Требования к типовому автоматизированному рабочему месту муниципального сегмента региональной информационной системы

1 Требования к системе защиты информации

1.1 Общие требования

1.1.1 Требования к структуре и функционированию

АРМ муниципального сегмента РИС ЕГЭ должен иметь подключение к ресурсам сетей связи общего пользования.

Режим обработки ПДн – многопользовательский.

Режим разграничения прав доступа пользователей ИСПДн – система с разграничением прав доступа.

Перечень мероприятий по обеспечению безопасности ПДн при их обработке в муниципальном сегменте РИС ЕГЭ должен быть определен исходя из необходимости реализации мер защиты информации ГИС 3-го класса защищенности (К3).

.1.1.1.1 Перечень подсистем, их назначение и основные характеристики

Подсистема идентификации и аутентификации субъектов доступа и объектов доступа

Подсистема идентификации и аутентификации субъектов доступа и объектов доступа должна обеспечивать присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).

Подсистема должна реализовывать меры защиты информации ГИС 3-го класса защищенности (К3):

Меры защиты информации в информационных системах

Идентификация и аутентификация пользователей, являющихся работниками оператора
Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов
Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации
Защита обратной связи при вводе аутентификационной информации
Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)

Подсистема управление доступом субъектов доступа к объектам доступа

Подсистема управления доступом субъектов доступа к объектам доступа должна обеспечивать управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивать контроль соблюдения этих правил.

Подсистема должна реализовывать меры защиты информации ГИС 3-го класса защищенности (К3):

Меры защиты информации в информационных системах
Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей
Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа
Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы
Назначение минимально необходимых прав и привилегий пользователям, администраторам и

лицам, обеспечивающим функционирование информационной системы
Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)
Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу
Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации
Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети
Регламентация и контроль использования в информационной системе технологий беспроводного доступа
Регламентация и контроль использования в информационной системе мобильных технических средств
Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)

Подсистема ограничения программной среды

Подсистема ограничения программной среды должна обеспечивать установку и (или) запуск только разрешенного к использованию в информационной системе программного обеспечения или исключать возможность установки и (или) запуска запрещенного к использованию в информационной системе программного обеспечения.

Подсистема должна реализовывать меры защиты информации ГИС 3-го класса защищенности (К3):

Меры защиты информации в информационных системах
Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов

Подсистема защиты машинных носителей информации

Подсистема защиты машинных носителей информации (средства обработки (хранения) информации, съемные машинные носители информации) должна исключать возможность несанкционированного доступа к машинным носителям и хранящейся на них информации, а также несанкционированное использование съемных машинных носителей информации.

Подсистема должна реализовывать меры защиты информации ГИС 3-го класса защищенности (К3):

Меры защиты информации в информационных системах
Учет машинных носителей информации
Управление доступом к машинным носителям информации
Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания)

Подсистема регистрации событий безопасности

Подсистема регистрации событий безопасности должна обеспечивать сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.

Подсистема должна реализовывать меры защиты информации ГИС 3-го класса защищенности (К3):

Меры защиты информации в информационных системах
Определение событий безопасности, подлежащих регистрации, и сроков их хранения
Определение состава и содержания информации о событиях безопасности, подлежащих регистрации
Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения
Реагирование на сбои при регистрации событий

безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти
Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них
Генерирование временных меток и (или) синхронизация системного времени в информационной системе
Защита информации о событиях безопасности

Подсистема антивирусной защиты

Подсистема антивирусной защиты должна обеспечивать обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

Подсистема должна реализовывать меры защиты информации ГИС 3-го класса защищенности (К3):

Меры защиты информации в информационных системах
Реализация антивирусной защиты
Обновление базы данных признаков вредоносных компьютерных программ (вирусов)

Подсистема обнаружения (предотвращения) вторжений

Подсистема обнаружения (предотвращения) вторжений должна обеспечивать обнаружение действий в информационной системе, направленных на преднамеренный несанкционированный доступ к информации, специальные воздействия на информационную систему и (или) информацию в целях ее добывания, уничтожения, искажения и блокирования доступа к информации, а также реагирование на эти действия.

Меры защиты информации для ГИС 3 класса защищенности не предъявляются.

Подсистема контроля (анализа) защищенности информации

Подсистема контроля (анализа) защищенности информации должна обеспечивать контроль уровня защищенности информации, содержащейся в информационной системе, путем проведения мероприятий по анализу защищенности информационной системы и тестированию ее системы защиты информации.

Подсистема должна реализовывать меры защиты информации ГИС 3-го класса защищенности (К3):

Меры защиты информации в информационных системах
Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей
Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации
Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации
Контроль состава технических средств, программного обеспечения и средств защиты информации
Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе

Подсистема обеспечения целостности информационной системы и информации

Подсистема обеспечения целостности информационной системы и информации должна обеспечивать обнаружение фактов несанкционированного нарушения целостности информационной системы и содержащейся в ней

информации, а также возможность восстановления информационной системы и содержащейся в ней информации.

