документ (утв. ФСТЭК России 11.02.2014) // СПС КонсультантПлюс.
25. Авдошин, С. М. Технологии и продукты Microsoft в обеспечении информационной безопасности: учебное пособие для СПО / С. М. Авдошин, А. А. Савельева, В. А. Сердюк. — Саратов: Профобразование, 2021. — 431 с. — ISBN 978-5-4488-1015-2. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/102208.html>
26. Гордеев, С. И. Организация баз данных в 2 ч. Часть 1: учебник для среднего профессионального образования / С. И. Гордеев, В. Н. Волошина. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2023. — 310 с. — (Профессиональное образование). — ISBN 978-5-534-11626-7. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/518510>
27. Гордеев, С. И. Организация баз данных в 2 ч. Часть 2: учебник для среднего профессионального образования / С. И. Гордеев, В. Н. Волошина. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2023. — 513 с. — (Профессиональное образование). — ISBN 978-5-534-11625-0. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/518511>
28. Грошев, А. С. Основы работы с базами данных: учебное пособие для СПО / А. С. Грошев. — Саратов: Профобразование, 2021. — 255 с. — ISBN 978-5-4488-1006-0. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/102199.html>
29. Дибров, М. В. Компьютерные сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 1: учебник и практикум для среднего профессионального образования / М. В. Дибров. — Москва: Издательство Юрайт, 2023. — 333 с. — (Профессиональное образование). — ISBN 978-5-534-04638-0. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/513518>
30. Дибров, М. В. Компьютерные сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 2: учебник и практикум для среднего профессионального образования / М. В. Дибров. — Москва: Издательство Юрайт, 2023. — 351 с. — (Профессиональное образование). — ISBN 978-5-534-04635-9. — Текст:

- электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/514019>
31. Епишкина, А. В. Нормативное регулирование в области защиты информации. Конспект лекций: учебное пособие / А. В. Епишкина, С. В. Запечников. — Москва: Национальный исследовательский ядерный университет «МИФИ», 2021. — 116 с. — ISBN 978-5-7262-2807-5. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/125496.html>
 32. Илюшечкин, В. М. Основы использования и проектирования баз данных: учебник для среднего профессионального образования / В. М. Илюшечкин. — испр. и доп. — Москва: Издательство Юрайт, 2023. — 213 с. — (Профессиональное образование). — ISBN 978-5-534-01283-5. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/513827>
 33. Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения: учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва: Издательство Юрайт, 2023. — 342 с. — (Профессиональное образование). — ISBN 978-5-534-10671-8. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/518005>
 34. Киренберг, А. Г. Информационная безопасность современных операционных систем: учебное пособие / А. Г. Киренберг. — Кемерово: Кузбасский государственный технический университет имени Т.Ф. Горбачева, 2022. — 138 с. — ISBN 978-5-00137-320-9. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/128393.html>
 35. Киренберг, А. Г. Системное администрирование и информационная безопасность сетей ЭВМ: учебное пособие / А. Г. Киренберг. — Кемерово: Кузбасский государственный технический университет имени Т.Ф. Горбачева, 2022. — 119 с. — ISBN 978-5-00137-292-9. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/128406.html>
 36. Молдованова, О. В. Информационные системы и базы данных: учебное пособие для СПО / О. В. Молдованова. — Саратов: Профобразование, 2021. — 177 с. — ISBN 978-5-4488-1177-7. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/106617.html>
 37. Нестеров, С. А. Базы данных: учебник и практикум для среднего профессионального образования / С. А. Нестеров. — Москва: Издательство Юрайт, 2023. — 230 с. — (Профессиональное образование). — ISBN 978-5-534-11629-8. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/518507>
 38. Никифоров, С. Н. Методы защиты информации. Защищенные сети: учебное пособие / С. Н. Никифоров. — 2-е изд., стер. — Санкт-Петербург: Лань, 2021. — 96 с. — ISBN 978-5-8114-8123-1. — Текст: электронный // Лань: электронно-библиотечная система. — URL: <https://e.lanbook.com/book/171868>
 40. Олифер, В. Г. Основы сетей передачи данных: учебное пособие для СПО / В. Г. Олифер, Н. А. Олифер. — Саратов: Профобразование, 2021. — 219 с. — ISBN 978-5-4488-1007-7. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/102200.html>
 39. Операционные системы: учебное пособие для СПО / составители И. В. Винокуров. — Саратов, Москва: Профобразование, Ай Пи Ар Медиа, 2022. —

