**ТЕХНИЧЕСКОЕ ЗАДАНИЕ**

**Выполнение технологических работ по обеспечению информационной безопасности в рамках обработки персональных данных в информационных системах Муниципального учреждения «Многофункциональный центр предоставления государственных и муниципальных услуг Мытищинского муниципального района»**

**(МУ «МФЦ ММР»)**

**1. Наименование**

Предметом конкурса является выполнение технологических работ по обеспечению информационной безопасности в рамках обработки персональных данных в информационных системах Муниципального учреждения «Многофункциональный центр предоставления государственных и муниципальных услуг Мытищинского муниципальногорайона» (МУ «МФЦ ММР»). Технологические работы включают в себя поставку необходимых технических средств, программного обеспечения и оказание необходимых услуг.

**2. Место, срок и условия оказания выполнения работ.**

Технологические работы по обеспечению информационной безопасности в рамках обработки персональных данных в информационных системах Заказчика выполняются Исполнителем по адресам:

* г. Мытищи, ул. К. Маркса, д. 4;
* г. Мытищи, ул. Лётная, д. 20/3;

Период оказания услуг: 30 рабочих дней с даты заключения Государственного контракта. Все работы должны быть завершены в срок до 01 декабря 2013г.

3. Термины и определения:

|  |  |
| --- | --- |
| ИС | Информационная система, включающая в свой состав техническое, программное, информационное обеспечение, объединенные в информационные сервисы, автоматизированные системы, аппаратно-программные комплексы и прикладные программные комплексы и средства |
| Пользователь | Лицо, участвующее в функционировании ИС или использующее результаты ее функционирования |
| ПО | Программное обеспечение ИС (совокупность программ на носителях данных и программных документов, предназначенных для отладки, функционирования и проверки работоспособности ИС) |
| ИО | Информационное обеспечение ИС (совокупность форм документов, классификаторов, нормативной базы и реализованных решений по объемам, размещению и формам существования информации, применяемой в ИС при ее функционировании) |
| АРМ | Автоматизированное рабочее место пользователя ИС |
| БД | База данных |
| СУБД | Система управления БД |
| ЛВС | Локальная вычислительная сеть ИС |
| ИБ | Информационная безопасность |
| НСД | Несанкционированный доступ |
| ПДн | Персональные данные |
| МФЦ | Многофункциональный Центр |
| ИСПДн | Информационная система (подсистема, аппаратно-программный комплекс, программно-технический комплекс, комплекс программных средств), обрабатывающая персональные данные |
| СЗПДн | Система защиты Персональных данных |
| МЭ | Межсетевой экран |

**4. Основание для выполнения работ**

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

- Специальные требования и рекомендации по технической защите конфиденциальной информации, утвержденные приказом Гостехкомиссии от 30.08.2002 г. № 282.

**5. Требования к выполнению технологических работ**

# **Общие требования**

Разработанные документы и проекты организационно-распорядительных документов должны соответствовать требованиям действующего законодательства Российской Федерации, в том числе:

* Федеральный Закон РФ №63-ФЗ от 6 апреля 2011 г. «Об электронной подписи».
* Конвенция Совета Европы «О защите физических лиц при автоматизированной обработке персональных данных». Страсбург, 28 января 1981 г.
* Конституция Российской Федерации, 12 декабря 1993 г.
* Федеральный закон Российской Федерации от 19 декабря 2005 г. №160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных».
* Федеральный закон от 27 июля 2006 г. №152-ФЗ «О персональных данных».
* Федеральный закон Российской Федерации от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации».
* Федеральный закон Российской Федерации от 08 августа 2001 №128-ФЗ «О лицензировании отдельных видов деятельности».
* Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации. Утверждено Постановлением Правительства Российской Федерации от 15 сентября 2008 г №687.
* Указ Президента Российской Федерации от 6 марта 1997 г. №188 «Перечень сведений конфиденциального характера».
* Состава и содержания организационных итехнических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденное Приказом ФСТЭК России от 18 февраля 2013 г. № 21
* Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена заместителем директора ФСТЭК России 15 февраля 2008 г.

# **Порядок оформления и предъявления Заказчику результатов работ**

* По завершении работ по каждому этапу, Исполнитель предоставляет Заказчику необходимую отчетную документацию.
* Сдача работ осуществляется путем предоставления результата работ в электронной форме на оптическом носителе информации (CD-диск), а так же предоставления в бумажной форме комплекта технической и организационно-распорядительной документации на листах формата А4.
* Вся документация должна быть выполнена на русском языке.

# **Перечень заявляемых информационных систем персональных данных**

Объекты информатизации представляют собой локальные вычислительные системы, состоящие из автоматизированных рабочих мест с сетевым и периферийным оборудованием, подключенные к другим локальным вычислительным сетям, имеющие подключение к телекоммуникационным сетям общего пользования и размещенные в выделенных помещениях по адресам:

* г. Мытищи, ул. К. Маркса, д. 4;
* г. Мытищи, ул. Лётная, д. 20/3;

Объекты информатизации предназначены для решения универсальных задач хранения, обработки и передачи информации в локальную вычислительную сеть (далее- ЛВС).

ЛВС имеет структурированную схему. В сети используется стек протоколов TCP/IP. Обработка персональных данных осуществляется на **37 АРМ**.