Подсистема должна реализовывать меры защиты информации ГИС 3-го класса защищенности (К3):

Меры защиты информации в информационных системах
Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций

Подсистема обеспечения доступности информации

Подсистема обеспечения доступности информации должна обеспечивать авторизованный доступ пользователей, имеющих права по такому доступу, к информации, содержащейся в информационной системе, в штатном режиме функционирования информационной системы.

Меры защиты информации для ГИС 3 класса защищенности не предъявляются.

Подсистема защиты среды виртуализации

Подсистема защиты среды виртуализации должна исключать несанкционированный доступ к информации, обрабатываемой в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры, а также воздействие на информацию и компоненты, в том числе к средствам управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системе хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам, а также системе резервного копирования и создаваемым ею копиям.

Подсистема должна реализовывать меры защиты информации ГИС 3-го класса защищенности (К3):

Меры защиты информации в информационных системах
Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации
Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин
Регистрация событий безопасности в виртуальной инфраструктуре
Реализация и управление антивирусной защитой в виртуальной инфраструктуре

Подсистема защиты технических средств

Подсистема защиты технических средств должна исключать несанкционированный доступ к стационарным техническим средствам, обрабатывающим информацию, средствам, обеспечивающим функционирование информационной системы (далее – средства обеспечения функционирования), и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий, а также защиту информации, представленной в виде информативных электрических сигналов и физических полей.

Подсистема должна реализовывать меры защиты информации ГИС 3-го класса защищенности (К3):

Меры защиты информации в информационных системах
Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования
Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения

функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены
Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр

Подсистема защиты информационной системы, ее средств, систем связи и передачи данных

Подсистема защиты информационной системы, ее средств, систем связи и передачи данных должны обеспечивать защиту информации при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы, проектных решений по ее системе защиты информации, направленных на обеспечение защиты информации.

Подсистема должна реализовывать меры защиты информации ГИС 3-го класса защищенности (К3):

Меры защиты информации в информационных системах
Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи
Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств
Защита беспроводных соединений, применяемых в информационной системе

Защита мобильных технических средств, применяемых в информационной системе

1.1.1.2 Требования к характеристикам взаимосвязей между компонентами СЗПДн, её совместимости и способам обмена информацией

Компонентами СЗПДн являются программные и программно-аппаратные средства, реализующие в муниципальном сегменте РИС ЕГЭ функции защиты информации.

Взаимосвязь между компонентами СЗПДн должна обеспечиваться их интеграцией в действующую СЗПДн ИСПДн и муниципальный сегмент РИС ЕГЭ путем доработки (модернизации) последнего.

Вновь устанавливаемые средства должны быть совместимы со штатным ПО муниципального сегмента РИС ЕГЭ.

1.1.1.3 Требования к режимам функционирования

Комплекс средств защиты (КСЗ) должен обеспечивать следующие режимы обработки:

- коллективный (многопользовательский).

СЗПДн должна обеспечивать следующие режимы разграничения прав доступа пользователей муниципального сегмента РИС ЕГЭ:

- с разграничением прав доступа (разные права доступа);

СЗПДн должна обеспечивать следующие режимы применения (функционирования):

- непрерывного длительного применения (при круглосуточном режиме работы);

- многократного циклического применения для САЗ.

1.1.1.4 Требования по диагностированию системы

СЗПДн должна иметь встроенные средства диагностирования и (или) использовать функции контроля целостности, входящих в состав СЗИ.

1.1.1.5 Перспективы развития и модернизации системы

СЗПДн должна обеспечивать возможность масштабирования системы путем применения дополнительных средств защиты без существенных ограничений работоспособности муниципального сегмента РИС ЕГЭ.

1.1.1.6 Требования к численности и квалификации персонала СЗПДн и режиму его работы

СЗПДн не должна увеличивать численность персонала Заказчика, а также не должна изменять требования к квалификации персонала, порядку его подготовки, контролю знаний и навыков.

Режим работы персонала определяется соответствующими должностными и регламентирующими инструкциями Заказчика и его подразделений.

1.1.2 Требования к показателям назначения

Параметрами, характеризующими степень соответствия СЗПДн её назначению, является достижение показателей защищенности муниципального сегмента РИС ЕГЭ, в виде мероприятий, обеспечивающих соответствие СЗПДн «Требований о защите информации, не составляющей государственную тайну, содержащихся в государственных информационных системах» и достаточных для нейтрализации актуальных угроз безопасности ПДн, определенных в соответствии с Моделью угроз.

1.1.3 Требования к надежности

В общем виде требования к надежности СЗПДн должны соответствовать требованиям по надежности, заданным для ИСПДн, в том числе по времени восстановления.

Вместе с тем, надежность СЗПДн в условиях и режимах эксплуатации, установленных п. 1.1.1.3 настоящего Отчета, должна характеризоваться значениями показателей надежности (ПН), определяемыми свойствами ремонтопригодности элементов СЗПДн в случае их отказа или отказа сбойного характера (сбоя):

– среднее время восстановления на объекте эксплуатации силами Заказчика – не более 8 ч;

– средний срок службы – не менее 5 лет (или в установленных случаях определяется сроком действия документа, подтверждающего оценку соответствия требованиям безопасности информации).

