Приложение 1

к извещению об осуществлении закупки

**Описание объекта закупки**

**1.** **Предмет муниципального контракта**: оказание услуг по аттестации рабочих мест по требованиям безопасности информации, не составляющей государственную тайну (код ОКПД2 62.02.20.120).

**2. Используемые сокращения:**

АРМ - автоматизированное рабочее место;

ИСПДн – информационная система персональных данных;

ГИС – государственная информационная система;

МЭ – межсетевой экран;

НСД - несанкционированный доступ;

ОС – операционная система;

ПАК – программно-аппаратный комплекс;

ПДн – персональные данные;

ПО - программное обеспечение;

ПЭВМ - персональная электронно-вычислительная машина;

СЗИ – система защиты информации;

СЗПДн - система защиты информационной системы персональных данных;

СрЗИ - средство защиты информации;

СКЗИ - средства криптографической защиты информации;

ТЗ – описание объекта закупки, техническое задание;

ФСТЭК России - Федеральная служба по техническому и экспортному контролю России;

ФСБ России - Федеральная служба безопасности России.

**3.** **Общие требования к предоставляемым услугам:**

3.1. В соответствии с требованиями Заказчика должны быть оказаны услуги по проведению аттестации информационных систем персональных данных на 3 (трёх) автоматизированных рабочих местах отдела по организации деятельности комиссии по делам несовершеннолетних и защите их прав администрации города Югорска (создание системы защиты информации).

3.2. Цели и задачи оказания услуг:

Основной целью услуги является создание системы защиты информационной системы персональных данных администрации города Югорска.

Достижение указанной цели обеспечивается выполнением следующих задач:

1) выполнение требований нормативных правовых актов Российской Федерации, руководящих документов ФСТЭК России и ФСБ России, регламентирующих вопросы защиты персональных данных;

2) обеспечение безопасности информации и персональных данных при их обработке в ИСПДн путём нейтрализации актуальных угроз безопасности;

3) построение системы защиты информационной системы персональных данных.

3.3. Место оказания услуг: г. Югорск, Ханты-Мансийский автономный округ-Югра, Тюменская область, ул. Ленина, д.41.

3.4. Комплекс мероприятий должен соответствовать следующим нормативным правовым актам и руководящим документам:

- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;

- Указ Президента Российской Федерации от 17.03.2008 № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»;

- постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

- приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

- приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

- «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утверждённая ФСТЭК России 15.02.2008;

- «Методика оценки угроз безопасности информации», утверждённая ФСТЭК России 05.02.2021 г.;

- приказ ФСБ от 10.07.2014 № 378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищённости»;

- «Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», утверждённая приказом ФАПСИ от 13.06.2001 № 152.

**4. Объём и содержание оказываемых услуг**

4.1. Объектом защиты СЗИ является конфиденциальная информация, обрабатываемая в ИСПДн администрации города Югорска.

Подробное описание ИСПДн представлено в таблице 1.

Таблица 1. Описание ИСПДн

|  |  |
| --- | --- |
| Уровень защищённости ИСПДн | 3 |
| Класс защищённости | К3 |
| Категории ПДн | Специальные |
| Объем обрабатываемых ПДн | Менее 1 000 субъектов |
| Наличие подключения к сетям международного информационного обмена | ИСПДн, имеющая многоточечное подключение к сетям связи международного информационного обмена |
| Режим обработки ПДн | Многопользовательский |
| Структура ИСПДн | Локальная |
| Тип актуальных угроз | 3-ий тип |

Количество информационных систем, в которых ведётся обработка персональных данных – 1 шт (ИС «КДН»).

Количество рабочих станций, подлежащих защите – 3 шт.

Имеющиеся у заказчика средства защиты информации: право на использование программного обеспечения ViPNet Client for Windows 4.x (КС3) в количестве 1 шт. и лицензия на антивирусную защиту Kaspersky в количестве 3 шт. Сертифицированный медиа комплект антивирусной защиты Kaspersky у Заказчика имеется.

В соответствии с подпунктом 1 пункта 1 статьи 13 Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», ИСПДн относятся к государственным информационным системам.

