Федеральное государственное бюджетное образовательное учреждение высшего образования
«ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ ДВАЖДЫ ГЕРОЯ СОВЕТСКОГО СОЮЗА, ЛЕТЧИКА-КОСМОНАВТА А.А. ЛЕОНОВА»

КОЛЛЕДЖ КОСМИЧЕСКОГО МАШИНОСТРОЕНИЯ И ТЕХНОЛОГИЙ

ПРОГРАММА ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

по специальности

10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем»

Королев, 2023

Программа Государственной итоговой аттестации. – Королев: ТУ им. А.А. Леонова, 2023.

Программа Государственной итоговой аттестации составлена в соответствии с требованиями Федерального государственного образовательного стандарта среднего профессионального образования (далее – ФГОС СПО) и учебного плана по специальности 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем».

Содержание

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

В соответствии со ст. 59 Федерального Закона «Об образовании в Российской Федерации» итоговая аттестация выпускников, завершающих обучение по программам среднего профессионального образования, является обязательной.

Программа государственной итоговой аттестации выпускников по специальности 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем» разработана в соответствии с требованиями Федерального государственного образовательного стандарта среднего профессионального образования (далее – ФГОС СПО) по специальности 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем» (утвержден приказом Министерства образования и науки РФ от 09 декабря 2016 г. № 1551), Федерального закона «Об образовании в Российской Федерации» от 29 декабря 2012 г. № 273-ФЗ и приказа Минпросвещения России «Об утверждении Порядка проведения государственной итоговой аттестации по образовательным программам среднего профессионального образования» от 08.11.2021г. №800.

Государственная итоговая аттестация (далее – ГИА) является частью образовательной программы среднего профессионального образования (далее – образовательная программа) (программы подготовки специалистов среднего звена) по специальности 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем» и представляет собой форму оценки степени и уровня освоения обучающимися образовательной программы.

НАЗНАЧЕНИЕ И ЦЕЛИ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

ГИА проводится в форме демонстрационного экзамена и защиты дипломного проекта (работы).

Распределение бюджета времени государственной итоговой аттестации:

Этапы государственной итоговой аттестации	Количество недель
Демонстрационный экзамен	2
Защита дипломного проекта (работы)	

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

Демонстрационный экзамен проводится по двум уровням:

демонстрационный экзамен базового уровня проводится на основе требований к результатам освоения образовательной программы, установленных ФГОС СПО;

демонстрационный экзамен профильного уровня проводится по решению образовательной организации на основании заявлений выпускников на основе требований к результатам освоения образовательной программы, установленных ФГОС СПО, включая квалификационные требования, заявленные организациями, работодателями, заинтересованными в подготовке кадров соответствующей квалификации, в том числе являющимися стороной договора о сетевой форме реализации образовательных программ и (или) договора о практической подготовке обучающихся (далее – организации-партнеры).

Дипломный проект (работа) направлен на систематизацию и закрепление знаний выпускника по специальности, а также определение уровня готовности выпускника к самостоятельной профессиональной деятельности. Дипломный проект (работа) предполагает самостоятельную подготовку (написание) выпускником проекта (работы), демонстрирующего уровень знаний выпускника в рамках выбранной темы, а также сформированность его профессиональных умений и навыков.

Темы дипломных проектов (работ) определяются на заседании цикловой комиссии. Выпускнику предоставляется право выбора темы дипломного проекта (работы), в том числе предложения своей тематики с необходимым обоснованием целесообразности ее разработки для практического применения. Тематика дипломного проекта (работы) должна соответствовать содержанию одного или нескольких профессиональных модулей, входящих в образовательную программу.

Для подготовки дипломного проекта (работы) выпускнику назначается руководитель и при необходимости консультанты, оказывающие выпускнику методическую поддержку.

Закрепление за выпускниками тем дипломных проектов (работ), назначение руководителей и консультантов осуществляется приказом руководителя образовательной организации.

ПОДГОТОВКА ПРОВЕДЕНИЯ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

В целях определения соответствия результатов освоения выпускниками имеющих государственную аккредитацию образовательных программ среднего профессионального образования соответствующим требованиям ФГОС СПО ГИА проводится государственной экзаменационной комиссией (далее – ГЭК), создаваемой образовательной организацией по специальности 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем».

ГЭК формируется из числа педагогических работников образовательных

организаций, лиц, приглашенных из сторонних организаций, в том числе:

педагогических работников;

представителей организаций – партнеров, направление деятельности которых соответствует области профессиональной деятельности, к которой готовятся выпускники.

При проведении демонстрационного экзамена в составе ГЭК создается экспертная группа из числа лиц, приглашенных из сторонних организаций и обладающих профессиональными знаниями, навыками и опытом в сфере, соответствующей специальности среднего профессионального образования, по которой проводится демонстрационный экзамен.

Состав ГЭК утверждается приказом руководителя образовательной организации и действует в течение одного календарного года. В состав ГЭК входят председатель ГЭК, заместитель председателя ГЭК и члены ГЭК.

ГЭК возглавляет председатель, который организует и контролирует деятельность ГЭК, обеспечивает единство требований, предъявляемых к выпускникам.

Председатель ГЭК утверждается не позднее 20 декабря текущего года на следующий календарный год (с 1 января по 31 декабря) по представлению образовательной организации федеральным органом исполнительной власти, в ведении которого соответственно находится образовательная организация.

Председателем ГЭК образовательной организации утверждается лицо, не работающее в образовательной организации, из числа:

руководителей или заместителей руководителей организаций, осуществляющих образовательную деятельность, соответствующую области профессиональной деятельности, к которой готовятся выпускники;

представителей организаций-партнеров, при условии, что направление деятельности данных представителей соответствует области профессиональной деятельности, к которой готовятся выпускники.

Руководитель образовательной организации является заместителем председателя ГЭК. В случае создания в образовательной организации нескольких ГЭК назначается несколько заместителей председателя ГЭК из числа заместителей руководителя образовательной организации или педагогических работников.

Экспертная группа создается по специальности 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем».

Экспертную группу возглавляет главный эксперт, включенный в состав ГЭК.

Главный эксперт организует и контролирует деятельность возглавляемой экспертной группы, обеспечивает соблюдение всех требований к проведению демонстрационного экзамена и не участвует в оценивании результатов демонстрационного экзамена.

К ГИА допускаются выпускники, не имеющие академической задолженности и в полном объеме выполнившие учебный план или индивидуальный учебный план.

Демонстрационный экзамен базового и профильного уровня проводится с использованием единых оценочных материалов, включающих в себя конкретные комплекты оценочной документации, варианты заданий и критерии оценивания (далее – оценочные материалы), разрабатываемых организацией, определяемой Министерством просвещения Российской Федерации из числа подведомственных ему организаций.