Ограничения по способам обеспечения заданных значений ПН, определяются тем, что защита СЗПДн от сбоев и отказов, должна обеспечиваться средствами и системами бесперебойного питания, программными средствами архивирования и резервного копирования, реализуемыми в муниципальном сегменте РИС ЕГЭ вне работ, выполняемых по настоящему Отчету.

Восстановление свойств функций безопасности СЗПДн после сбоев и отказов оборудования должно обеспечиваться в соответствии с требованиями РД ФСТЭК России, установленных для соответствующих средств и систем защиты информации.

При этом, отказ СЗИ не должен приводить к разрушению программ и данных, обеспечивающих нормальное функционирование муниципального сегмента РИС ЕГЭ.

Компоненты СЗПДн могут быть невосстанавливаемыми, если их ремонт силами Заказчика не предусмотрен. Для невосстанавливаемых компонент должно быть предусмотрено следующее:

- для программных компонент – ведение двух копий ПО, их периодическое обновление и контроль работоспособности;

- для аппаратных компонент – ведение резервирования и контроль их работоспособности.

По характеристикам последствий отказов СЗПДн должна состоять из компонент, отказы или переход в предельное состояние которых не приводит к последствиям катастрофического (критического) характера (без угрозы для

жизни и здоровья людей, незначительным или «умеренным» экономическим потерям).

Вышеуказанные требования к надежности могут уточняться на этапах проектирования, предварительных и приемо-сдаточных испытаниях по показателям надежности, заявленным производителями в эксплуатационной документации, прилагающейся к СЗИ, поставляемым в рамках выполнения настоящего Отчета.

1.1.4 Требования по безопасности

При монтаже электроустановок должны выполняться требования ГОСТ 12.3.032-84.

СЗПДн не должна нарушать защиту от воздействия электрического тока, электромагнитных полей, акустических шумов и т.п., а также ухудшать допустимые уровни освещенности, вибрационных и шумовых нагрузок, установленные в муниципальном сегменте РИС ЕГЭ.

1.1.5 Требования к эргономике и технической эстетике

Обеспечение комфортности условий работы персонала и требований к технической эстетике не является предметом работ, выполняемых по настоящему Отчету.

СЗПДн не должна ухудшать установленные в ИСПДн эргономические требования, если они были выполнены в соответствии с:

- ГОСТ 20.39.108-85 Комплексная система общих технических требований. Требования по эргономике, обитаемости и технической эстетике. Номенклатура и порядок выбора;
- ГОСТ 12.2.032-78 Система стандартов безопасности труда. Рабочее место при выполнении работ сидя. Общие эргономические требования;
- ГОСТ 12.2.033-78 Система стандартов безопасности труда. Рабочее место при выполнении работ стоя. Общие эргономические требования;

– ГОСТ 21480-76. Система «Человек-машина». Мнемосхемы. Общие эргономические требования;

– ГОСТ 21786-76. Система «Человек-Машина». Сигнализаторы звуковые неречевых сообщений. Общие эргономические требования;

– ГОСТ 21958-76. Система «Человек-Машина». Зал и кабины операторов. Взаимное расположение рабочих мест. Общие эргономические требования;

– ГОСТ 21829-76. Система «Человек-Машина». Кодирование зрительной информации. Эргономические требования;

– ГОСТ 21889-76. Система «Человек-Машина». Кресло человека-оператора. Общие эргономические требования;

– ГОСТ 22269-79. Система «Человек-Машина». Рабочее место оператора. Взаимное расположение элементов рабочего места. Общие эргономические требования;

– ГОСТ 29.05.002-82 Система стандартов эргономических требований и эргономического обеспечения. Индикаторы цифровые знакосинтезирующие. Общие эргономические требования;

– ГОСТ 29.05.006-85 Система стандартов эргономических требований и эргономического обеспечения. Трубки электронно-лучевые приемные. Общие эргономические требования;

– ГОСТ 30.001-83 Система стандартов эргономики и технической эстетики. Основные положения;

– ГОСТ ИСО 8995-2002 Принципы зрительной эргономики. Освещение рабочих систем внутри помещений;

– ГОСТ Р 50923-96 Дисплеи. Рабочее место оператора. Общие эргономические требования и требования к производственной среде. Методы измерения;