4.2. Настоящее Описание объекта закупки предполагает выполнение следующих этапов услуги:

* + - 1. обследование информационной системы с целью определения текущего состояния обеспечения безопасности информации и определения состава и структуры системы защиты информации;
			2. формирование требований к системе защиты информации;
			3. разработка организационно-распорядительной документации по защите информации;
			4. поставка, установка и конфигурирование программных средств для обеспечения защиты персональных данных;
			5. оценка соответствия (аттестация) системы защиты информации требованиям безопасности информации.

4.3. Требования к содержанию услуги.

4.3.1. Обследование информационной системы включает в себя следующие работы:

* + - 1. Сбор сведений о ИСПДн (тип операционной системы, количество АРМ, структурная схема ИСПДн);
			2. Обследование состояния защищённости ИСПДн по требованиям безопасности информации осуществляется путём анкетирования, опроса специалистов и посещения объектов информатизации для изучения.

В ходе обследования:

- осуществляется сбор и систематизация данных об используемых основных и вспомогательных технических средствах и системах, а также каналах передачи данных;

- уточняется состав каждого выявленного объекта информатизации (ИСПДн);

- уточняется перечень информации, подлежащих защите на каждом объекте ИСПДн;

- уточняется состав защищаемой информации, обрабатываемой автоматизированным способом;

- собирается информация о защищённости ИСПДн на каждом объекте ИСПДн;

- уточняются условия расположения ИСПДн относительно границ контролируемой зоны;

- уточняются конфигурация, компоненты и топология ИСПДн, их физические, функциональные и технологические связи как внутри этих систем, так и с другими системами различного уровня и назначения;

- уточняются состав технических средств и систем, предполагаемых к использованию в СЗИ, условия их расположения, общесистемные и прикладные программные средства;

- производится сбор документации, необходимой для достижения целей обследования (методы и способы сбора документации определяются Исполнителем совместно с Заказчиком), в частности: действующих политик информационной безопасности; документов, определяющих организационную структуру Заказчика; сведений об ИТ-инфраструктуре; сведений о действующей системе обеспечения информационной безопасности;

- определяется состав ИСПДн и проводится её классификация (определение уровня защищённости ПДн в ИСПДн, класса защищённости ИСПДн).

Обследование и анализ имеющейся системы защиты информации и применяемых технических мер (средства защиты информации и т.п.).

В ходе обследования:

- уточняется состав используемых средств защиты информации;

- подготавливается описание существующей системы защиты для ИСПДн;

- уточняются режимы обработки информации в ИСПДн в целом и в отдельных её компонентах.

4.3.2. Формирование требований к системе защиты персональных данных включает в себя:

* + - 1. Определение актуальных угроз безопасности персональных данных;
			2. Определение уровней защищённости персональных данных;
			3. Уточнение и дополнение базового набора мер.

Актуальные угрозы безопасности информации определяются по результатам оценки возможностей и потенциала нарушителей (внешних, внутренних), анализа возможных уязвимостей ИСПДн, а также с учётом структурно-функциональных характеристик ИСПДн.

Класс защищённости ИСПДн определяется в соответствии с Приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

Уровень защищённости персональных данных при обработке в ИСПДн определяется в соответствии с Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Предварительно определённый уровень защищённости ПДн в ИСПДн – УЗ 3.

Предварительно определённый класс защищённости ИСПДн – К3.

Базовый набор мер, который необходимо реализовать при создании системы защиты информации с учётом предварительно определённых уровня защищённости ПДн в ИСПДн и класса защищённости ИСПДн, приведён в таблице 2.