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

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

Комплекты оценочной документации для проведения демонстрационного экзамена профильного уровня разрабатываются оператором с участием организаций-партнеров, отраслевых и профессиональных сообществ.

Программа ГИА утверждается образовательной организацией после обсуждения на заседании педагогического совета с участием председателей ГЭК, после чего доводится до сведения выпускников не позднее, чем за шесть месяцев до начала ГИА.

Пример комплекта оценочной документации для проведения демонстрационного экзамена

ДЕМОНСТРАЦИОННЫЙ ЭКЗАМЕН КОД

ЗАДАНИЕ ДЕМОНСТРАЦИОННОГО ЭКЗАМЕНА

Код комплекта оценочной документации	КОД 1.1-2023-2025
Год действия задания	2023
Номер варианта задания	2

ОПИСАНИЕ ЗАДАНИЯ

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 “DemoDept” в корневом каталоге оснастки “Пользователи и компьютеры” AD сервера.

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

Логин: iwtm-admin, пароль: xxXX2233, права пользователя домена

Логин: ldap-sync, пароль: xxXX2233, права пользователя домена

Логин: iwdm-root, пароль: xxXX2233, права администратора домена и локального администратора

Логин: user-pc, пароль xxXX2233, права пользователя домена

Логин: user-gp, пароль xxXX2233, 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.

Необходимо проверить наличие активной лицензии и в случае ее отсутствия обратиться к экспертам.

Необходимо 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 iwtm-admin 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 iwdm-root (важно).

После входа в систему необходимо переместить введенный в домен компьютер в ранее созданное подразделение “DemoDept” на домене.

Установить базу данных PostgreSQL или функциональный аналог с паролем суперпользователя xxXX2233.

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 xxXX2233

Синхронизировать каталог пользователей и компьютеров с Active Directory.

После синхронизации настроить беспарольный вход в консоль управления от ранее созданного доменного пользователя iwdm-root, 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.

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

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

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

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

Установить агент мониторинга:

На машину 1 (user-pc) с помощью задачи первичного распространения с сервера агентского 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.

На машину 2 (user-gp) с помощью групповых политик домена. Допускается как удаленная установка созданного вручную пакета, так и с помощью удаленной установки компонента Deploy Agent с последующей установкой через задачи сервера агентского мониторинга.

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

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

Задача 5: Установка и настройка подсистемы сканирования сетевых ресурсов (Crawler)

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

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

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

Зафиксировать выполнение задания скриншотом настройки и работоспособности в WEB-консоли.

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 термин «Демо экзамен» (в любом регистре), установить низкий уровень угрозы для всех событий, добавить тег «ДЭ».

Для отработки правил через сервер агентского мониторинга необходимо создавать правила в отдельной политике «Модуль 1». 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 1 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.

Зафиксировать выполнение скриншотом выполненной выборки или конструктора выборки.

Задача 7: Защита системы с помощью сертификатов

Создайте дерево сертификатов формата PKCS для защиты веб-соединения с DLP-сервером по протоколу HTTPS. Сертификат и используемый ключ должен удовлетворять общепринятым на сегодня стандартам и требованиям (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:

1. корневой root-сертификат (ca)
2. серверный (server) сертификат
3. по желанию допускается использование пользовательского и промежуточного сертификата

Дополнительная информация сертификатов должна включать в себя:

- Страна: RU
- Город: StPetersburg
- Компания (и иные дополнительные поля): demolab
- Отдел: Admins
- Почтовый адрес: из домена demo.lab
- Пароли ключей (если применимо): xxXX2233

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 для доверенного подключения к веб-консоли IWTM.

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

Итоговый результат должен включать:

Дерево из 2-3 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 о компании Demo.lab и т. п.

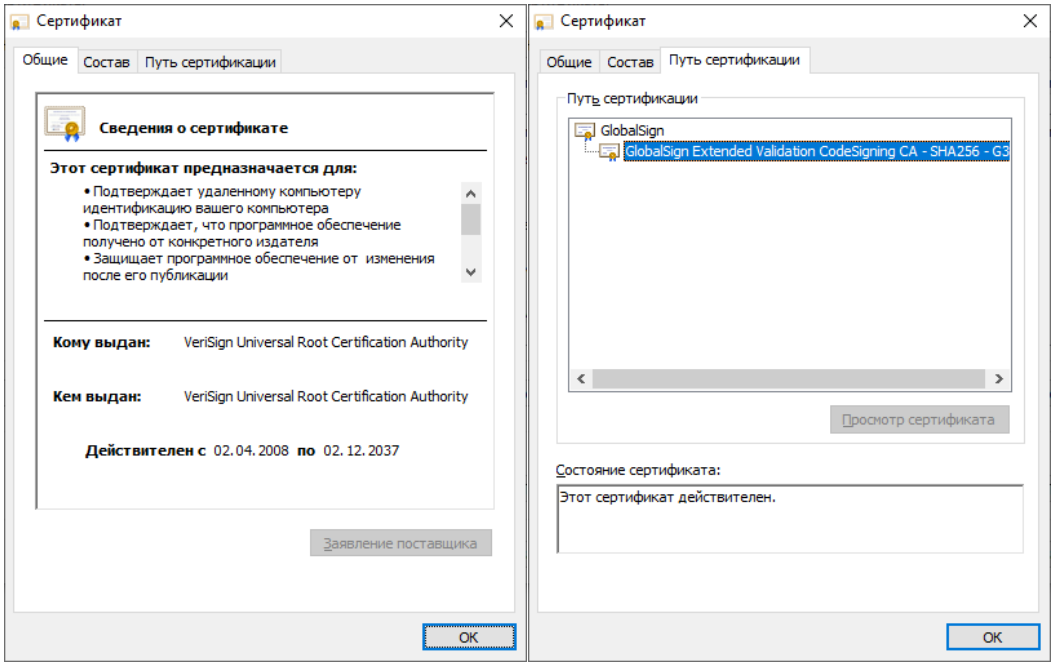

Рис. 1. Пример скриншотов задания

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). 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: CP-1.jpg

где CP – сокращение от англ. creating a policy, 1 – номер задания

Пример 2 для сохранения скриншота работающей политики: PW-1.jpg

где PW – сокращение от англ. policy work, 1 – номер задания.

Пример 3 для сохранения нескольких скриншотов одной работающей политики: PW-1-2.jpg

где PW – сокращение от англ. policy work, 1 – номер задания; 2 – номер скриншота для задания 1.

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: «Департамент 1» и «Департамент 2», а также создать 2 новых политики: «Департамент 1» и «Департамент 2». Каждая из политик должна применяться только на соответствующие группы. Компьютер 1 (user-pc) необходимо перенести в Департамент 1, а компьютер 2 (user-gp) — в Департамент 2.