Территориально АРМ размещены по адресам:

* г. Мытищи, ул. К. Маркса, д. 4 – 18 АРМ;
* г. Мытищи, ул. Лётная, д. 20/3 – 19 АРМ;

# **Требования к разрабатываемой системе**

При проектировании СЗПДн должны быть предусмотрены:

* изменение численности рабочих мест обработки персональных данных;
* совместимости с применяемым специальным программным обеспечением;
* должна иметь развитые средства администрирования;
* возможности последующей модернизации СЗПДн при минимальных временных и финансовых затратах по направлениям изменения системной платформы (операционная система) и изменение специального программного обеспечения;
* для исключения избыточности технологических процедур для реализации однотипного функционала должны быть предложены одинаковые средства защиты информации и унифицированные программные средства;
* предлагаемое решение должно быть масштабируемым и обеспечивать выполнение заявленных требований;

СЗПДн должна обеспечивать противодействие угрозам безопасности персональных данных.

Безопасность информации в системе должна обеспечиваться на всех технологических этапах обработки информации и во всех режимах функционирования технических средств наименование системы.

В состав СЗПДн должны входить:

* подсистема защиты от несанкционированного доступа (НСД);
* подсистема антивирусной защиты;
* подсистема межсетевого экранирования;
* подсистема обнаружения вторжений;
* подсистема анализа защищенности;
* подсистема криптографической защиты информации.

### Требования к функциям безопасности подсистемы защиты от НСД

* СЗИ от НСД должна представлять собой программный комплекс средств защиты информации в ОС семейства Windows с возможностью подключения аппаратных идентификаторов.
* СЗИ от НСД должна быть предназначена для ПЭВМ типа IBM PC, под управлением операционных систем Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows 8, Windows Server 2012 в многопользовательском режиме их эксплуатации.
* СЗИ от НСД должна поддерживать 32-х и 64-х битные версии операционных систем.
* Система должна быть предназначена для использования на персональных компьютерах, портативных компьютерах (ноутбуках), серверах (в том числе контроллерах домена и терминального доступа), также поддерживать виртуальные среды и технологию Windows To Go.
* СЗИ от НСД должна быть сертифицирована по требованиям Руководящих документов (РД) ФСТЭК России (Гостехкомиссии России) по 5-му классу защиты от НСД для СВТ и 4 уровню контроля отсутствия НДВ, разрабатываться и производиться на основании лицензии органов, имеющих федеральные полномочия в указанной сфере.
* Сертификат соответствия должен позволять использовать СЗИ от НСД при создании защищенных автоматизированных систем до класса защищенности 1Г включительно и ИСПДн до уровня 1 включительно.
* СЗИ от НСД должна обеспечивать:
* Регистрацию различных пользователей: локальных, доменных, сетевых. Определение количества одновременных сеансов для пользователя.
* Идентификацию и проверку подлинности пользователей при входе в операционную систему, а также аутентификация при входе на ПЭВМ до начала загрузки ОС. Возможность двухфакторной идентификации по паролю и аппаратному идентификатору. Возможность записи авторизационных данных в идентификатор.
* Реализацию настроек сложности паролей и механизм генерации пароля, соответствующего настройкам.
* Должен быть реализован независимый от механизмов ОС механизм разграничения прав доступа к объектам файловой системы, к запуску программ и к печати документов. Разграничения должны касаться доступа к объектам файловой системы (FAT и NTFS), доступа к сети, доступа к сменным накопителям. Разграничения должны касаться всех пользователей – локальных, сетевых, доменных, терминальных.
* Для предотвращения утечки информации с использованием сменных накопителей СЗИ от НСД должна позволять разграничивать доступ, как к отдельным типам накопителей, так и к конкретным экземплярам.
* В соответствии с требованиями к СЗИ от НСД должен использоваться дискреционный принцип контроля доступа, который обеспечивает доступ к защищаемым объектам (дискам, каталогам, файлам) в соответствии со списками пользователей (групп) и их правами доступа (матрица доступа).
* Возможность ограничивать средствами СЗИ от НСД, круг доступных сетевых ресурсов (с точностью до отдельных удалённых рабочих станция и отдельных папок общего доступа).
* Регистрация и учет (аудит) действий пользователей, независимыми от ОС средствами (вход/выход пользователей, доступ к ресурсам, печать документов с возможностью добавления штампов и сохранение теневых копий распечатываемых документов, запуск\остановка процессов, администрирование). Должны вестись непрерывные журналы (т.е. новые записи не должны затирать более старые) с возможностью сортировки и архивации записей.
* Возможность организации замкнутой программной среды (ЗПС) и различные способы её организации.
* Возможность локального и удалённого администрирования (управление пользователями, политиками безопасности, правами доступа, аудитом, просмотр журналов).
* Возможность контроля целостности программно-аппаратной среды при загрузке ПЭВМ, по команде администратора и по расписанию. А также контроль целостности файлов при доступе и блокировка входа в ОС при выявлении изменений.
* Очистку остаточной информации (освобождаемого дискового пространства, зачистку определённых файлов и папок по команде пользователя), а также возможность полной зачистки дисков и разделов. Запрет смены пользователей без перезагрузки.
* Возможность самодиагностики основного функционала СЗИ от НСД с формированием отчета.
* Возможность сохранения теневых копий распечатываемых документов.
* Возможность сохранения конфигурации для последующего восстановления СЗИ от НСД.
* Ведение двух копий программных средств защиты информации и возможность возврата к настройкам по умолчанию.
* 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.
* Блокировка доступа к файлам по расширению.
* Возможность настройки всех параметров СЗИ от НСД из единой консоли администрирования.
* Возможность создания отчета по назначенным правам и формирование паспорта программного обеспечения, установленного на ПЭВМ.
* 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.
* Возможность построения иерархии управления при помощи специального модуля - менеджера, управляющего несколькими модулями централизованного управления.
* Возможность использования механизма удаленной установки СЗИ от НСД средствами модуля централизованного управления самой СЗИ или средствами групповых политик Active Directory.
* Реализация СЗИ от НСД должна быть полностью программной, но с возможностью подключения аппаратных средств считывания индивидуальных идентификаторов пользователей, включая идентификаторы USB-flash-накопители, Touch Memory (iButton), eToken Pro/Java (в том числе смарт-карты eToken), Rutoken, Rutoken ЭЦП.
  1. **Технические требования к носителю ключевой информации**
* Носитель ключевой информации представляет собой защищенное устройство, предназначенное для строгой аутентификации, безопасного хранения секретных данных, выполнения криптографических вычислений и работы с асимметричными ключами и цифровыми сертификатами.
* Программное обеспечение носителя ключевой информации должно обеспечивать возможность контроля длины и качества задаваемого пользователем PIN-кода и запрета использования "слабых" комбинаций с позиций качества используемых символов PIN- кода (нулевых, повторяющихся, циклических с короткими циклами и т.п.) и реализована возможность изменения параметров безопасности PIN-кода (длина, используемые символы и т.п.)
* Программное обеспечение носителя ключевой информации должно обеспечивать возможность разблокирования ключевых носителей, заблокированных при исчерпании количества попыток неправильного ввода PIN-кода и возможность приведения исправных, возможно заблокированных, ключевых носителей в первоначальное обезличенное состояние. Должна обеспечиваться возможность проведения этой операции удаленно самим пользователем с помощью системы управления ключевыми носителями.