- ГОСТ Р 50948-2001 Средства отображения информации индивидуального пользования. Общие эргономические требования и требования безопасности;
- ГОСТ Р 50949-2001 Средства отображения информации индивидуального пользования. Методы измерений и оценки эргономических параметров и параметров безопасности;
- ГОСТ Р 52324-2005 Эргономические требования к работе с визуальными дисплеями, основанными на плоских панелях. Часть 2. Эргономические требования к дисплеям с плоскими панелями;
- ГОСТ Р ИСО 13406-1-2007 Эргономические требования к проведению офисных работ с использованием плоскопанельных терминалов. Часть 1. Введение;
- ГОСТ Р 52870-2007 Средства отображения информации коллективного пользования. Требования к визуальному отображению информации и способы измерения;
- ГОСТ Р ИСО 15265-2006 Менеджмент риска. Основы стратегии оценки риска для предупреждения стресса и дискомфорта в термальных рабочих средах;
- ГОСТ Р ИСО 9241-3-2003 Эргономические требования при выполнении офисных работ с использованием видеодисплейных терминалов (ВДТ). Часть 3. Требования к визуальному отображению информации;
- ГОСТ Р ИСО 9241-7-2007 Эргономические требования при выполнении офисных работ с использованием видеодисплейных терминалов (ВДТ). Часть 7. Требования к дисплеям при наличии отражений;
- ГОСТ Р ИСО 9241-8-2007 Эргономические требования при выполнении офисных работ с использованием видеодисплейных терминалов (ВДТ). Часть 8. Требования к отображаемым цветам.

1.1.6 Требования к эксплуатации, техническому обслуживанию, ремонту и хранению компонентов СЗПДн

В эксплуатационной документации на устанавливаемые СЗИ должны содержаться рекомендации по регламенту обслуживания СЗИ и составу персонала, минимально достаточному для обеспечения работы.

Эксплуатационная документация должна содержать рекомендации администратору безопасности информации по восстановлению работоспособности СЗИ.

1.1.7 Требования по сохранности информации

Устойчивость СЗПДн к внутренним воздействующим факторам на информацию (отказы, сбои, ошибки) обеспечивается в соответствии с требованиями по надежности и должна соответствовать устойчивости функционирования ИСПДн или ее компонентов по ГОСТ 16325, ГОСТ 20397, ГОСТ 21552, ГОСТ 27201.

Технические средства СЗПДн должны обеспечивать сохранность информации при отключении электропитания, при авариях, а также в условиях неблагоприятных природных явлении и стихийных бедствий.

1.1.8 Требования к средствам защиты от внешних воздействий

Предотвращение изменения информации за счет внешних воздействий и факторов на СЗПДн должно соответствовать требованиям, предъявляемым к ее компонентам по ГОСТ 16325, ГОСТ 20397. ГОСТ 21552, ГОСТ 27201, которые, при необходимости, уточняются Заказчиком.

Требования по предотвращению изменения защищаемой информации за счет внешних побочных явлений (электромагнитных полей) устанавливаются в соответствии с нормами по электромагнитной совместимости и нормативными документами по показателям, действующим в муниципальном сегменте РИС ЕГЭ, которые, при необходимости, уточняются Заказчиком на стадии технического проектирования.

1.2 Требования к функциям (задачам), выполняемым СЗПДн (функциональные требования)

Для предотвращения актуальных угроз безопасности ПДн, определенных в «Модели угроз…», в СЗПДн должно обеспечиваться выполнение следующих задач:

1) При угрозе выявления паролей.

В муниципальном сегменте должны применяться:

- физическая охрана ИС, предусматривающая контроль доступа в помещения ИС посторонних лиц, наличие надежных препятствий для несанкционированного доступа в помещения;

- предотвращение внедрения в информационные системы вредоносных программ (программ-вирусов) и программных закладок;

- анализ защищенности информационных систем, предполагающий применение специализированных программных средств (сканеров безопасности) и иные методы (способы) защиты информации

2) При угрозе удаленного запуска приложений.

В муниципальном сегменте должны применяться:

- проверка подлинности отправителя (удаленного пользователя) и целостности передаваемых по информационно-телекоммуникационной сети Интернет (сети связи общего пользования) данных;

- управление доступом к защищаемым ПДн информационной системы;

- использование атрибутов безопасности и иные методы (способы) защиты информации.

3) При угрозе внедрения по сети вредоносных программ.

В муниципальном сегменте должны применяться:

- межсетевое экранирование с целью управления доступом, фильтрации сетевых пакетов и трансляции сетевых адресов для скрытия структуры информационной системы;

- обнаружение вторжений в ИС, нарушающих или создающих предпосылки к нарушению установленных требований по обеспечению безопасности ПДн;

- анализ защищенности информационных систем, предполагающий применение специализированных программных средств (сканеров безопасности);

- наличие средств восстановления системы защиты ПДн, предусматривающих ведение двух копий программных компонент средств защиты информации, их периодическое обновление и контроль работоспособности;

- идентификация и проверка подлинности пользователя при входе в систему ИС по паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов;

- регистрация входа (выхода) пользователя в систему (из системы) либо регистрация загрузки и инициализация операционной системы и ее программного останова.

4) При угрозе сбоя системы электроснабжения.

В муниципальном сегменте ко всем ключевым элементам ИСПДн должны быть подключены источники бесперебойного питания и осуществляться резервное копирование информации.