Зафиксировать выполнение скриншотом.

Задача 2

Для удобства работы офицера безопасности необходимо установить дополнительную консоль управления сервером агентского мониторинга на любую машину нарушителя для удаленного доступа к серверу агентского мониторинга. Необходимо хотя бы 1 раз подключиться с удаленной консоли.

Зафиксировать выполнение скриншотом (в заголовке окна консоли будет указан IP-адрес или DNS имя удаленного сервера).

Задача 3

Необходимо установить (сменить) пароль для удаления агента мониторинга на всех машинах нарушителей с помощью средств сервера агентского мониторинга (удаленно). Пароль: xxXX2233

Проверить работоспособность и зафиксировать выполнение скриншотами.

Следующие правила создаются в политике «Департамент 1».

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 DropBox, остальные сервисы настроить только в режиме чтения (разрешить скачивание).

Зафиксировать факт настройки правил (политик) скриншотами.

Правило 3

Запретить запуск приложения calculator и mspaint.

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

Правило 4

Необходимо запретить создание снимков экрана в текстовых процессорах (Word или Libre/Open Office Writer) для предотвращения утечки секретных расчетов и баз данных.

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

Правило 5

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

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

Правило 6

С учетом ранее созданной блокировки необходимо разрешить копирование только на один доверенный USB-накопитель с помощью белого списка. В случае отсутствия USB-накопителей создать исключение для любого другого конкретного устройства (кроме CD/DVD).

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).

Следующие правила создаются в политике «Департамент 2».

Правило 9

Необходимо запретить доступ к буферу обмена в приложениях wordpad и firefox.

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

Правило 10

Необходимо поставить на контроль печать документов на принтерах. Продемонстрировать работоспособность на любую из политик IWTM.

Проверить работоспособность, зафиксировать факт настройки правил (политик) и их работоспособность скриншотами (обязательно с рабочим событием печати в веб-консоли).

Правило 11

На машине нарушителя необходимо запретить использование буфера обмена при подключении к удаленным машинам по протоколу RDP.

Проверить работоспособность, зафиксировать факт настройки правил (политик) и их работоспособность скриншотами. Для проверки работоспособности необходимо будет включить RDP доступ на любой из машин.

Правило 12

Необходимо установить контроль за компьютером потенциального нарушителя в случае использования браузера edge (или Internet explorer) путем создания снимков экрана каждые 90 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 13

Запретить передачу файлов документов типа MS Excel, Libre/Open Office Calc 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 2 (user-gp), 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: 30 дней
- Минимальная длина пароля: 6 символов
- Блокировка пользователя при неправильном вводе пароля: 5
- Блокировка учетной записи при вводе пароля: 20 минут

Зафиксировать настройки политики скриншотами.

Групповая политика 2

Запретить запуск приложений notepad++.exe, charmap.exe.

Зафиксировать настройки политики и выполнение скриншотами.

Групповая политика 3

Запретить использование командной строки и редактора реестра пользователем стандартной политикой запрета (не с помощью списка).

Зафиксировать настройки политики и выполнение скриншотами.

Групповая политика 4

Запретить пользователю самостоятельно менять изображение блокировки экрана.

Зафиксировать настройки политики и выполнение скриншотами.

Групповая политика 5

Изменить изображение рабочего стола пользователя групповыми политиками с использованием SYSVOL или общего каталога в домене.

Изображение необходимо создать самостоятельно, должно содержать в себе название компании (Демолаб, demo.lab) текстом в картинке.

Изменение изображения вручную не будет считаться корректным выполнением задания.

Зафиксировать настройки политики и выполнение скриншотами.

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

Создайте в DLP-системе политики безопасности согласно нижеперечисленным заданиям.

Политики должны автоматически блокировать трафик и/или предупреждать о нарушении в соответствии с заданием.

Способ, которым создана корректная политика, оставлен на усмотрение самого экзаменуемого.

При выявлении уязвимости DLP-система должна автоматически устанавливать уровень угрозы в соответствии с заданием.

После создания всех политик может быть запущен автоматический «генератор трафика», который передаст поток данных, содержащих как утечки, так и легальную информацию.

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

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

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

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

Задания на разработку политик можно выполнять в любом порядке.

Наиболее сложные политики находятся в конце.

Внимание!

Необходимо называть политики / объекты / категории / теги и прочее ТОЛЬКО в соответствии с номером и названием задания

Политики — Политика X, например «Политика 4».

Для комбинированных политик формат: Политика 4.1, 4.2 и т.д.

Объект защиты — Объект X, например «Объект 11».

Все политики «по умолчанию», находящиеся в консоли управления в процессе выполнения заданий должны быть отключены или удалены, так как могут помешать корректной оценке.

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, Политика 4, Политика 5, Политика 6, Политика 7, Политика 8, Политика 9, Политика 10, Политика 11, Политика 12

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

Необходимо выключить или удалить стандартные политики и отключить стандартные каталоги объектов защиты. Стоит учесть, что стандартные политики и объекты можно модифицировать под свои нужды.

Задача 2

Создайте локальную группу пользователей «Подозрительные сотрудники» в Traffic Monitor. Добавьте в нее трех любых пользователей.

Задача 3

Создать список веб-ресурсов «Партнерские домены». Добавить в список следующие сайты: megademo.lab, act-demolab.ru, sysdem.lab.

Задача 4

Для работы системы необходимо настроить периметр компании:

- Почтовый домен: demo.lab.
- Список веб ресурсов «Партнерские домены» (созданный ранее).
- Группа персон: пользователи домена (все).
- Исключить из перехвата почту генерального директора.

Политика 1

В связи с тем, что компания является оператором обработки персональных данных, необходимо запретить всем сотрудникам кроме отдела бухгалтерии (Financial) отправлять документы, содержащие информацию о СНИЛС и паспортных данных (в текстовом и графическом виде) за пределы компании. Отдел бухгалтерии может отправлять файлы без ограничений. Можно использовать стандартные технологии и объекты.

Вердикт: заблокировать

Уровень нарушения: средний

Тег: Политика 1

Политика 2

Для контроля за движением официальных документов необходимо вести наблюдение за передачей как пустых, так и заполненных шаблонов документа «Договор.docx» за пределы компании. Стоит учесть, что содержимое документа может изменяться в пределах 35%.

Вердикт: разрешить

Уровень нарушения: низкий

Тег: Политика 2

Политика 3

В связи с введением оплаты с помощью кредитных карт, необходимо запрещать передачу как текстовых, так и графических данных о кредитных картах за пределы компании для всех сотрудников, кроме отдела договоров (accounting). Политика может быть настроена с использованием стандартных технологий и объектов.