**Требования к аппаратной платформе**

* Носитель ключевой информации должен соответствовать следующим требованиям к аппаратной платформе:
* Объем защищенной памяти не менее 72 КБ
* Форм факторы носителя ключевой информации:
* USB-ключа;
* смарт-карты.

**Технические требования к носителю ключевой информации**

Корпус: Твердый пластик, не допускающий необнаружимого вскрытия

Рабочая температура: 0°C – 70°C

Температура хранения: -40°C – 85°C

Влажностный режим: 0-100% без конденсата

Водонепроницаемость: Соответствие стандарту IP X8 – IEC 529

Срок хранения данных в памяти: Не менее 10 лет

Среднее время наработки на отказ электронных компонентов не менее 10 лет.

Количество циклов перезаписи памяти: Не менее 500,000

**Требования к поддерживаемым интерфейсам и стандартам**

PKCS#11 – стандарт криптографической работы с электронными ключами): v2.01;

Спецификация ISO (Международная организация по стандартизации): ISO 7816-3,

7816-4;

CAPI – интерфейс программирования приложений, поддерживающий работу с

ассиметричными и симметричными ключами;

PC/CS – набор спецификаций для доступа к смарткартам (команды APDU –

команды для работы со смарт-картами);

хранение сертификатов X.509 v3;

SSL v3 - криптографический протокол, обеспечивающий установление безопасного

соединения между клиентом и сервером;

IPSec/IKE - набор протоколов для обеспечения защиты данных, передаваемых по

межсетевому протоколу IP, осуществляющий подтверждение подлинности и/или

шифрование IP-пакетов;

Microsoft CCID – стандарт электронных ключей eToken PRO (Java);

Microsoft Smartcard Minidriver – драйвер для устройства чтения смарткарт.

**Требования к аппаратно реализованным криптографическим алгоритмам:**

Криптографический алгоритм с открытым ключом - RSA 1024/2048,

Симметричный алгоритм шифрования - DES,

Симметричный блочный шифр - Triple DES,

Алгоритм криптографического хеширования - SHA1

**Требования к поддерживаемым платформам**

Microsoft Windows 2000/2003/XP/Vista/2008/2008 R2/7 (32 и 64-битные версии);

Linux;

Mac OS;

**Требования к сертификации ключевого носителя**

Носитель ключевой информации должен иметь следующий сертификат:

Носитель ключевой информации должен иметь сертификат соответствия ФСТЭК России – как программно-аппаратное средство аутентификации и хранения ключевой информации пользователей в автоматизированных системах, обрабатывающих конфиденциальную информацию.

### Требования к подсистеме антивирусной защиты

Средства антивирусной защиты, должны быть сертифицированы уполномоченным органом (ФСТЭК) на соответствие требованиям руководящего документа Гостехкомиссии России «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» по уровню контроля не ниже 4 и требованиям технических условий.