5) При угрозе кражи носителей информации, уничтожение и модификация информации, содержащей ПДн.

В муниципальном сегменте должны быть выполнены следующие мероприятия:

- введен контроль доступа (разрешительная система допуска) в контролируемую зону;

- установлена охранная сигнализация, двери закрываться на замок;

- ведение учета и хранения носителей в сейфе;

- разработана матрица доступа, доступ пользователей к информационным ресурсам должен осуществляться в соответствии с матрицей, в соответствующих журналах должно регистрироваться начало и окончание работ пользователей;

- съемные МНИ, предназначенные для обработки и хранения ПДн, должны учитываться и маркироваться, их выдача (прием) должна регистрироваться в журнале;

- должна осуществляться также идентификация и проверка подлинности пользователя при входе в систему ИС по паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов, а также регистрация входа (выхода) пользователя в систему (из системы) либо регистрация загрузки и инициализация операционной системы и ее программного останова.

В рамках выполнения работ по настоящему Отчету решение вышеперечисленных задач должно быть достигнуто (и ограниченно) следующими способами:

- применением средств защиты информации от НСД;
- применением средств межсетевого экранирования;
- применением средств антивирусной защиты;
- применение средств анализа защищенности;
- применением средств криптографической защиты информации;
- применением организационных и технических мер, предусматривающих использование реализованных в СЗИ ИСПДн и муниципальном сегменте РИС ЕГЭ способов разграничения, контроля и управления доступом к защищаемым ресурсам и помещениям, тестирования и контроля (аудита) безопасности информации, обеспечения установленного режима безопасности, физической

защиты, ТСО, архитектурно-планировочных решений, электромагнитной совместимости.

Функции, которые должны быть реализованы в СЗПДн для решения вышеперечисленных задач, определяются следующим перечнем:

- предупреждение о проявлении угроз безопасности информации;
- обнаружение, нейтрализацию и локализацию воздействия угроз безопасности информации;
- управление доступом к защищаемой информации;
- восстановление системы защиты информации и защищаемой информации после воздействия угроз;
- регистрацию событий и попыток несанкционированного доступа к защищаемой информации и несанкционированного воздействия на нее;
- обеспечение контроля функционирования средств и системы защиты информации и немедленное реагирование на их выход из строя.

Необходимый состав функций, которые должны быть реализованы в СЗПДн для решения вышеуказанных задач по каждой подсистеме защиты, определяются характеристиками, указанными в п. 2.1.1.1.1 настоящего Отчета и устанавливаются на стадии технического проектирования.

1.3 Требования к видам обеспечения

1.3.1 Требования к математическому обеспечению

Не предъявляются. Разработка математических методов, моделей и алгоритмов в соответствии с настоящим Отчете не предусмотрена.

1.3.2 Требования к информационному обеспечению

СЗПДн не должна нарушать действующие в ИСПДн требования к:

- составу, структуре и способам организации данных;
- информационному обмену между компонентами системы;
- информационной совместимости со смежными системами;

– применению СУБД;

– к защите данных от разрушений при авариях и сбоях в электропитании системы;

– контролю, хранению, обновлению и восстановлению данных;

– процедуре придания юридической силы документам, продуцируемым техническими средствами ИСПДн.

Обеспечение требований к структуре процесса сбора, обработки, передачи данных в системе и представления данных определяется в соответствии характеристиками подсистем СЗПДн, заданными в п. 1.1.1.1 настоящего Отчета.

1.3.3 Требования к лингвистическому обеспечению

Диалоговый режим интерфейсов СЗИ при взаимодействии с пользователем должен обеспечивать поддержку русского языка.

1.3.4 Требования к программно-аппаратному обеспечению

Все программные и программно-аппаратные СЗИ должны быть покупными. Разработка СЗИ в рамках работ по настоящему Отчету не предусматривается.

Программные средства защиты информации должны функционировать в существующей сетевой инфраструктуре муниципального сегмента РИС ЕГЭ совместно с общим, специальным и сетевым программным обеспечением и не нарушать функциональные характеристики объектов защиты.

1.3.5 Требования к техническому обеспечению

Не предъявляются.

1.3.6 Требования к метрологическому обеспечению

Не предъявляются.

1.3.7 Требования к организационному обеспечению

СЗПДн не должна изменять действующую в муниципальном сегменте РИС ЕГЭ:

- структуру и функции подразделений, участвующих в функционировании системы и обеспечивающих её эксплуатацию;
- организацию функционирования системы и порядок взаимодействия персонала СЗИ и персонала муниципального сегмента РИС ЕГЭ.

Защита от ошибочных действий персонала СЗПДн определяется в соответствии с характеристиками подсистем СЗПДн, заданными в п. 1.1.1.1 настоящего Отчета.

Организационные мероприятия должны обеспечивать защиту от преднамеренных действий пользователей, содержать меры по разграничению доступа в контролируемую зону и помещения, где расположены аппаратно-программные средства муниципального сегмента РИС ЕГЭ.