Вердикт: заблокировать

Уровень нарушения: средний

Тег: Политика 3

Политика 4

Необходимо отслеживать любые документы, передающиеся за пределы компании и содержащие печать компании всем сотрудникам, кроме отдела продаж (Sales) и директора компании. Они могут обмениваться документами внутри и за пределами компании без контроля.

Вердикт: разрешить

Уровень нарушения: низкий

Тег: Политика 4

Политика 5

В связи с распространением коронавирусной инфекцией сотрудники стали чаще обсуждать различные новости, мешая рабочему процессу. Необходимо отслеживать следующие термины: COVID (внутри любой фразы), SARS (внутри любой фразы, например SARS-CoV-2), Коронавирус.

Вердикт: разрешить

Уровень нарушения: низкий

Тег: Политика 5

Политика 6

Сотрудники отдела ИТ 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 отдела информатизации, для остальных контролировать не нужно.

Критичными данными в выгрузке являются телефоны, ИНН, ОКПО, ОКФС, ОКОГУ и ОКОПФ и в 1 документе присутствует 4 или более компаний. Для настройки используйте файл «Выгрузка из БД.csv».

Вердикт: разрешить

Уровень нарушения: средний

Тег: Политика 6

Политика 7

Офицеру безопасности стало известно, что многих сотрудников не устраивает уровень заработной платы, поэтому планируется проведение несанкционированного мероприятия. Необходимо создать политику, которая позволит узнать точную дату и время проведения мероприятия.

Сообщение с датой можно найти по ключевым словам: «митинг», «пикет», «маленькая зарплата» Если в документе встречается только по 1 слову из перечисленных — политика срабатывать не должна.

Правило должно работать на всех сотрудников, кроме совета директоров (BOD) и директора, которые могут отсылать информацию свободно.

Вердикт: разрешить

Уровень нарушения: средний

Тег: Политика 7

Политика 8

В последнее время сотрудники стали чаще обсуждать популярные сериалы в мессенджерах и социальных сетях, из-за чего упала общая производительность на 8%. Было решено отследить, кто больше всего занимается не рабочей деятельностью, для чего необходимо создать политику для отслеживания 5 популярных на данный момент сериалов при передаче через веб-сообщения и почту.

Список сериалов:

«Игра в кальмара», «Бумажный дом», «Рик и Морти», «Очень странные дела», «Мир дикого запада».

Вердикт: разрешить

Уровень нарушения: низкий

Тег: Политика 8

Политика 9

Оказалось, что сотрудники не только обсуждают сериалы, а еще и обмениваются ссылками и torrent-файлами для их скачивания, после чего скачивают их, используя интернет-канал компании или обмениваются скачанным материалом внутри компании, что также нагружает сеть.

В связи с этим необходимо блокировать передачу (а где это невозможно — просто контролировать) файлов формата .torrent и ссылок формата magnet: (и содержащей urn (хеш) файла). Ложных срабатываний просто на слово Magnet (в т. ч. с двоеточием) быть не должно.

Вердикт: Заблокировать

Уровень нарушения: средний

Тег: Политика 9

Политика 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 доменов компании: demo и demolab, демо, демолаб.

Важно, чтобы в одном сообщении содержалось минимум 4 адреса (т. к. в противном случае будут детектироваться все почтовые сообщения)!

Возможные домены первого уровня: ru, org, lab. Детектирование только частей адресов (например @demo.ru) недопустимо. Пример формата адресов: e-mail@demolab.ru , mail+tag@demo.lab, elepochta@demo.org и т. п. Разрешенные спецсимволы в почте: _ . - +

Вердикт: разрешить

Уровень нарушения: высокий

Тег: Политика 10

Политика 11

Сотрудники и партнеры компании стали получать много спама на телефоны, в связи с чем возникло подозрение о том, что кто-то производит «слив» номеров из баз данных компании путем передачи информации за пределы компании через браузер, почту или флешки. Необходимо контролировать передачу как минимум 3 номеров в сообщении, т.к. передача всего одного номера может быть контактной информацией.

Мобильные номера могут быть только операторов РФ (код страны 7, код оператора начинается с 9), в различных форматах, например:

+7 (987) 123-45-67, +79871234567, +7 987 123 4567, 8-987 123-4567 и т.д.

Необходимо учесть все варианты только для мобильных номеров, комбинации пробелов, скобок, дефисов.

Вердикт: разрешить

Уровень нарушения: средний

Тег: Политика 11

Политика 12

Необходимо контролировать передачу (веб, почта) любых зашифрованных архивов только за пределы компании.

Вердикт: разрешить

Уровень нарушения: низкий

Тег: Политика 12

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 правами просмотра и выполнения сводок, отчетов и событий. Прав на редактирование (изменение) быть не должно.

Пользователь: infouser, пароль: xxXX2233

Задача 2: Сводки

Создайте новые вкладки сводки в разделе «Сводка» под названием «ДЭ» и «Выборка»

Задача 3: Виджеты

При создании выборок для сводок необходимо помещать их в каталог выборок «ДЭ»

Создайте в сводке «ДЭ» 4 виджета:

1. Выборка по событиям краулера за последний месяц
2. Выборка по политикам с технологиями: графические объекты, печати, эталонные документы за последние 7 дней
3. Статистика по политикам за последний месяц
4. Топ нарушителей за последнюю неделю

Задача 4

Необходимо создать виджет в разделе «Сводка», вкладка «Выборка», отображающий события с уровнем угрозы от низкого до среднего на правила передачи и работы в приложениях (буфера) за последние 3 дня.

Зафиксировать скриншотом конструктора выборки.

Задача 5

Необходимо создать виджет в разделе «Сводка», вкладка «Выборка» для отображения нарушений только от обоих компьютеров нарушителей (виртуальных машин) с низким и высоким уровнем угрозы за последние 30 дней.

Требования к оформлению письменных материалов

Отчеты выполняются только в электронном виде в соответствии с заданием.

Представление результатов работы

Предоставляется в виде снимков экрана и текстового отчета.

Необходимые приложения

Необходимые приложения смотреть в папке «КОД 1.1 Приложения к вариантам»

Приложение 1: Карточка настроек сети и оборудования (docx)

Приложение 2: Шаблоны документов для задания (zip)

Структура и объем дипломного проекта (работы)

В дипломном проекте (работе) должны содержаться следующие структурные части в порядке их следования:

– титульный лист;

– задание на дипломный проект (работу);

– содержание (оглавление);

– перечень условных обозначений, специальных терминов и сокращений (желательно, но не обязательно);

– введение;

– основная часть;

– заключение (выводы);

– список использованных источников;

– приложения;

– отзыв руководителя;

– рецензия.