В рамках всей организации должны использоваться единые антивирусные средства независимо от степени конфиденциальности обрабатываемой информации. Отдельно стоящие ПК, то есть не подключённые к единой системе антивирусной защиты, в том числе находящиеся на удаленных территориях, должны быть защищены интегрированным программным продуктом, включающим в себя защиту от всех типов вредоносных программ (антивирус), спама (персональный антиспам) и сетевых атак (персональный межсетевой экран), и обеспечивать возможность их включения в единую систему антивирусной защиты.

Программный интерфейс всех антивирусных средств, включая средства управления должен быть на русском языке.

Все антивирусные средства, включая средства управления, должны обладать контекстной справочной системой на русском языке.

Антивирусные средства должны включать:

• программные средства антивирусной защиты рабочих станций и серверов;

• программные средства антивирусной защиты почтовых и интернет шлюзов;

• программные средства защиты пользователей от нежелательных массовых почтовых рассылок – спама;

• программные средства централизованного управления, мониторинга и обновления;

• обновляемые базы данных сигнатур вредоносных программ и атак;

• эксплуатационную документацию на русском языке.

**Требования к программным средствам антивирусной защиты рабочих станций под управлением ОС семейства Microsoft Windows**

Программные средства антивирусной защиты систем рабочих станций под управлением семейства ОС Microsoft Windows должны функционировать на следующих версиях ОС:

• Microsoft Windows 2000 Professional (Service Pack 4 и выше);

• Microsoft Windows XP Home Edition;

• Microsoft Windows XP Professional (Service Pack 1 и выше);

• Microsoft Windows XP Professional x64 Edition;

• Microsoft Windows Vista;

• Microsoft Windows Vista x64;

• Microsoft Windows 7;

• Microsoft Windows 7 x64.

Программные средства антивирусной защиты систем рабочих станций под управлением семейства ОС Microsoft Windows должны обеспечивать реализацию следующих функциональных возможностей:

• резидентный антивирусный мониторинг;

• программные средства защиты от сетевых атак;

• эвристический анализатор, позволяющий более эффективно распознавать и блокировать ранее неизвестные вредоносные программы;

• обнаружение скрытых процессов;

• антивирусное сканирование по команде пользователя или администратора и по расписанию;

• антивирусную проверку и лечение файлов, упакованных программами типа PKLITE, LZEXE, DIET, EXEPACK и пр.;

• антивирусную проверку и лечение файлов в архивах форматов RAR, ARJ, ZIP, CAB, LHA, JAR, ICE, в том числе и защищенных паролем;

• защиту электронной корреспонденции, как от вредоносных программ, так и от спама. Проверку трафика на следующих протоколах:

-IMAP, SMTP, POP3, независимо от используемого почтового клиента;

-NNTP (только проверка на вирусы), независимо от почтового клиента;

-Независимо от типа протокола (в том числе MAPI, HTTP) в рамках работы плагинов, встроенных в почтовые программы Microsoft Office Outlook и The Bat!;

• Защиту HTTP-трафика - проверку всех объектов, поступающих на компьютер пользователя по протоколу HTTP, FTP;

• Проверку скриптов - проверку всех скриптов, обрабатываемых в Microsoft Internet Explorer, а также любых WSH-скриптов (JavaScript, Visual Basic Script и др.), запускаемых при работе пользователя на компьютере, в том числе и в интернете;

• проверка трафика ICQ и MSN, для обеспечения безопасности работы с интернет-пейджерами;

• запуск задач по расписанию и/или сразу после загрузки операционной системы;

• защиту от еще не известных вредоносных программ на основе анализа их поведения и контроле изменений системного реестра, с возможностью автоматического восстановления изменённых вредоносной программой значений системного реестра;

• защиту от хакерских атак, путем использования межсетевого экрана с системой обнаружения и предотвращения вторжений (IDS/IPS) и правилами сетевой активности для наиболее популярных приложений при работе в вычислительных сетях любого типа, включая беспроводные;

• защиту от программ-маскировщиков, программ автодозвона на платные сайты, блокировку баннеров, всплывающих окон, вредоносных сценариев, загружаемых с Web-страниц и распознавание фишинг-сайтов;

• осуществлять контроль работы пользователя с внешними устройствами ввода / вывода, позволяя ограничивать доступ к внешним USB-носителям, мультимедийным устройствам и другим устройствам хранения данных.

• ускорения процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось;

• гибкого управления использованием ресурсов ПК для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства;

• настройки проверки критических областей компьютера в качестве отдельной задачи;

• технологии самозащиты приложения, защиты от удаленного несанкционированного управления сервисом приложения, а также защиты доступа к параметрам приложения с помощью пароля, позволяющих избежать отключения защиты со стороны вредоносных программ, злоумышленников или неквалифицированных пользователей.

**Требования к программным средствам антивирусной защиты серверов под управлением ОС семейства Microsoft Windows**

Программные средства антивирусной защиты систем серверов под управлением семейства ОС Microsoft Windows должны функционировать на следующих версиях ОС:

• Microsoft Windows 2000 Server/Advanced Server (Service Pack 4 и выше, все текущие обновления);

• Microsoft Windows Server 2003 Standard/Enterprise Edition, Microsoft Windows Server 2003 Web Edition, Microsoft Windows Storage Server 2003, Microsoft Small Business Server 2003 все Service Packs, все текущие обновления;

• Microsoft Windows Server 2003 R2 Standard x64 Edition, Microsoft Windows Server 2003 R2 Enterprise x64 Edition, Microsoft Windows Server 2003 R2 Standard Edition, Microsoft Windows Server 2003 R2 Enterprise Edition;

• Microsoft Windows Server 2008;

• Microsoft Windows Server 2008 R2.