Таблица 2 –Базовый набор мер, который необходимо реализовать

при создании системы защиты информации в ГИС (К3, УЗ3)

| **Условное обозначение и номер меры** | **Содержание мер по обеспечению безопасности персональных данных** |
| --- | --- |
|
|  |
| I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ) |
| ИАФ.1 | Идентификация и аутентификация пользователей, являющихся работниками оператора |
| ИАФ.3 | Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов |
| ИАФ.4 | Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации |
| ИАФ.5 | Защита обратной связи при вводе аутентификационной информации |
| ИАФ.6 | Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей) |
| II. Управление доступом субъектов доступа к объектам доступа (УПД) |
| УПД.1 | Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей |
| УПД.2 | Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа |
| УПД.3 | Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами |
| УПД.4 | Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы |
| УПД.5 | Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы |
| УПД.6 | Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе) |
| УПД.10 | Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу |
| УПД.11 | Разрешение (запрет) действий пользователей, разрешённых до идентификации и аутентификации |
| УПД.13 | Реализация защищённого удалённого доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети |
| УПД.14 | Регламентация и контроль использования в информационной системе технологий беспроводного доступа |
| УПД.15 | Регламентация и контроль использования в информационной системе мобильных технических средств |
| УПД.16 | Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы) |
| III. Ограничение программной среды (ОПС) |
| ОПС.3 | Установка (инсталляция) только разрешённого к использованию программного обеспечения и (или) его компонентов |
| IV. Защита машинных носителей информации (ЗНИ) |
| ЗНИ.1 | Учёт машинных носителей информации |
| ЗНИ.2 | Управление доступом к машинным носителям информации |
| ЗНИ.8 | Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) |
| V. Регистрация событий безопасности (РСБ) |
| РСБ.1 | Определение событий безопасности, подлежащих регистрации, и сроков их хранения |
| РСБ.2 | Определение состава и содержания информации о событиях безопасности, подлежащих регистрации |
| РСБ.3 | Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения |
| РСБ.4 | Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объёма (ёмкости) памяти |
| РСБ.5 | Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них |
| РСБ.6 | Генерирование временных меток и (или) синхронизация системного времени в информационной системе |
| РСБ.7 | Защита информации о событиях безопасности |
| VI. Антивирусная защита (АВЗ) |
| АВЗ.1 | Реализация антивирусной защиты |
| АВЗ.2 | Обновление базы данных признаков вредоносных компьютерных программ (вирусов) |
| VIII. Контроль (анализ) защищённости персональных данных (АНЗ) |
| АНЗ.1 | Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей |
| АНЗ.2 | Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации |
| АНЗ.3 | Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации |
| АНЗ.4 | Контроль состава технических средств, программного обеспечения и средств защиты информации |
| АНЗ.5 | Контроль правил генерации и смены паролей пользователей, заведения и удаления учётных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе |
| IX. Обеспечение целостности информационной системы и информации (ОЦЛ) |
| ОЦЛ.3 | Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций |
| XI. Защита среды виртуализации (ЗСВ) |
| ЗСВ.1 | Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации |
| ЗСВ.2 | Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин |
| ЗСВ.3 | Регистрация событий безопасности в виртуальной инфраструктуре |
| ЗСВ.9 | Реализация и управление антивирусной защитой в виртуальной инфраструктуре |
| ЗСВ.10 | Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей |
| XII. Защита технических средств (ЗТС) |
| ЗТС.2 | Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования |
| ЗТС.3 | 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 |
| ЗТС.4 | Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр |
| XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС) |
| ЗИС.3 | 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 |
| ЗИС.5 | Запрет несанкционированной удалённой активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удалённо, и оповещение пользователей об активации таких устройств |
| ЗИС.20 | Защита беспроводных соединений, применяемых в информационной системе |
| ЗИС.30 | Защита мобильных технических средств, применяемых в информационной системе |
| XV. Управление конфигурацией информационной системы и системы защиты персональных данных (УКФ) |
| УКФ.1 | Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных |
| УКФ.2 | Управление изменениями конфигурации информационной системы и системы защиты персональных данных |
| УКФ.3 | Анализ потенциального воздействия планируемых изменений в конфигурации информационной системы и системы защиты персональных данных на обеспечение защиты персональных данных и согласование изменений в конфигурации информационной системы с должностным лицом (работником), ответственным за обеспечение безопасности персональных данных |
| УКФ.4 | Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных |

Актуальные угрозы безопасности информации определяются по результатам оценки возможностей и потенциала нарушителей (внешних, внутренних), анализа возможных уязвимостей информационной системы персональных данных, возможных последствий от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности), а также с учётом структурно-функциональных характеристик ИСПДн.