Во введении необходимо обосновать актуальность и практическую значимость выбранной темы, сформулировать цель и задачи, объект и предмет, круг рассматриваемых проблем. Объем введения должен быть в пределах 4 – 5 страниц. Основная часть дипломного проекта (работы) включает главы (параграфы, разделы) в соответствии с логической структурой изложения. Название главы не должно дублировать название темы, а название параграфов – название глав. Формулировки должны быть лаконичными и отражать суть главы (параграфа). Основная часть дипломного проекта (работы) должна содержать две главы.

Первая глава посвящается теоретическим аспектам изучаемого объекта и предмета дипломного проекта (работы). В ней содержится обзор используемых источников информации, нормативной базы по теме дипломного проекта (работы). В этой главе могут найти место статистические данные, построенные таблицы и графики.

Вторая глава посвящается анализу практического материала, полученного во время производственной практики (преддипломной). В этой главе содержится:

– анализ конкретного материала по избранной теме;

– описание выявленных проблем и тенденций развития объекта и предмета изучения на основе анализа конкретного материала по избранной теме;

– описание способов решения выявленных проблем;

– обоснование экономической эффективности.

В ходе анализа могут использоваться аналитические таблицы, расчеты, формулы, схемы, диаграммы и графики.

Заключение не должно составлять более 5 страниц текста. Заключение содержит выводы и предложения с их кратким обоснованием в соответствии с поставленной целью и задачами, раскрывает значимость полученных результатов.

Список использованных источников отражает перечень источников, которые использовались при написании дипломного проекта (работы) (не менее 20), составленный в следующем порядке:

– Федеральные законы (в очередности от последнего года принятия к предыдущим);

– указы Президента Российской Федерации (в той же последовательности);

– постановления Правительства Российской Федерации (в той же очередности);

– иные нормативные правовые акты;

– иные официальные материалы (резолюции-рекомендации международных организаций и конференций, официальные доклады, официальные отчеты и др.);

– монографии, учебники, учебные пособия (в алфавитном порядке);

– иностранная литература;

– Интернет-ресурсы.

Приложения могут состоять из дополнительных справочных материалов, имеющих вспомогательное значение, например: копий документов, выдержек из отчетных материалов, статистических данных, схем, таблиц, диаграмм, программ, положений и т.п.

Объем дипломного проекта (работы) не менее 30 страниц, не включая приложений.

Тематика дипломных проектов (работ)

Тематика дипломных проектов (работ) может включать решение следующих основных задач:

- разработка специальных программных защитных средств;
- разработка проектов использования имеющихся средств для защиты выбранного объекта;
- разработка комплексной системы защиты информации предприятия, его отдельных помещений;
- разработка методов анализа эффективности использования различных видов защиты информации на объектах защиты;
- разработка требований, нормативно-правовой базы, процедур по обеспечению безопасности объектов;
- исследование методов обеспечения надежной защиты объектов информатизации;
- автоматизация процессов обеспечения безопасности объектов.

Порядок выполнения дипломных проектов (работ)

Выпускник выполняет дипломный проект (работу) по графику. Законченные главы дипломного проекта в установленные сроки должны сдаваться руководителю на проверку. Руководитель, проверив главу, может вернуть ее выпускнику для доработки со своими письменными замечаниями.

По окончании работы, но не позднее срока сдачи по графику, дипломный проект (работу), подписанный выпускником сдается руководителю. При положительном решении, руководитель подписывает работу и дает письменный отзыв о дипломном проекте (работе), где отмечает правильность понимания выпускником задач, поставленных темой и степень их проработки, существенную новизну и наиболее интересные решения, практическую полезность работы (внедрения, публикации и др.), качество разработки и оформления дипломного проекта, умение анализировать и делать обоснованные выводы и предложения, знания, навыки и отношение к работе, показанные во время написания дипломного проекта (работы), степень самостоятельности в решении поставленных задач, возможность допуска дипломного проекта (работы) к защите и присвоения ее автору квалификации «техник по защите информации» по специальности 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем» (без оценки в баллах).

При положительном отзыве руководителя дипломный проект (работа) направляется на внешнюю рецензию. Внешний рецензент назначается из числа ведущих специалистов предприятия или организации, где проходил практику выпускник.

В рецензии отмечается актуальность темы, соответствие выполненной дипломного проекта заданию, оценку степени разработки новых вопросов, оригинальности решений (предложений), теоретической и практической значимости дипломного проекта (работы), глубина и обоснованность решений, возможность практического использования полученных результатов, качество дипломной работы, слабые стороны и недостатки, общий вывод о дипломном проекте, ее оценка, мнение о возможности присвоения автору квалификации по специальности. После рецензирования всякие исправления в дипломном проекте (работе) не допускаются.

К защите дипломного проекта (работы) выпускник должен совместно с руководителем подготовить доклад на 10 – 15 минут, в котором необходимо отразить полное наименование темы и ее актуальность, поставленные цели и задачи, расчет экономической эффективности, заключение о возможности реализации предложений дипломного проекта (работы) и их дальнейшее совершенствование.

График выполнения дипломного проекта (работы)

№ п/п	Наименование этапа	Сроки сдачи
1.	Выбор темы	до 20.04.
2.	Подбор литературы и ее изучение по теме дипломного проекта (работы), сбор практического материала	до 17.05.
3.	Составление плана дипломного проекта (работы) и согласование его с руководителем	18.05.-19.05
4.	Разработка и представление на проверку введения	20.05-21.05
5.	Разработка и представление на проверку первой главы	22.05-25.05
6.	Разработка и представление на проверку второй главы с учетом материала, полученного на производственной (преддипломной) практике	26.05-29.05
7.	Разработка и представление на проверку третьей главы, заключения	30.05- 02.06
8.	Оформление отзыва руководителя дипломного проекта (работы)	03.06-04.06
9.	Внешнее рецензирование дипломного проекта (работы)	05.06-07.06
10.	Предварительная защита дипломного проекта (работы)	08.06-11.06
11.	Подготовка к защите дипломного проекта (работы)	12.06 -14.06
12.	Защита дипломного проекта (работы)	15.06-28.06.

ПРОВЕДЕНИЕ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

Демонстрационный экзамен проводится с использованием комплектов оценочной документации, включенных образовательными организациями в программу ГИА.

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

Образовательная организация обеспечивает необходимые технические условия для обеспечения заданиями во время демонстрационного экзамена выпускников, членов ГЭК, членов экспертной группы.

Демонстрационный экзамен проводится в центре проведения демонстрационного экзамена (далее - центр проведения экзамена), представляющем собой площадку, оборудованную и оснащенную в соответствии с комплектом оценочной документации.

Центр проведения экзамена может располагаться на территории образовательной организации, а при сетевой форме реализации образовательных программ - также на территории иной организации, обладающей необходимыми ресурсами для организации центра проведения экзамена.