Программные средства антивирусной защиты файловых систем серверов под управлением семейства ОС Microsoft Windows должны обеспечивать реализацию следующих функциональных возможностей:

• резидентный антивирусный мониторинг;

• эвристический анализатор, позволяющий более эффективно распознавать и блокировать ранее неизвестные вредоносные программы;

• обнаружение скрытых процессов;

• антивирусное сканирование по команде пользователя или администратора и по расписанию;

• антивирусную проверку и лечение файлов, упакованных программами типа PKLITE, LZEXE, DIET, EXEPACK и пр.;

• антивирусную проверку и лечение файлов в архивах форматов RAR, ARJ, ZIP, CAB, LHA, JAR, ICE, в том числе и защищенных паролем;

• запуск задач по расписанию и/или сразу после загрузки операционной системы;

• защиту от еще не известных вредоносных программ, принадлежащих зарегистрированным семействам, на основе эвристического анализа;

• ускорения процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось;

• настройки проверки критических областей сервера в качестве отдельной задачи;

• регулировки распределения ресурсов сервера между антивирусом и другими приложениями в зависимости от приоритетности задач: возможность продолжать антивирусное сканирование в фоновом режиме;

• наличием множественных путей уведомления администраторов о важных произошедших событиях (почтовое сообщение, звуковое оповещение, всплывающее окно, запись в журнал событий);

• технологии самозащиты приложения, защиты от удаленного несанкционированного управления сервисом приложения, защита файлов приложения от несанкционированного доступа и изменения, а также защиты доступа к параметрам приложения с помощью пароля, позволяющими избежать отключения защиты со стороны вредоносных программ, злоумышленников или неквалифицированных пользователей.

**Требования к системе управления антивирусной защитой**

Программные средства управления для всех защищаемых ресурсов, реализованных на платформах ОС Microsoft Windows, Novell Netware, для файловых серверов и рабочих станций Linux и мобильных устройств на платформе Microsoft Windows Mobile и Symbian должны обеспечивать реализацию следующих функциональных возможностей:

• установка системы антивирусной защиты из единого дистрибутива;

• выбор установки в зависимости от количества защищаемых узлов;

• создание групп логической сети на основе структуры Active Directory;

• централизованную установку/обновление/удаление программных средств антивирусной защиты, настройку, администрирование, просмотр отчетов и статистической информации по их работе;

• удаленная установка программных средств антивирусной защиты с последней версией баз приложения

• автоматизированное обновление программных средств антивирусной защиты и антивирусных баз (для защищаемых ресурсов на базе ОС Microsoft Windows, Novell Netware, для файловых серверов и рабочих станций Linux);

• доставку обновлений на рабочие места пользователей сразу после их получения;

• построение многоуровневой системы управления с возможностью настройки ролей администраторов и операторов, а также форм предоставляемой отчетности на каждом уровне;

• обновление программных средств и антивирусных баз из разных источников, как по каналам связи, так и на машинных носителях информации;

• централизованный сбор информации и создание отчетов о состоянии антивирусной защиты;

• наличие механизма оповещения о событиях в работе установленных приложений антивирусной защиты и настройку рассылки почтовых уведомлений о них;

• централизованный сбор информации о всех установленных на клиентских компьютерах приложениях;

• экспорта отчетов в файлы форматов PDF и XML;

• централизованное управление объектами резервных хранилищ и карантинов по всем ресурсам сети, на которых установлено антивирусное программное обеспечение;

• наличие системы контроля возникновения вирусных эпидемий.

Требования к обновлению антивирусных баз

Обновляемые антивирусные базы данных должны обеспечивать реализацию следующих функциональных возможностей:

• регламентное обновление антивирусных баз не реже 24 раз в течение календарных суток, а баз антиспама не реже одного раза в 5 минут;

• множественность путей обновления, в том числе – по каналам связи и на отчуждаемых электронных носителях информации;

• проверку целостности и подлинности обновлений средствами электронной цифровой подписи.

Требования к эксплуатационной документации

Эксплуатационная документация для всех программных продуктов антивирусной защиты, включая средства управления, должна включать документы, подготовленные в соответствии с требованиями государственных стандартов, на русском языке, в том числе:

• руководство пользователя (администратора).

Документация, поставляемая с антивирусными средствами, должна детально описывать процесс установки, настройки и эксплуатации соответствующего средства антивирусной защиты.

Требования к технической поддержке

Техническая поддержка антивирусного программного обеспечения должна:

• Предоставляться на русском языке сертифицированными специалистами производителя средств антивирусной защиты и его партнеров на всей территории Российской Федерации круглосуточно без праздников и выходных по телефону, электронной почте и через Интернет;

• Web-сайт производителя АПО должен быть на русском языке, иметь специальный раздел, посвящённый технической поддержке АПО, пополняемую базу знаний, а также форум пользователей программных продуктов.