В рамках данного этапа исполнитель производит анализ уязвимостей ИСПДн, сертифицированным ФСТЭК России сканером безопасности.

Требования к системе защиты информации определяются для ИСПДн с учётом адаптированного базового состава мер по защите информации в зависимости от уровня защищённости ПДн при их обработке в ИСПДн, класса защищённости ИСПДн и актуальных угроз безопасности информации и должны учитывать выявленные на данном этапе уязвимости ИСПДн.

Состав конкретных мер по защите информации определяется на основе адаптации и уточнения базового набора мер по обеспечению безопасности информации, с учётом структурно-функциональных характеристик, информационных технологий, особенностей функционирования ИСПДн (в том числе исключение из базового набора мер, непосредственно связанных с информационными технологиями, не используемыми в ИСПДн, или структурно-функциональными характеристиками, не свойственными ИСПДн).

При невозможности технической реализации отдельных выбранных мер по обеспечению безопасности информации, а также с учётом экономической целесообразности на этапах адаптации базового набора мер и (или) уточнения адаптированного базового набора мер разрабатываются иные (компенсирующие) меры, направленные на нейтрализацию актуальных угроз безопасности информации. При этом должны быть оценены достаточность и актуальность компенсирующих мер для блокирования (нейтрализации) угроз безопасности информации.

Результаты работ по формированию требований к системе защиты информации отражаются в следующих документах:

- Акт определения уровня защищённости ПДн при их обработке в ИСПДн;

- Акт классификации ИСПДн;

- Уточнённый состав мер по защите информации для реализации в системе защиты информации ИСПДн;

- Частное техническое задание на создание системы защиты информации;

- Модель угроз и нарушителя безопасности информации и персональных данных в ИСПДн.

4.3.3. Поставка программных средств, оборудования и товара для обеспечения защиты персональных данных.

Исполнителем поставляются программные средства для обеспечения защиты персональных данных в соответствии с таблицей 3.