Выпускники проходят демонстрационный экзамен в центре проведения экзамена в составе экзаменационных групп.

Место расположения центра проведения экзамена, дата и время начала проведения демонстрационного экзамена, расписание сдачи экзаменов в составе

экзаменационных групп, планируемая продолжительность проведения демонстрационного экзамена, технические перерывы в проведении демонстрационного экзамена определяются планом проведения демонстрационного экзамена, утверждаемым ГЭК совместно с образовательной организацией не позднее чем за двадцать календарных дней до даты проведения демонстрационного экзамена. Образовательная организация знакомит с планом проведения демонстрационного экзамена выпускников, сдающих демонстрационный экзамен и лиц, обеспечивающих проведение демонстрационного экзамена в срок не позднее чем за пять рабочих дней до даты проведения экзамена.

Количество, общая площадь и состояние помещений, предоставляемых для проведения демонстрационного экзамена, должны обеспечивать проведение демонстрационного экзамена в соответствии с комплектом оценочной документации.

Центр проведения экзамена может быть дополнительно обследован оператором на предмет соответствия условиям, установленным комплектом оценочной документации, в том числе в части наличия расходных материалов.

Не позднее чем за один рабочий день до даты проведения демонстрационного экзамена главным экспертом проводится проверка готовности центра проведения экзамена в присутствии членов экспертной группы, выпускников, 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 демонстрационного экзамена, а также распределение рабочих мест между выпускниками с использованием способа случайной выборки. Результаты распределения обязанностей между членами экспертной группы и распределения рабочих мест между выпускниками фиксируются главным экспертом в соответствующих протоколах.

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

Технический эксперт под подпись знакомит главного эксперта, членов экспертной группы, выпускников с требованиями охраны труда и безопасности производства.

В день проведения демонстрационного экзамена в центре проведения экзамена присутствуют:

а) руководитель (уполномоченный представитель) организации, на базе которой организован центр проведения экзамена;

б) не менее одного члена ГЭК, не считая членов экспертной группы;

в) члены экспертной группы;

г) главный эксперт;

д) представители организаций-партнеров (по согласованию с образовательной организацией);

е) выпускники;

ж) технический эксперт;

з) представитель образовательной организации, ответственный за сопровождение выпускников к центру проведения экзамена (при необходимости);

и) тьютор (ассистент), оказывающий необходимую помощь выпускнику из числа лиц с ограниченными возможностями здоровья, детей-инвалидов, инвалидов (далее - тьютор (ассистент);

к) организаторы, назначенные образовательной организацией из числа педагогических работников, оказывающие содействие главному эксперту в обеспечении соблюдения всех требований к проведению демонстрационного экзамена.

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

Допуск выпускников в центр проведения экзамена осуществляется главным экспертом на основании документов, удостоверяющих личность.

В день проведения демонстрационного экзамена в центре проведения экзамена могут присутствовать:

а) должностные лица органа исполнительной власти субъекта Российской Федерации, осуществляющего управление в сфере образования (по решению указанного органа);

б) представители оператора (по согласованию с образовательной организацией);

в) медицинские работники (по решению организации, на территории которой располагается центр проведения демонстрационного экзамена);

г) представители организаций-партнеров (по решению таких организаций по согласованию с образовательной организацией).

Указанные в настоящем пункте лица присутствуют в центре проведения экзамена в день проведения демонстрационного экзамена на основании документов, удостоверяющих личность.

Лица, присутствующие на демонстрационном экзамене, 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 выпускниками при выполнении ими заданий, не передавать им средства связи и хранения информации, иные предметы и материалы.

Члены ГЭК, не входящие в состав экспертной группы, наблюдают за ходом проведения демонстрационного экзамена и вправе сообщать главному эксперту о выявленных фактах нарушения порядка проведения государственной итоговой аттестации.

Члены экспертной группы осуществляют оценку выполнения заданий демонстрационного экзамена самостоятельно.

Главный эксперт вправе давать указания по организации и проведению демонстрационного экзамена, обязательные для выполнения лицами, привлеченными к проведению демонстрационного экзамена, и выпускникам, удалять из центра проведения экзамена лиц, допустивших грубое нарушение требований порядка проведения государственной итоговой аттестации, требований охраны труда и безопасности производства, а также останавливать, приостанавливать и возобновлять проведение демонстрационного экзамена при возникновении необходимости устранения грубых нарушений требований Порядка, требований охраны труда и производственной безопасности.

Главный эксперт может делать заметки о ходе демонстрационного экзамена.

Главный эксперт обязан находиться в центре проведения экзамена до окончания демонстрационного экзамена, осуществлять контроль за соблюдением лицами, привлеченными к проведению демонстрационного экзамена, выпускниками требований порядка проведения государственной итоговой аттестации.

При привлечении медицинского работника организация, на базе которой организован центр проведения экзамена, обязана организовать помещение, оборудованное для оказания первой помощи и первичной медико-санитарной помощи.

Технический эксперт вправе:

наблюдать за ходом проведения демонстрационного экзамена;

давать разъяснения и указания лицам, привлеченным к проведению демонстрационного экзамена, выпускникам по вопросам соблюдения требований охраны труда и производственной безопасности;

сообщать главному эксперту о выявленных случаях нарушений лицами, привлеченными к проведению демонстрационного экзамена, выпускниками 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 демонстрационного экзамена, выпускников действия выпускников по выполнению заданий, действия других лиц, находящихся в центре проведения экзамена с уведомлением главного эксперта.

Представитель образовательной организации располагается в изолированном от центра проведения экзамена помещении.

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

Выпускники вправе:

пользоваться оборудованием центра проведения экзамена, необходимыми материалами, средствами обучения и воспитания в соответствии с требованиями комплекта оценочной документации, задания демонстрационного экзамена;

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

получить копию задания демонстрационного экзамена на бумажном носителе;

Выпускники обязаны:

во время проведения демонстрационного экзамена не пользоваться и не иметь при себе средства связи, носители информации, средства ее передачи и хранения, если это прямо не предусмотрено комплектом оценочной документации;

во время проведения демонстрационного экзамена использовать только средства обучения и воспитания, разрешенные комплектом оценочной документации;

во время проведения демонстрационного экзамена не взаимодействовать с другими выпускниками, экспертами, иными лицами, находящимися в центре проведения экзамена, если это не предусмотрено комплектом оценочной документации и заданием демонстрационного экзамена.

Выпускники могут иметь при себе лекарственные средства и питание, прием которых осуществляется в специально отведенном для этого помещении согласно плану проведения демонстрационного экзамена за пределами центра проведения экзамена.

Допуск выпускников к выполнению заданий осуществляется при условии обязательного их ознакомления с требованиями охраны труда и производственной безопасности.