Квалификация персонала, обслуживающего СЗПДн, должна соответствовать текущим требованиям к уровню знаний предметной области. Персонал должен иметь соответствующие знания проблемной части ИСПДн, реализации каждого процесса, выполняющегося в ИСПДн, а также достаточный уровень знаний руководящих документов ФСБ России и ФСТЭК России.

1.4 Описание решения

Решение обеспечивается применением следующих средств защиты информации:

- средства защиты информации «Secret Net 6» (Вариант К);
- программного изделия «Kaspersky Endpoint Security 10 для Windows»;
- сетевого сканера безопасности XSpider 7.8;
- программного комплекса «ViPNet Клиент, версия 3.2»;

- программой поиска и гарантированного уничтожения информации на дисках Terrier (версия 3.0).

Сертификаты средств защиты информации:

- Сертификат соответствия ФСТЭК России №1549/1 от 26 мая 2010г., продлен до 26 мая 2016г., удостоверяющий, что программный комплекс "ViPNet CUSTOM 3.2" является программным средством защиты от несанкционированного доступа к информации в сетях с IP-протоколом, соответствует требованиям руководящих документов "Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей" (Гостехкомиссия России, 1999) - по 3 уровню контроля, "Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации" (Гостехкомиссия России, 1997) - по 3 классу защищенности и заданию по безопасности "Программный комплекс "ViPNet CUSTOM 3.2", имеет оценочный уровень доверия ОУД 4+ в соответствии с требованиями руководящего документа "Безопасность информационных технологий" (Гостехкомисия Россси, 2002), а также может использоваться при создании автоматизированных систем до класса защищенности 1В включительно и для защиты информации в информационных системах персональных данных до 1 класса.
- Сертификат соответствия ФСБ России №СФ/525-2224 от 25 сентября 2013г., действителен до 25 сентября 2016г., удостоверяющий, что изделие «Программный комплекс ViPNet Client 3.2 КС3» соответствует требованиям ФСБ России к устройствам типа межсетевые экраны по 4 классу защищенности;

- Сертификат соответствия ФСБ России №СФ/124-2178 от 17 июля 2013г., действителен до 17 июля 2016г., удостоверяющий, что изделие "Программный комплекс ViPNet Client 3.2 КС3" соответствует требованиям ФСБ России к средствам криптографической защиты информации класса КС3 и возможность применения для криптографической защиты информации не содержащей сведений, составляющих государственную тайну;
- Сертификат соответствия ФСТЭК России №2227 от 03 декабря 2010г., продлен до 03 декабря 2016г., удостоверяющий, что средство защиты информации Secret Net 6 (вариант К) является программным средством защиты от несанкционированного доступа к информации, не содержащей государственную тайну, соответствует требованиям руководящих документов "Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации" (Гостехкомиссия России, 1992) - по 5 классу защищенности , "Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей" (Гостехкомиссия России, 1999) - по 4 уровню контроля.
- Сертификат соответствия ФСТЭК России №3247 от 24 октября 2014г., действителен до 24 октября 2017г., удостоверяющий, что сетевой сканер безопасности XSpider 7.8.24 является средством автоматизированного анализа защищенности и обнаружения уязвимостей автоматизированных систем, обрабатывающих информацию, не содержащих сведений, составляющих государственную тайну, соответствует требованиям руководящего документа «Защита от несанкционированного доступа к

информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999г.) - по 4 уровню контроля, технических условий и может применяться для анализа защищенности информационных систем персональных данных до 1 класса включительно.

- Сертификат соответствия ФСТЭК России №3025 от 25 ноября 2013г., действителен до 25 ноября 2016г., удостоверяющий, что программное изделие «Kaspersky Endpoint Security 10 для Windows» является средством антивирусной защиты и соответствует требованиям документов «Требования к средствам антивирусной защиты» (ФСТЭК России, 2012), «Профиль защиты средств антивирусной защиты типа Б второго класса защиты. ИТ.САВЗ.Б2.ПЗ» (ФСТЭК России, 2012), «Профиль защиты средств антивирусной защиты типа В второго класса защиты. ИТ.САВЗ.В2.ПЗ» (ФСТЭК России, 2012), «Профиль защиты средств антивирусной защиты типа Г второго класса защиты. ИТ.САВЗ.Г2.ПЗ» (ФСТЭК России, 2012).

Для обеспечения защиты информации, содержащейся в информационной системе, провести следующие мероприятия:

- разработка организационно-распорядительной документации;

- внедрение системы защиты информации ИС;

- аттестация ИС по требованиям защиты информации и ввод ее в действие;

- обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы.

2 Требования к нормативно-методической и организационно-распорядительной документации

Организационно-распорядительные документы должны четко обозначать ответственных за функционирование муниципального сегмента РИС ЕГЭ сотрудников и регламентировать их действия в области:

- доступа к базам ПДн;
- антивирусной защиты;
- парольной защиты;
- доступа к техническим средствам;
- восстановления работоспособности технических средств;
- проведения регламентных работ.