Таблица 3

Требования к поставляемым программным средствам

для обеспечения защиты персональных данных

|  |  |  |
| --- | --- | --- |
| **№****п/п** | **Параметры требований к программным средствам для обеспечения защиты персональных данных** | **Требования к программным средствам для обеспечения защиты персональных данных** |
|  | Передача неисключительных прав на использование средства защиты информации от несанкционированного доступа (для платформ Windows) | Средство защиты информации (ПО) от несанкционированного доступа должно иметь следующие характеристики:1. Для применения на ПК под управлением операционных систем Windows XP, Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows Server 2003, Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016 в многопользовательском режиме их эксплуатации и поддержкой 32-х/64-х битных версий.2. Сертификация по требованиям Руководящих документов (РД) ФСТЭК России (Гостехкомиссии России) по не менее чем 5 классу защиты от НСД для СВТ и по не менее, чем по 4 классу защиты.3. Обеспечивать:- возможность настройки всех параметров из единой консоли администрирования;- разграничение прав пользователей при работе на ПЭВМ. Разграничения должны касаться доступа к объектам файловой системы (FAT и NTFS), доступа к сети, доступа к сменным накопителям. Должен быть реализован независимый от механизмов ОС механизм разграничения прав доступа к объектам файловой системы. Разграничения должны касаться всех пользователей – локальных, сетевых, доменных, терминальных. - блокировку файлов по расширению;- генерация сложных паролей;- возможность ограничивать его средствами, круг доступных сетевых ресурсов (с точностью до отдельных удалённых рабочих станция и отдельных папок общего доступа);- аудит действий пользователей, независимыми от ОС средствами (вход/выход, доступ к ресурсам, запуск процессов, печать документов, управление учётными записями и политиками безопасности). Должны вестись непрерывные журналы (т.е. новые записи не должны затирать более старые);- возможность локального и удалённого администрирования (управление пользователями, политиками безопасности, правами доступа, аудитом; просмотр журналов);- возможность регистрации доменных учётных записей с помощью маски (\*\\*);- возможность периодического контроля целостности файлов и программно-аппаратной среды, а также контроля по команде администратора и по расписанию.- очистку остаточной информации (принудительная зачистка определённых файлов и папок);- возможность организации режима замкнутой программной среды;- возможность самодиагностики основного функционала;- ведение двух копий программных средств защиты информации;- возможность создания отчёта по назначенным правам;- возможность ограничивать круг доступных сетевых ресурсов (с точностью до отдельных удалённых рабочих станций и отдельных папок общего доступа);- преобразование данных в файл-контейнер для хранения их на внешних носителях либо для передачи по различным каналам связи. Возможность использования встроенного алгоритма преобразования ГОСТ 28147-89, либо подключение внешнего криптопровайдера, в том числе сертифицированного;- удалённое администрирование;- централизованное управление защищёнными рабочими станциями при помощи специального модуля. С помощью этого модуля должно осуществляться централизованное управление учётными записями пользователей, политиками, правами пользователей. Также этим модулем должен осуществляться периодический сбор журналов со всех защищённых рабочих станций;- возможность построения иерархии управления при помощи специального модуля - менеджера, управляющего несколькими модулями централизованное управления;- установка должна производиться локально, с помощью модуля централизованного управления, средствами групповых политик AD;- сигнализация попыток несанкционированного доступа и его деактивации. Отправка сообщений о попытках несанкционированного доступа на почту;- должно быть полностью программной, но с возможностью подключения аппаратных средств считывания индивидуальных идентификаторов пользователей, включая идентификаторы Touch Memory (iButton), eTokenPro/Java(в том числе смарт-карты eToken), Rutoken, Rutoken ЭЦП.У поставляемой системы защиты информации срок действия лицензии должен быть - «бессрочно».Права на средство защиты информации от несанкционированного доступа передаются с сопутствующими дистрибутивами на физическом носителе. Физический носитель имеет формуляр, в котором указаны специальные учётные номера ФСТЭК России.Комплект поставки:- формуляр;- копия сертификата соответствия ФСТЭК России;- краткое руководство пользователя;- верифицированный дистрибутив (компакт диск).**Количество – 2 шт.** |
|  | Передача неисключительных прав на использование средства защиты информации от несанкционированного доступа (для платформ Windows) с модулем «Межсетевой Экран» | Средство защиты информации (ПО) от несанкционированного доступа должно иметь следующие характеристики:1. Должно быть предназначено для применения на ПК под управлением операционных систем Windows XP, Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows Server 2003, Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2 в многопользовательском режиме их эксплуатации и поддержкой 32-х/64-х битных версий.2. Должно быть сертифицировано по требованиям Руководящих документов (РД) ФСТЭК России (Гостехкомиссии России) по не менее чем 5 классу защиты от НСД для СВТ, по не ниже 4 классу защиты МЭ тип "В" (ИТ.МЭ.В4.ПЗ).Сертификат соответствия должен позволять обеспечивать 3 класс защищённости информационной системы.3. Должно обеспечивать:- возможность настройки всех параметров из единой консоли администрирования;- разграничение прав пользователей при работе на ПЭВМ. Разграничения должны касаться доступа к объектам файловой системы (FAT и NTFS), доступа к сети, доступа к сменным накопителям. Должен быть реализован независимый от механизмов ОС механизм разграничения прав доступа к объектам файловой системы. Разграничения должны касаться всех пользователей – локальных, сетевых, доменных, терминальных;- блокировку файлов по расширению;- генерация сложных паролей;- возможность ограничивать его средствами, круг доступных сетевых ресурсов (с точностью до отдельных удалённых рабочих станция и отдельных папок общего доступа);- аудит действий пользователей, независимыми от ОС средствами (вход/выход, доступ к ресурсам, запуск процессов, печать документов, управление учётными записями и политиками безопасности). Должны вестись непрерывные журналы (т.е. новые записи не должны затирать более старые);- возможность локального и удалённого администрирования (управление пользователями, политиками безопасности, правами доступа, аудитом; просмотр журналов);- возможность регистрации доменных учётных записей с помощью маски (\*\\*);- возможность периодического контроля целостности файлов и программно-аппаратной среды, а также контроля по команде администратора и по расписанию;- очистку остаточной информации (принудительная зачистка определённых файлов и папок);- возможность организации режима замкнутой программной среды;- возможность самодиагностики основного функционала;- ведение двух копий программных средств защиты информации;- возможность создания отчёта по назначенным правам;- возможность ограничивать круг доступных сетевых ресурсов (с точностью до отдельных удалённых рабочих станций и отдельных папок общего доступа);- гибкая настройка правил фильтрации в соответствии с сетевой моделью OSI всех уровней, в том числе:- настройка правил прикладного уровня с возможностью контроля определённых приложений (исполняемых модулей);- настройка правил на уровне указания сетевых драйверов (в частности, для корректной работы приложений типа «банк-клиент»);- настройка правил, действующих для определённых пользователей.- гибкую настройку уведомлений о попытках нарушения сетевых правил с возможностью запуска внешнего процесса при срабатывании правил;преобразование данных в файл-контейнер для хранения их на внешних носителях либо для передачи по различным каналам связи. Возможность использования встроенного алгоритма преобразования ГОСТ 28147-89, либо подключение внешнего криптопровайдера, в том числе сертифицированного;- удалённое администрирование;- централизованное управление защищёнными рабочими станциями при помощи специального модуля. С помощью этого модуля должно осуществляться централизованное управление учётными записями пользователей, политиками, правами пользователей. Также этим модулем должен осуществляться периодический сбор журналов со всех защищённых рабочих станций;- возможность построения иерархии управления при помощи специального модуля - менеджера, управляющего несколькими модулями централизованное управления;- установка должна производиться локально, с помощью модуля централизованного управления, средствами групповых политик AD;- сигнализация попыток несанкционированного доступа и его деактивации; - отправка сообщений о попытках несанкционированного доступа на почту;- должна быть полностью программной, но с возможностью подключения аппаратных средств считывания индивидуальных идентификаторов пользователей, включая идентификаторы Touch Memory (iButton), eTokenPro/Java(в том числе смарт-карты eToken), Rutoken, Rutoken ЭЦП.У поставляемой системы защиты информации срок действия лицензии должен быть не ниже «бессрочно»Права на средство защиты информации от несанкционированного доступа передаются с сопутствующими дистрибутивами на физическом носителе. Физический носитель имеет формуляр, в котором указаны специальные учётные номера ФСТЭК России.**Количество – 1 шт.** |