В соответствии с планом проведения демонстрационного экзамена главный эксперт ознакамливает выпускников с заданиями, передает им копии заданий демонстрационного экзамена.

После ознакомления с заданиями демонстрационного экзамена выпускники занимают свои рабочие места в соответствии с протоколом распределения рабочих мест.

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

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

После объявления главным экспертом начала демонстрационного экзамена выпускники приступают к выполнению заданий демонстрационного экзамена.

Демонстрационный экзамен проводится при неукоснительном соблюдении выпускниками, лицами, привлеченными к проведению демонстрационного экзамена, требований охраны труда и производственной безопасности, а также с соблюдением принципов объективности, открытости и равенства выпускников.

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

Видеоматериалы о проведении демонстрационного экзамена в случае осуществления видеозаписи подлежат хранению в образовательной организации не менее одного года с момента завершения демонстрационного экзамена.

Явка выпускника, его рабочее место, время завершения выполнения задания демонстрационного экзамена подлежат фиксации главным экспертом в протоколе проведения демонстрационного экзамена.

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

Главный эксперт сообщает выпускникам о течении времени выполнения задания демонстрационного экзамена каждые 60 минут, а также за 30 и 5 минут до окончания времени выполнения задания.

После объявления главным экспертом окончания времени выполнения заданий выпускники прекращают любые действия по выполнению заданий демонстрационного экзамена.

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

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

Результаты выполнения выпускниками заданий демонстрационного экзамена подлежат фиксации экспертами экспертной группы в соответствии с требованиями комплекта оценочной документации и задания демонстрационного экзамена.

Организация защиты дипломного проекта (работы)

После завершения написания дипломного проекта (работы) организуется предварительная защита, на которой особое внимание уделяется отработке доклада (формы и содержания). Предварительная защита проводится не позднее чем за 1 неделю до государственной итоговой аттестации.
К предварительной защите выпускник представляет:

1. готовый дипломный проект (работу), подписанный автором, руководителем и рецензентом. Название темы дипломного проекта (работы) должно точно соответствовать ее формулировке, указанной в приказе руководителя образовательной организации;
2. презентацию дипломного проекта (работы) в электронном виде на USB-накопителе;
3. отзыв руководителя;
4. рецензию;
5. документы об использовании и внедрении на производстве результатов дипломного проекта (работы) (при их наличии).

Завершающим этапом подготовки дипломного проекта (работы) является ее защита на открытом заседании ГЭК.

Выпускник в течение 10-15 минут излагает основные положения своей работы. Выступление должно начинаться с обоснования актуальности темы и характеристики объекта исследования. Далее следует раскрыть основное содержание работы, обращая особое внимание на освещенный в работе передовой опыт и отличительные недостатки в практике, а также на те выводы и рекомендации, которые, по мнению выпускника, будут способствовать максимальному использованию высокотехнологичного оборудования. Доклад не следует перегружать цифровыми показателями, а привести лишь те данные, на которые сделаны ссылки в раздаточных материалах. Выпускник должен излагать основное содержание своей работы свободно, не читая письменного текста.

Заканчивая выступление, выпускник должен ответить на замечания рецензента, соглашаясь с ними, объясняя причину недоработок, указывая способы их устранения или аргументировано опровергая их, отстаивая свою точку зрения.

Важный и ответственный момент защиты дипломного проекта (работы) – ответы на вопросы. Вопросы выпускнику задают сразу после его выступления в устной форме члены ГЭК. Количество вопросов, задаваемых выпускнику при защите дипломного проекта (работы), не ограничивается. При подготовке ответов на вопросы и замечания рецензента выпускник имеет право пользоваться своей работой. Ответы на вопросы должны быть убедительны, теоретически обоснованы, а при необходимости подкреплены цифровым материалом. Следует помнить, что ответы на вопросы, их полнота и глубина, влияют на оценку по защите дипломного проекта (работы), поэтому их необходимо тщательно продумывать. Может быть предусмотрено выступление руководителя дипломного проекта (работы), а также рецензента, если они присутствуют на заседании государственной экзаменационной комиссии.

После доклада выпускника и ответов на заданные ему вопросы секретарем комиссии зачитывается рецензия.

Решение о качестве и уровне дипломного проекта (работы) принимается на закрытом заседании ГЭК простым большинством голосов членов комиссии, участвующих в заседании (при равном числе голосов голос председателя является решающим).

ОЦЕНИВАНИЕ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

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 демонстрационного экзамена осуществляется членами экспертной группы по 100-балльной системе в соответствии с требованиями комплекта оценочной документации.

Баллы выставляются в протоколе проведения демонстрационного экзамена, 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 демонстрационного экзамена далее передается в ГЭК для выставления оценок по итогам ГИА.

Оригинал протокола проведения демонстрационного экзамена передается на хранение в образовательную организацию в составе архивных документов.

Перевод баллов демонстрационного экзамена базового уровня в оценку:

Оценка ГИА	«2»	«3»	«4»	«5»
Отношение полученного количества баллов к максимально возможному (в процентах)	0,00 % - 14,99 %	15 % - 29,99 %	30 % - 59,99 %	60 % - 100 %

Перевод баллов демонстрационного экзамена профильного уровня в оценку:

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

Результаты защиты дипломного проекта (работы) определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

При определении окончательной оценки по защите дипломного проекта (работы) учитываются:

- доклад выпускника по каждому разделу дипломного проекта (работы);
- ответы на вопросы;
- оценка рецензента;
- отзыв руководителя.

Оценки ***«отлично»*** заслуживает работа, в которой полно и всесторонне раскрыто теоретическое содержание темы, дан глубокий критический анализ действующей практики учетно-аналитической работы. Творчески были решены проблемные вопросы, сделаны экономически обоснованные предложения. Выпускник при защите дал аргументированные ответы на все вопросы членов комиссии, проявил творческие способности в понимании и изложении ответов на вопросы.

Оценка ***«хорошо»*** выставляется за дипломный проект (работу), который имеет положительный отзыв руководителя и рецензента. При его защите выпускник показывает знания вопросов темы, оперирует данными исследования, вносит предложения по теме исследования, во время доклада использует наглядные пособия, без особых затруднений отвечает на поставленные вопросы.

Оценка ***«удовлетворительно»*** выставляется за дипломный проект (работу), в отзывах руководителя и рецензента которого имеются замечания по содержанию работы и методике анализа. В работе теоретические вопросы в основном раскрыты, выводы в основном правильные, предложения представляют интерес, но недостаточно убедительно аргументированы и не на все вопросы членов комиссии студент при защите дал правильные ответы.

Оценка ***«неудовлетворительно»*** выставляется за дипломный проект (работу), который в основном отвечает предъявляемым требованиям, но при

защите выпускник не дал правильных ответов на большинство заданных вопросов, т.е. обнаружил серьезные пробелы в профессиональных знаниях.