Для муниципального сегмента РСИ ЕГЭ необходимо разработать следующую организационно-распорядительную документацию в области обеспечения безопасности персональных данных:

1. Акт классификации информационной системы;
2. Приказ о контролируемой зоне в ИС;
3. Приказ об утверждении перечня лиц имеющих доступ к ИС;
4. Инструкция администратора информационной безопасности;
5. Инструкция пользователей и технология обработки информации;
6. Инструкция по проведению антивирусного контроля;
7. Инструкция по организации парольной защиты;
8. Инструкция по резервному копированию и восстановлению технических средств и программного обеспечения ИС;
9. Разрешительная система доступа в ИС;
10. Описание технологического процесса в ИС;
11. Журнал по учету мероприятий по контролю обеспечения защиты;
12. Журнал учета носителей информации в ИС;
13. Журнал учета средств защиты информации информационной системы;
14. Журнал регистрации смены паролей в ИС;

15. Модель угроз для ИС;
16. Технический паспорт на ИС;
17. Перечень баз данных, обрабатываемых в ИС;
18. План внутренних проверок режима защиты информации;
19. План мероприятий по обеспечению защиты информации;
20. Положение о порядке организации и проведения мероприятий по обеспечению безопасности персональных данных.

3 Требования к организационным мерам защиты информации

3.1 Меры обеспечения надёжности работы ИС

Необходимо:

- предусмотреть возможность замены устройств коммутации (коммутаторов, сетевых карт, межсетевых экранов и т.д.) – подготовить комплект ЗИП;
- предусмотреть периодическое резервное копирование информации;
- обеспечить АРМ источником бесперебойного питания.

3.2 Требования по эксплуатации

При эксплуатации ИС необходимо:

- обеспечить управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации;
- обеспечить установку (инсталляцию) только разрешенного к использованию программного обеспечения и (или) его компонентов;
- обеспечить учет машинных носителей информации;
- обеспечить управление доступом к машинным носителям информации;
- обеспечить уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации

для ремонта или утилизации, а также контроль уничтожения (стирания) ;

- определить события безопасности, подлежащих регистрации, и сроки их хранения;

- определить состав и содержание информации о событиях безопасности, подлежащих регистрации;

- обеспечить сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения;

- обеспечить реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти;

- обеспечить мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них;

- обеспечить защиту информации о событиях безопасности;

- обеспечить обновление базы данных признаков вредоносных компьютерных программ (вирусов);

- обеспечить выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей;

- обеспечить контроль установки обновлений программного обеспечения;

- обеспечить контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации;

- обеспечить контроль состава технических средств, программного обеспечения и средств защиты информации;

- обеспечить контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей,

реализации правил разграничения доступом, полномочий пользователей в информационной системе;

- обеспечить восстановление программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций;

- обеспечить контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены;

- обеспечить размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр;

- обеспечить запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно.

Для уменьшения угрозы внедрения вредоносных программ необходимо:

- обеспечить организационными мерами использование только учтенных сторонних носителей данных;

- обеспечить организационными мерами и средствами антивирусной защиты проверку сторонних носителей данных на наличие ВП.

.4 Требования к техническим мерам защиты

4.1 Размещение основных технических средств и систем

Размещение технических средств, предназначенных для обработки информации ограниченного доступа и вывода на печать (принтер) выполнить с

учетом максимального затруднения визуального просмотра информации посторонними лицами. Окна помещения должны быть оборудованы шторами (жалюзи), во время обработки информации шторы (жалюзи) на окнах должны быть закрыты.

4.2 Технические средства охраны

Необходимо помещение, в котором располагается муниципальный сегмент РИС ЕГЭ, оснастить техническими средствами охраны, включающие в себя:

1. Прибор приемно-контрольный;
2. Извещатель охранный на движение;
3. Извещатель охранный на разбитие стекла (при наличии окон);
4. Извещатель охранный магнитоконтактный (на входную дверь);
5. Свето-звуковой оповещатель.

4.3 Требования по вскрытию ТС

Для обеспечения отсутствия предпосылок к внедрению «закладок» в технические средства, осуществляющих обработку информации, ограниченного доступа, необходимо опечатать все технические средства для исключения их вскрытия.

5 Общие требования

Администратору безопасности ИСПДн необходимо пройти курсы по повышению квалификации специалистов в области защиты информации по программе, согласованной с ФСТЭК России.

Следует довести до пользователей муниципального сегмента РИС ЕГЭ содержание всех приказов, положений, регламентов и инструкций, необходимых для работы в муниципальном сегменте РИС ЕГЭ.

Ограничить доступ в технические помещения, в которых располагается серверное и коммутационным оборудование.

Требования к типовому автоматизированному рабочему месту общеобразовательных учреждений полностью идентичны требованиям к типовому автоматизированному рабочему месту муниципального сегмента региональной информационной системы.

3. Сметная стоимость выполнения требований к типовому автоматизированному рабочему месту муниципального сегмента региональной информационной системы.