Программное обеспечение передаётся Заказчику в соответствии с действующим законодательством с предоставлением сублицензионного договора и актов приёма-передачи неисключительных прав.

4.3.4. Установка и настройка средств защиты информации осуществляется Исполнителем в соответствии с решениями, изложенными в техническом задании на систему защиты информационных систем персональных данных.

При установке и настройке СрЗИ должна производиться их интеграция с имеющимися средствами защиты информации. Настройка СрЗИ должна обеспечить функционирование подсистемы защиты от несанкционированного доступа, межсетевого экранирования и антивирусной защиты.

Настроенные средства защиты не должны нарушать функционирование защищаемых информационных систем персональных данных. В целях снижения вероятности возникновения ошибок и нарушения работы ИСПДн, настройка СрЗИ должна производиться последовательно в несколько этапов.

Настройка СрЗИ должна быть произведена для соответствующего уровня защищённости персональных данных и в соответствии с матрицей доступа пользователей к защищаемым ресурсам.

Результаты работ по установке и настройке средств защиты информации отражаются в следующих документах:

– акт установки и настройки средств защиты информации.

Установка и настройка программных СЗИ от НСД не должна существенно нарушать рабочий процесс Заказчика. Время прекращения функционирования не должно превышать 1,5 часа для АРМ, 1 час для серверов.

4.3.5. Разработка организационно-распорядительной документации по защите информации.