### Требования к функциям безопасности подсистемы межсетевого экранирования

Все средства защиты информации, планируемые к установке, должны быть сертифицированы как средства защиты информации, что подтверждается сертификатом ФСТЭК/ФСБ

**Требования к программному обеспечению, реализующему функции управления защищённой сетью:**

Программного обеспечения, реализующего функции управления защищённой сетью должно отвечать следующим требованиям:

* состоять из центра управления сетью и ключевого удостоверяющего центра;
* совместимо (полностью) с программным обеспечением, реализующим функции криптографического шлюза и клиента;
* выработка ключей, соответствующих ГОСТ 28147-89, ГОСТ Р 34.11-94, ГОСТ Р34.10-2001;
* создание узлов защищенной сети (криптографические шлюзы и клиенты), удаление узлов защищенной сети, определение политик связей защищённых узлов между собой, определение политики безопасности и формирование списков прикладных задач для узлов защищенной сети;
* автоматическая рассылка справочной и ключевой информации;
* проведение автоматического обновления программного обеспечения криптошлюзов и криптографических клиентов;
* формирование симметричных ключей связи узлов (криптошлюзы и криптографические клиенты) между собой;
* формирование сертификатов электронно-цифровой подписи формата X.509 v.3;
* ведение списков отозванных сертификатов электронно-цифровой подписи;
* наличие модуля гарантированной доставки обновления справочной-ключевой информации на криптошлюзы и криптографические клиенты;
* поддержка операционных систем:

Windows 2000 Professional;

Windows XP Home/Professional;

Windows 2000 Server;

Windows 2003 Server.

**Требования к Криптографическому шлюзу:**

Программного обеспечения, реализующего функции криптографического шлюза должно отвечать следующим требованиям:

* совместимо (полностью) с программным обеспечением, реализующим функции управления защищённой сетью, представленным в настоящем запросе котировок (ПО Тип 1): обновление программного обеспечения, обновление справочно-ключевой информацией, управлением политиками безопасности;
* совместимо (полностью) с программным комплексом, реализующим функции криптографического клиента, представленным в настоящем запросе котировок (ПО Тип 1):
* шифрование/дешифрование направляемого/принимаемого IP-трафика;
* поддержка операционных систем:
* Microsoft Windows 2000 Professional;
* Microsoft Windows XP Home/Professional;
* Microsoft Windows Vista (вся линейка);
* Microsoft Windows 7 (вся линейка).
* наличие в составе программного обеспечения, соответствующего требованиям ФСТЭК России к межсетевым экранам по 3 классу, отсутствию недекларируемых возможностей по 3 уровню, иметь ОУД не ниже 4+ и возможностью использования в АС до класса 1В включительно;
* наличие сертификата ФСБ России по классу КС2 (КС3);
* осуществление функции прокси-сервера защищенных соединений;
* встроенный межсетевой экран, соответствующий 3-ому классу по требованиям ФСТЭК России;
* предоставление функции туннелирующего сервера;
* предоставление функции сервера IP-адресов;
* криптошлюз должен использовать IP-адресацию для организации зачищенных каналов связи с другими криптошлюзами и криптографическими клиентами, основанную на шестнадцатеричных индентификаторах;

- программное обеспечение, реализующее функции криптографического шлюза, должно шифровать каждый IP-пакет на уникальном ключе, основанном на паре симметричных ключей связи с другими криптографическими шлюзами и клиентами, выработанных в программном обеспечении, реализующем функции управления защищённой сетью

**Требования к криптографическому клиенту:**

Программного обеспечения, реализующего функции криптографического клиента должно отвечать следующим требованиям:

* совместимо (полностью) с программным обеспечением, реализующим функции управления защищённой сетью, представленным в настоящем запросе котировок (Тип 1): обновление программного обеспечения, обновление справочно-ключевой информации, управлением политиками безопасности;
* совместимо (полностью) с программным комплексом, реализующим функции криптографического шлюза, представленным в настоящем запросе котировок: шифрование/дешифрование направляемого/принимаемого IP-трафика;
* поддержка операционных систем:
* Microsoft Windows 2000 Professional;
* Microsoft Windows XP Home/Professional;
* Microsoft Windows Vista (вся линейка);
* Microsoft Windows 7 (вся линейка).
* наличие в составе программного обеспечения, соответствующего требованиям ФСТЭК России к межсетевым экранам по 3 классу, отсутствию недекларируемых возможностей по 3 уровню, иметь ОУД не ниже 4+ и возможностью использования в АС до класса 1В включительно;
* наличие сертификата ФСБ России по классу КС2 (КС3);
* иметь встроенный персональный экран, соответствующий 3-му классу по требованиям ФСТЭК России;
* предоставлять функции клиента службы обмена файлами и сообщениями, защищенной электронной почты с функциями шифрования писем и вложений для обмена с другими криптографическими клиентами;
* предоставлять функции контроля запускаемых в операционной системе приложений;
* предоставлять функции контентной фильтрации прикладных протоколов http, ftp;
* программное обеспечение, реализующее функции криптографического клиента, должно шифровать каждый IP-пакет на уникальном ключе, основанном на паре симметричных ключей связи с другими криптографическими шлюзами и клиентами, выработанных в программном обеспечении, реализующем функции управления защищённой сетью;

взаимодействие с другими криптографическими клиентами с использованием технологии «клиент-клиент» (без использования криптографического шлюза»).