№ п/п	Вид услуг	Кол-во	Цена руб. (с учетом НДС)	Сумма руб. (с учетом НДС)	Вид отчетности
1. Создание автоматизированного рабочего места					
1.1 Поставка технических средств, программного обеспечения					
1	Компьютер HP 280 G1 MT + монитор VV2072a (комплект), Intel Celeron G1840, DDR3 4Гб, 500Гб, Intel HD Graphics, DVD-RW, Windows 7 Professional, черный	1	32650	32650	Накладная
2	Источник бесперебойного питания IPPON Back Power Pro 400 New, 400ВА	1	3000	3000	Накладная
			Итого (пункты 1-2)	**35650**	**рублей с НДС**
1.2 Установка программного обеспечения					
3	Установка операционной системы Microsoft Windows 7	1	3500	3500	Акт установки
			Итого (пункт 3)	**3500**	**рублей с НДС**
			Итого (пункты 1-3)	***39150***	***рублей с НДС***
2. Создание системы защиты персональных данных					
2.1 Поставка средств защиты информации					
4	Средство защиты информации «Secret Net 6» (Вариант К)	1	10000	10000	Накладная
5	Программное изделие «Kaspersky Endpoint Security 10 для Windows»	1	8250	8250	Накладная
6	Сетевой сканер безопасности XSpider 7.8 (на 4 хоста)	1	10800	10800	Накладная
7	Программный комплекс «ViPNet Клиент, версия 3.2»	1	8100	8100	Накладная
8	Программа поиска и гарантированного уничтожения информации на дисках Terrier (версия 3.0)	1	4000	4000	Накладная
			Итого (пункты 4-8)	**41150**	**рублей с НДС**
2.2 Установка средств защиты информации					
9	Установка средства защиты информации «Secret Net 6» (Вариант К)	1	3500	3500	Акт установки
10	Установка программного изделия «Kaspersky Endpoint Security 10 для Windows»	1	3000	3000	Акт установки
11	Установка сетевого сканера безопасности XSpider 7.8	1	3000	3000	Акт установки
12	Установка программного комплекса	1	3500	3500	Акт установки

	«ViPNet Клиент, версия 3.2»				
13	Установка программы поиска и гарантированного уничтожения информации на дисках Terrier (версия 3.0)	1	3000	3000	Акт установки
			Итого (пункты 9-13)	**16000**	**рублей с НДС**
	2.3 Разработка организационно-распорядительной документации				
14	Разработка проектов ОРД	1	15000	15000	Проекты ОРД
			Итого (пункт 14)	**15000**	**рублей с НДС**
	2.4 Аттестация автоматизированного рабочего места				
15	Обследование автоматизированного рабочего места (АРМ) и проверка выполнения организационных и технических мероприятий по защите информации: - ознакомление с размещением АРМ, уточнение состава АРМ, контролируемой зоны, проверка обоснованности классификации АРМ; обоснование состава и характеристик системы защиты информации на АРМ;	1	3600	3600	Раздел в «Заключении..»
16	Разработка программы и методики аттестационных испытаний объекта информатизации и согласование ее с Заказчиком	1	2500	2500	Программа - методика
17	Проведение аттестационных испытаний системы защиты информации от несанкционированного доступа автоматизированного рабочего места	1	6500	6500	Протокол
18	Разработка документов по аттестации автоматизированного рабочего места	1	9200	9200	Заключение Аттестат
			Итого (пункты 15-18)	**21800**	**рублей с НДС**
			Итого (пункты 4-18)	***93950***	***рублей с НДС***
	3. Создание системы охранной сигнализации				
	3.1 Поставка технических средств охраны				
19	Прибор приемно-контрольный Кварц (версия 1), считыватель, 2 ключа	1	4000	4000	Накладная
20	Датчик движения Астра-5А	1	1200	1200	Накладная
21	Датчик акустический Стекло-3 (разбития стекла)	1	1400	1400	Накладная
22	Извещатель охранный магнитоконтактный ИО102-2	1	100	100	Накладная
23	Оповещатель свето-звуковой Маяк-12-КПМ2	1	600	600	Накладная
24	Считыватель Touch Memory (+2 ключа)	1	1000	1000	Накладная
25	Аккумулятор АКБ 12В, 1,2А\ч	1	1000	1000	Накладная
26	Кабель, 60м	1	600	600	Накладная

27	Пластиковый короб, 60м	1	800	800	Накладная
	Итого (пункты 19-27)			**10700**	**рублей с НДС**
	3.2 Установка и настройка технических средств охраны				
28	Монтаж линий охранной сигнализации; Установка, настройка, пуско-наладка технических средств охраны	1	20000	20000	Акт монтажа, установки, настройки, пуско-наладки
	Итого (пункт 28)			**20000**	**рублей с НДС**
	Итого (пункты 19-28)			***30700***	***рублей с НДС***
	ИТОГО (пункты 1 - 28)			**163800**	**рублей с НДС**