Разработка внутренних нормативных и организационно-распорядительных документов по защите информации с обеспечением доступа к онлайн-сервису по разработке, корректировке и поддержанию в актуальном состоянии организационной распорядительной документации по защите информации сроком не менее 12 месяцев, с внесением информации в онлайн-сервис для формирования комплекта организационно-распорядительной документации по защите информации.

Доступ к онлайн-сервису по разработке, корректировке и поддержанию в актуальном состоянии организационной распорядительной документации по защите информации предоставляется Заказчику путём передачи Права на использование Онлайн-сервиса сроком не менее 12 месяцев.

Онлайн-сервис должен обеспечивать выполнение следующих функций:

- предоставление возможности прохождения электронного согласования разрабатываемых документов специалистами Заказчика, с возможностью выбора маршрута согласуемого документа – последовательно/параллельно;

- двухфакторная аутентификация пользователей с применением связки логин – пароль, а также электронной подписи;

- защита подключения к сервису с использованием сертифицированного криптопровайдера;

- формирование актуального пакета нормативной распорядительной документации по защите персональных данных, систем согласно законодательству Российской Федерации;

- наличие функционала, позволяющего автоматизировать подготовку внутренних распорядительных документов;

- наличие инструментария для планирования мероприятий по защите информации с уведомлением пользователя о приближении запланированного мероприятия через сервис и на электронную почту;

- ведение в электронном виде (в режиме онлайн) всех журналов, формы которых присутствуют в формируемом пакете документов, с возможностью выгрузки журналов целиком, а также заданного интервала записей;

- ведение версионности (истории изменений) документов, с возможностью восстановления электронного документа из резервной копии;

- хранение подписанных электронной подписью документов;

- уведомление должностного лица, использующего онлайн-сервис, об обновлениях системы, изменениях законодательства, возможных перерывах в работе онлайн-сервиса, в связи с внесением изменений, а также внесение соответствующих изменений в анкеты и шаблоны документов онлайн-сервиса;

- выгрузка документов в форматах \*.doc и \*.pdf;

- выгрузка всего пакета документов в едином файле-архиве.

Исполнителем производится аудит информационных систем персональных данных, вносится необходимая информация в программное обеспечение для автоматизации формирования и актуализации внутренней документации. Исполнитель выгружает пакет организационно-распорядительной документации по защите информации (далее – ОРД) из программного обеспечения для автоматизации формирования и актуализации внутренней документации. В случае необходимости Исполнителем вносятся правки в ОРД с учётом технологии обработки персональных данных Заказчиком. ОРД согласовываются и утверждаются Заказчиком.

Вся организационно-распорядительная документация должна соответствовать единой технологии обработки информации. Организационно-распорядительная документация должна создавать условия для обеспечения защиты информации от угроз несанкционированного доступа, инсайдерских угроз, угроз хищения носителей информации. ОРД должны предусматривать выполнение требований к составу и содержанию организационных мер защиты информационных систем персональных данных.

4.3.6. Оценка соответствия (аттестация) системы защиты информации требованиям безопасности информации

Аттестация информационной системы организуется Заказчиком и включает проведение комплекса организационных и технических мероприятий (аттестационных испытаний), в результате которых подтверждается соответствие системы защиты информации требованиям по защите информации.

Исполнителем разрабатывается программа и методика аттестационных испытаний для ИСПДн (далее – Программа-методика). Программа-методика определяет цели, задачи, методы, условия, объем, порядок и методику проведения оценки соответствия принимаемых мер по обеспечению безопасности информации в ИСПДн на соответствие требованиям законодательства по безопасности информации. Программа-методика согласовывается с Заказчиком.

В соответствии с Программой-методикой Исполнителем выполняется оценка соответствия принимаемых мер по обеспечению безопасности информации требованиям безопасности информации для ИСПДн. По результатам аттестационных испытаний оформляются протоколы аттестационных испытаний, заключение о соответствии информационной системы требованиям по защите информации и аттестат соответствия в случае положительных результатов аттестационных испытаний.