**Требования к функциям безопасности подсистемы криптографической защиты:**

- Все средства криптозащиты должны иметь возможность использовать единый или распределенный Сертификационный (удостоверяющий) центр на базе открытого распределения криптографических ключей.

- Все документальные данные и файлы, передаваемые по сети передачи данных, должны удостоверяться электронной цифровой подписью (ЭЦП), подтверждаемой Центром сертификации и регистрации (ЦСР).

- Должны иметь сертификаты ФСБ на соответствие требованиям к безопасности информации по уровню КС1 и КС2.

- Услуги должны быть выполнены в соответствии с приложением к приказу ФСБ России от 09.02.2005 г. №66 Положение «ПКЗ-2005».

**Требования к службе обработки сообщений:**

Оказание услуг по обмену электронными сообщениями осуществляется в соответствии с п.3.2 руководящего документа отрасли «Телематические службы» утвержденным Приказом Министерства Российской Федерации по связи и информатизации от 23.07.2001 г. № 175.

**Требование по передаче информации:**

- Все данные должны передаваться с использованием системы распределения ключевой информации, построенной на базе открытого распределения криптографических ключей удостоверяющего (сертификационного) центра.

- Достоверность и целостность отдельных единиц хранимой информации должны обеспечиваться использованием электронной цифровой подписи.

- Для обеспечения конфиденциальности информации не допускается привлечение соисполнителей.

# **Требования к надежности**

Оборудование СЗПДн должно обеспечивать:

* исключение случаев невосполнимого разрушения системы, потери информации при сбоях и отказах электропитания, отказах оборудования и других нештатных ситуациях;
* надежность всех СЗИ.

# **Требования к режимам функционирования**

Для СЗПДн должны быть определены следующие режимы функционирования:

* штатный режим функционирования;
* аварийный режим функционирования.

Основным режимом функционирования СЗПДн является штатный режим.

В штатном режиме функционирования системы:

* клиентское программное обеспечение и технические средства пользователей и администратора системы обеспечивают возможность функционирования в течение пяти рабочих дней с 08:00 до 17:00;
* серверное программное обеспечение и технические средства серверов обеспечивают возможность круглосуточного функционирования, с перерывами на обслуживание;
* исправно работает оборудование, составляющее комплекс технических средств;
* исправно функционирует системное, базовое и прикладное программное обеспечение системы.

Для обеспечения штатного режима функционирования системы необходимо выполнять требования и выдерживать условия эксплуатации программного обеспечения и комплекса технических средств системы, указанные в соответствующих технических документах (техническая документация, инструкции по эксплуатации и т.д.).

Аварийный режим функционирования системы характеризуется отказом одного или нескольких компонент программного и (или) технического обеспечения.

# **Требования к обеспечению безопасности в ходе разработки и внедрения СЗПДн.**

Все сведения о составе и характеристиках СЗПДн являются конфиденциальной информацией.

Разработчик СЗПДн обязуется:

- не проводить противозаконные действия по сбору, использованию и передаче третьей стороне информации циркулирующей и хранящейся в ИС;

- не осуществлять несанкционированный доступ к информационным ресурсам ИС;

- не проводить незаконное копирование информации, циркулирующей или хранящейся в ИС;

- не предпринимать манипулирование информацией, циркулирующей или хранящейся в ИС (фальсифицировать, модифицировать, подделывать, блокировать, уничтожать или искажать информацию);

- не нарушать технологию сбора, накопления, хранения, обработки, преобразования, отображения и передачи информации, в результате чего может быть осуществлено искажение, потеря или незаконное использование информации;

- не внедрять в ИС программы-вирусы (загрузочные, файловые и др.);

- не устанавливать программные и аппаратные закладные устройства в технические средства ИС;

- не устанавливать в технические средства ИС программное обеспечение, зараженное вирусами;

Нарушение настоящих требований влечет за собою гражданско-правовую, административную или уголовную ответственность в соответствии с законом Российской Федерации.

# **Требования к патентной чистоте**

Все средства СЗПДн должны обладать патентной чистотой и иметь возможность легального использования на территории Российской Федерации.

# **Требования к стандартизации и унификации**

Стандартизация должна охватывать все этапы разработки и внедрения СЗПДн.

Выполнение услуг по созданию системы должно осуществляться в соответствии с ГОСТ 34.601-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания».

Внесение изменений в настоящее техническое задание должно осуществляться по согласованию с Заказчиком в соответствии с положениями ГОСТ 34.602-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы».

## **Требования к гарантийному сопровождению**

Разработчиком СЗПДн должен быть обеспечен не менее чем в 12 месяцев с момента приемки системы в эксплуатацию базовый набор услуг по гарантийному сопровождению СЗПДн, включающий:

- устранение ошибок, выявленных в процессе эксплуатации;

- локализацию инцидентов, связанных с неправильными действиями специалистов Заказчика;

- консультирование специалистов Заказчика по вопросам эксплуатации в режиме «вопрос-ответ» (по телефону или посредством электронной почты);

- разработку и предоставление изменений настроек комплекса.

# **Дополнительные положения**

Требования по проведению специальных исследований, специальных проверок оборудования не предъявляются.