- 127 с. — ISBN 978-5-4488-1441-9, 978-5-4497-1444-2. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/115697.html>
40. Операционные системы. Программное обеспечение: учебник / составитель Т. П. Куль. — Санкт-Петербург: Лань, 2020. — 248 с. — ISBN 978-5-8114-4290-4. — Текст: электронный // Лань: электронно-библиотечная система. — URL: <https://e.lanbook.com/book/131045>
41. Сети и телекоммуникации: учебник и практикум для среднего профессионального образования / К. Е. Самуйлов [и др.]; под редакцией К. Е. Самуйлова, И. А. Шалимова, Д. С. Кулябова. — Москва: Издательство Юрайт, 2023. — 363 с. — (Профессиональное образование). — ISBN 978-5-9916-0480-2. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/517817>
42. Стасышин, В. М. Базы данных: технологии доступа: учебное пособие для среднего профессионального образования / В. М. Стасышин, Т. Л. Стасышина. — 2-е изд., испр. и доп. — Москва: Издательство Юрайт, 2023. — 164 с. — (Профессиональное образование). — ISBN 978-5-534-09888-4. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/516927>
43. Суворова, Г. М. Основы информационной безопасности: учебное пособие для СПО / Г. М. Суворова. — Саратов: Профобразование, 2021. — 135 с. — ISBN 978-5-4488-1294-1. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/108005.html>
44. Тумбинская, М. В. Комплексное обеспечение информационной безопасности на предприятии: учебник / М. В. Тумбинская, М. В. Петровский. — Санкт-Петербург: Лань, 2022. — 344 с. — ISBN 978-5-8114-3940-9. — Текст: электронный // Лань: электронно-библиотечная система. — URL: <https://e.lanbook.com/book/207095>
45. Тумбинская, М. В. Защита информации на предприятии: учебное пособие / М. В. Тумбинская, М. В. Петровский. — Санкт-Петербург: Лань, 2020. — 184 с. — ISBN 978-5-8114-4291-1. — Текст: электронный // Лань: электроннобиблиотечная система. — URL: <https://e.lanbook.com/book/130184>
46. Фомин, Д. В. Информационная безопасность: учебное пособие для СПО / Д. В. Фомин. — Саратов, Москва: Профобразование, Ай Пи Ар Медиа, 2022. — 218 с. — ISBN 978-5-4488-1351-1, 978-5-4497-1565-4. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/118458.html>
47. Фомин, Д. В. Защита информации: специализированные аттестованные программные и программно-аппаратные средства: практикум / Д. В. Фомин. — Саратов: Вузовское образование, 2021. — 218 с. — ISBN 978-5-4487-0795-7. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/110329.html>
48. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — 2-е изд. — Саратов: Профобразование, 2019. — 702 с. — ISBN 978-5-4488-0070-2. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/87995.html>
49. Швецов, В. И. Базы данных: учебное пособие для СПО / В. И. Швецов. — Саратов: Профобразование, 2019. — 219 с. — ISBN 978-5-4488-0357-4. — Текст:

электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/86192.html>

50. Щербак, А. В. Информационная безопасность: учебник для среднего профессионального образования / А. В. Щербак. — Москва: Издательство Юрайт, 2023. — 259 с. — (Профессиональное образование). — ISBN 978-5-534-15345-3. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/519614>

Титульный лист выпускной квалификационной работы (дипломный проект)