По результатам выполнения работ Исполнителем готовятся и передаются Заказчику следующие документы:

- программа и методика проведения аттестационных испытаний по требованиям безопасности информации ИСПДн;

- протокол аттестационных испытаний ИСПДн на соответствие требованиям безопасности информации;

- заключение по результатам аттестационных испытаний ИСПДн на соответствие требованиям безопасности информации;

- аттестат соответствия требованиям по безопасности информации ИСПДн (при положительном заключении по результатам аттестационных испытаний).

**5. Дополнительные требования.**

5.1. Требования к Исполнителю.

В соответствии с Федеральным законом от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности», постановлением Правительства Российской Федерации от 03.02.2012 № 79 «О лицензировании деятельности по технической защите конфиденциальной информации» для выполнения работ по защите информации, Исполнителю требуется лицензия или выписка из реестра лицензий ФСТЭК России на деятельность по технической защите конфиденциальной информации на следующие работы и услуги:

1) работы и услуги по аттестационным испытаниям и аттестации на соответствие требованиям по защите информации: средств и систем информатизации;

2) работы и услуги по проектированию в защищённом исполнении: средств и систем автоматизации;

3) услуги по установке, монтажу, наладке, испытаниям, ремонту средств защиты информации: программных (программно-технических) средств защиты информации.

5.2. Требования к надёжности.

Средства защиты, используемые при построении СЗИ, должны обеспечивать необходимый уровень защиты информации, не снижая при этом надёжности технологий обработки информации (в т.ч. времени выполнения технологических операций) и не оказывая существенного влияния на производительность средств вычислительной техники, входящих в состав ИСПДн.

При отказе одной или нескольких компонент СЗИ должна сохранять возможность функционирования.

5.3. Требования к безопасности.

Все оборудование, входящее в состав СЗИ, должно соответствовать действующим отечественным и международным стандартам в области безопасности.

При эксплуатации, обслуживании и ремонте технических средств СЗИ необходимо соблюдать правила техники безопасности для работ (услуг), связанных с эксплуатацией электрооборудования (до 1000 В).

В ходе оказания услуг Исполнитель обязан обеспечить сохранение целостности и доступности конфиденциальной информации, в том числе персональных данных, доступ к которым получен в ходе оказания услуг.

Оказание услуг осуществляется только при личном прибытии представителей Исполнителя на объекты информатизации Заказчика и осуществляется под непосредственным контролем назначенных должностных лиц, ответственных за обеспечение безопасности информации. Использование технологий удалённого доступа не допускается.

5.4. Требования к эксплуатации, техническому обслуживанию, ремонту и хранению компонентов СЗ ИСПДн.

К эксплуатации, техническому обслуживанию, ремонту и хранению компонентов СЗИ предъявляются следующие требования:

- СЗИ эксплуатируется круглосуточно за исключением времени технического обслуживания;

- обработка информации обеспечивается в реальном режиме времени;

- питание электроэнергией технических средств защиты информации осуществляется от однофазной сети переменного тока напряжением 220 В и частотой 50 Гц;

- для всех технических и программных средств должна быть предусмотрена техническая поддержка с возможностью её продления.

5.5. Требования к стандартизации и унификации.

Услуга должна проводиться с соблюдением действующих государственных стандартов в соответствии с областью их распространения.

Решения по использованию технических средств и ПО в СЗ ИС должны обеспечивать использование однотипных компонентов в целях снижения расходов на обслуживание и ремонт, взаимозаменяемости используемых компонентов и удобства эксплуатации.

Услуга должна обеспечивать совместимость технических средств и ПО СЗ ИС с техническими средствами и программным обеспечением, используемыми в ИСПДн Заказчика.

5.6. Требования по обеспечению конфиденциальности.

В период оказания услуги и после её окончания Исполнитель обязан не разглашать и не использовать конфиденциальную информацию, принадлежащую Заказчику, которая может стать ему известной в ходе оказания услуги. Исполнитель несёт ответственность за соблюдение этого требования в соответствии с законодательством Российской Федерации.

Согласовано:

Начальник отдела

информационных технологий: П.Н. Ефремов

Контрактная служба: О.В. Дергилев