Заседания государственной экзаменационной комиссии протоколируются. В протоколе записываются итоговая оценка дипломного проекта (работы), присуждение квалификации и особые мнения членов комиссии. Протоколы заседаний ГЭК подписываются председателем и ответственным секретарем.

После оформления протокола заседания ГЭК объявляются результаты защиты – оценка и решение о присуждении квалификации «техник по защите информации».

Статус победителя, призера чемпионатов профессионального мастерства, проведённых 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" выпускника по профилю осваиваемой образовательной программы среднего профессионального образования засчитывается в качестве оценки "отлично" по демонстрационному экзамену в рамках проведения ГИА по данной образовательной программе среднего профессионального образования.

В случае досрочного завершения ГИА выпускником по независящим от него причинам результаты ГИА оцениваются по фактически выполненной работе, или по заявлению такого выпускника ГЭК принимается решение об аннулировании результатов ГИА, а такой выпускник 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 образовательной организации.

Выпускникам, не прошедшим ГИА по уважительной причине, в том числе не явившимся по уважительной причине для прохождения одного из аттестационных испытаний, предусмотренных формой ГИА (далее - выпускники, не прошедшие ГИА по уважительной причине), предоставляется возможность пройти ГИА, в том числе не пройденное аттестационное испытание (при его наличии), без отчисления из образовательной организации.

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

получившие на ГИА неудовлетворительные результаты, могут быть допущены образовательной организацией для повторного участия в ГИА не более двух раз.

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

Выпускники, не прошедшие ГИА по неуважительной причине, и выпускники, получившие на ГИА неудовлетворительные результаты, отчисляются из образовательной организации и проходят ГИА не ранее чем через шесть месяцев после прохождения ГИА впервые.

Для прохождения ГИА выпускники, не прошедшие ГИА по неуважительной причине, и выпускники, получившие на ГИА неудовлетворительные результаты, восстанавливаются в образовательной организации на период времени, установленный образовательной организацией самостоятельно, но не менее предусмотренного календарным учебным графиком для прохождения ГИА соответствующей образовательной программы среднего профессионального образования.

ПОРЯДОК ПОДАЧИ И РАССМОТРЕНИЯ АПЕЛЛЯЦИЙ

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

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

Апелляция о нарушении порядка проведения государственной итоговой аттестации 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.

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

Состав апелляционной комиссии утверждается образовательной организацией 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 образовательной организации, не входящих в данном учебном году 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 выпускники, представителей организаций-партнеров или их объединений, включая экспертов, при условии, что направление деятельности данных представителей соответствует области профессиональной деятельности, к которой готовятся выпускники, при условии, что такое лицо не входит в состав ГЭК.

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 демонстрационного экзамена.

При проведении ГИА в форме демонстрационного экзамена 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.

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

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

Указанные лица должны при себе иметь документы, удостоверяющие личность.

Рассмотрение апелляции не является пересдачей ГИА.

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

об отклонении апелляции, если изложенные в ней сведения о нарушениях порядка проведения государственной итоговой аттестации не подтвердились и (или) не повлияли на результат ГИА;

об удовлетворении апелляции, если изложенные в ней сведения о допущенных нарушениях порядка проведения государственной итоговой аттестации 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. Выпускнику предоставляется возможность пройти ГИА в дополнительные сроки, установленные образовательной организацией без отчисления такого выпускника из образовательной организации в срок не более четырёх месяцев после подачи апелляции.

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 демонстрационного экзамена, письменные ответы выпускника (при их наличии), результаты работ выпускника, подавшего апелляцию, видеозаписи хода проведения демонстрационного экзамена (при наличии).

В случае рассмотрения апелляции о несогласии с результатами ГИА, полученными при защите дипломного проекта (работы), секретарь ГЭК не позднее следующего рабочего дня с момента поступления апелляции направляет в апелляционную комиссию дипломный проект (работу), протокол заседания ГЭК.

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 выпускника (при их наличии).

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 выпускника и выставления новых результатов в соответствии с мнением апелляционной комиссии.

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 выпускника в течение трех рабочих дней со дня заседания апелляционной комиссии.

Решение апелляционной комиссии является окончательным и пересмотру не подлежит.

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

ОСОБЕННОСТИ ПРОВЕДЕНИЯ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ ДЛЯ ВЫПУСКНИКОВ ИЗ ЧИСЛА ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ, ДЕТЕЙ-ИНВАЛИДОВ И ИНВАЛИДОВ

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

При проведении ГИА обеспечивается соблюдение следующих общих требований:

проведение ГИА для выпускников с ограниченными возможностями здоровья, выпускников из числа детей-инвалидов и инвалидов в одной аудитории совместно с выпускниками, не имеющими ограниченных возможностей здоровья, если это не создает трудностей для выпускников при прохождении ГИА;

присутствие в аудитории, центре проведения экзамена тьютора, ассистента, оказывающих выпускникам необходимую техническую помощь с учетом их индивидуальных особенностей (занять рабочее место, передвигаться, прочитать и оформить задание, общаться с членами ГЭК, членами экспертной группы);

пользование необходимыми выпускникам техническими средствами при прохождении ГИА с учетом их индивидуальных особенностей;

обеспечение возможности беспрепятственного доступа выпускников в аудитории, туалетные и другие помещения, а также их пребывания в указанных помещениях (наличие пандусов, поручней, расширенных дверных проемов, лифтов, при отсутствии лифтов аудитория должна располагаться на первом этаже, наличие специальных кресел и других приспособлений).

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

а) для слепых:

задания для выполнения, а также инструкция о порядке ГИА, комплект оценочной документации, задания демонстрационного экзамена 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;

выпускникам для выполнения задания при необходимости предоставляется комплект письменных принадлежностей и бумага для письма рельефно-точечным шрифтом Брайля, компьютер со специализированным программным

обеспечением для слепых;

б) для слабовидящих:

обеспечивается индивидуальное равномерное освещение не менее 300 люкс;

выпускникам для выполнения задания при необходимости предоставляется увеличивающее устройство;

задания для выполнения, а также инструкция о порядке проведения государственной аттестации оформляются увеличенным шрифтом;

в) для глухих и слабослышащих, с тяжелыми нарушениями речи:

обеспечивается наличие звукоусиливающей аппаратуры коллективного пользования, при необходимости предоставляется звукоусиливающая аппаратура индивидуального пользования;

г) 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;

д) также для выпускников из числа лиц с ограниченными возможностями здоровья и выпускников 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) .

Выпускники или родители (законные представители) несовершеннолетних выпускников 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 ПМПК, а дети-инвалиды, инвалиды - оригинала или заверенной копии справки, а также копии рекомендаций ПМПК при наличии.