**Форма бланка индивидуального задания на закрепление темы выпускной
квалификационной работы (дипломный проект)**

**Форма заявления на закрепление темы выпускной квалификационной работы
(дипломный проект)**

**График проверки хода выполнения выпускной квалификационной
работы (дипломный проект)**

**Форма отзыва руководителя на выпускную квалификационную работу
(дипломный проект)**

Внешняя рецензия на выпускную квалификационную работу (дипломный проект)

**Примерный перечень вопросов ГЭК во время защиты выпускной
квалификационной работы (дипломный проект)**

Пример задания демонстрационного экзамена базового уровня

Описание общих требований
<p>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:</p> <ul style="list-style-type: none"> • Контроллер домена; • DLP сервер установлен, активирована лицензия, есть LDAP синхронизация; • Виртуальная машина с установленным сервером агентского мониторинга; • Виртуальная машина «нарушителя» в домене (1 шт).
<p>В компании развернут домен со всеми сотрудниками с указанием ФИО, должности и контактов.</p> <p>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.</p>
<p>Модуль 1: Эксплуатация автоматизированных (информационных) систем в защищенном исполнении</p>
<p>При выполнении задания модуля необходимо достичь следующих целей:</p> <ol style="list-style-type: none"> 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. <p>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.</p> <p>Допускается последующее выделение рамкой, стрелкой или иным способом результата работы.</p>

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 токenu, 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 введенный 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 должны 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. rule 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

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

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 PostgreSQL или 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 введенные 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 редактирование конфигурационных файлов (для устранения предупреждения).

Задача 6: Проверка работоспособности системы

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

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

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

Зафиксировать выполнение скриншотом выполненной выборки или конструктора выборки.

Задача 7: Защита системы с помощью сертификатов

Создайте дерево сертификатов формата PKCS для защиты веб-соединения с DLP-сервером по протоколу HTTPS. Сертификат и используемый ключ должны 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 4

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 заблокировать) и маркировать инциденты безопасности. Не должно быть ложных срабатываний. Не должно быть неправильной маркировки. Должны быть выявлены все инциденты безопасности.

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

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

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

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

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

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

Список тегов для политик:

Политика 1, Политика 2, Политика 3, ...

При выполнении модуля С ставятся следующие цели:

1. Настроить систему предотвращения утечек для правильного функционирования политик безопасности.
2. Произвести настройку технологий, используемых в политиках безопасности, а именно: лингвистический анализ, регулярные выражения, эталонные документы, графические объекты, выгрузки из баз данных.
3. Произвести верную настройку объектов защиты, верно выстроить логику срабатывания.
4. Разработать политики безопасности для корректного срабатывания политик, указать направления передачи, уровень нарушений, вердикты, теги.
5. Произвести проверку работоспособности политик.

При выполнении модуля С ставятся следующие задачи: Задача 1.1

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

Задача 1.2

Создайте локальную группу пользователей и добавьте в нее пользователей.

Задача 1.3

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

Задача 1.4

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

Задача 2

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

Вердикт: разрешить Уровень нарушения: низкий Тег: Задача 2

Задача 3

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

Вердикт: заблокировать 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 документестречается только по 1 слову из перечисленных — Задача срабатывать не должна.

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

Вердикт: разрешить

Уровень нарушения: средний Тег: Задача 7

Задача 8

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

Генеральный директор и совет директоров могут обмениваться данной информацией совершенно свободно. Вердикт: разрешить Уровень нарушения: средний Задача 9

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

Вердикт: Заблокировать Уровень нарушения: средний Тег: Задача 9

Задача 10

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

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

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

Вердикт: разрешить

Уровень нарушения: высокий Тег: Задача 10

Задача 11

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

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

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

Стандартизированные форматы паролей (кириллица):

6 букв – 1 знак !?#\$%^/& – 2-4 цифры – 4 буквы – 2-3 знака !?#\$%^/& (например, ПаРоль#67pКнЕ!?)

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.