Требования по защите информации от утечки по каналам побочных электромагнитных излучений и наводок (ПЭМИН) в ИСПДн не предъявляются.

Требования по взаимосвязям СЗПДн со смежными системами не предъявляются.

# **Состав и содержание работ**

**Требования к порядку оказания услуг**

В соответствии с нормативно-методическими документами РФ Исполнитель обязуется провести аттестационные испытания Информационной системы включающей в себя основные узлы создаваемой «Сети», по требованиям Федеральным законом № 152-ФЗ. Указанные услуги должны включать в себя следующие стадии:

- Предпроектную стадию, включающую предпроектное обследование Информационной узлов создаваемой «Сети» и определение модели угроз.

- Стадию проектирования и реализации проекта защиты сети обработки персональных данных.

- Стадию ввода в действие, включающую опытную эксплуатацию и приемо-сдаточные испытания средств защиты «Сети».

*На предпроектной стадии Исполнителю необходимо провести следующие мероприятия:*

- провести анализ внутренних нормативных документов, регламентирующих порядок обработки и защиты ПДн в системах Заказчика;

- определить перечень ПДн, подлежащих защите;

- определить перечень и состав ИСПДн;

- определить используемые средства защиты ПДн, и оценить их соответствие требованиям нормативных документов Российской Федерации;

- определить степень участия персонала в обработке ПДн и характер взаимодействия персонала между собой;

- разработать технический проект на выполнение услуг по защите ИСПДн Заказчика

- представить Заказчику акт о результатах обследования текущего состояния ИСПДн;

*На стадии проектирования и создания СЗПДн Исполнителю необходимо провести следующие мероприятия:*

- разработать технический проект выполнения услуг по созданию и внедрению СЗПДн в соответствии с требованиями настоящего технического задания;

- выполнить услуги в соответствии с проектной документацией;

- обосновать и установить для использования в ИСПДн сертифицированные технические, программные и программно-технические средства защиты информации;

- разработать и реализовать разрешительную систему доступа пользователей к обрабатываемой на ИСПДн информации;

- совместно с Заказчиком определить лиц, ответственных за эксплуатацию средств защиты информации;

- разработать положение по организации и выполнению услуг по обеспечению безопасности персональных данных при обработке их в ИСПДн.

- разработать эксплуатационную документацию на ИСПДн и средства защиты информации, а также организационно-распорядительную документацию по защите персональных данных (технический паспорт на ИСПДн, необходимые инструкции, требования и другие документы);

- представить Заказчику акт о проведенных мероприятиях по созданию документации СЗПДн;

- выполнить другие мероприятия, характерные для ИСПДн и направлений обеспечения безопасности ПДн.

*На стадии ввода в действие Исполнителю необходимо:*

- передать Заказчику программно\аппаратные средства защиты информации, внедренные на стадии проектирования ИСПДн, по актам приема-передачи.

- совместно с Заказчиком провести опытную эксплуатацию СЗПДн в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе ИСПДн;

- совместно с Заказчиком выполнить приемо-сдаточные испытания СЗПДн по результатам опытной эксплуатации;

- совместно с Заказчиком выполнить мероприятия по организации охраны и физической защиты помещений ИСПДн, находящихся в муниципальных образованиях, исключающей НСД к техническим средствам ИСПДн, их хищение и нарушение работоспособности, хищение носителей информации;

- осуществить инструктаж лиц, использующих средства защиты информации, применяемые в СЗПДн, правилам работы с ними;

- оценить соответствие ИСПДн требованиям безопасности ПДн;

- аттестовать по требованиям безопасности информации ИСПДн;

- совместно с Заказчиком провести приемочные испытания и ввести в эксплуатацию СЗПДн;

- устранить все уязвимости с высоким уровнем опасности и рекомендациями исполнителя, выявленные ранее на этапе проведения предпроектного обследования.

- представить Заказчику акт о проведенных мероприятиях

- предоставить Заказчику пакет организационно-распорядительной документации:

Инструкция администратора безопасности ИС;

Инструкция пользователя ИС;

Инструкция по организации парольной защиты в ИС;

Технический паспорт на ИС

**Требования к проведению предпроектного обследования**

Анализ внутренних нормативных документов, регламентирующих порядок обработки и защиты ПДн.

На этом подэтапе осуществляется: сбор данных о существующей нормативной документации Заказчика, регулирующей порядок обработки и обеспечения защиты ПДн.

В ходе выполнения услуг по данному подэтапу Исполнителем выясняется необходимость подготовки (переработки) им проектов нормативной документации Заказчика в области обработки и защиты ПДн.

**Определение перечня ПДн, подлежащих защите**

На данном подэтапе определяется: перечень обрабатываемых ПДн, необходимость защиты категорий ПДн.

На основе вышеуказанной информации составляется «Перечень ПДн, обрабатываемых в ИСПДн, подлежащих защите».

**Определение перечня и состава ИСПДн**

На этом подэтапе Исполнителем определяется: перечень существующих ИСПДн в составе ИС, структура каждой ИСПДн, включая состав и размещение программно-аппаратных средств ИСПДн, вид и режим обработки ПДн, состав и количество обрабатываемых данных, взаимодействие ИСПДн между собой и другими информационными системами.

В ходе проведения перечисленных услуг также должны быть получены технические данные для дальнейшего проектирования по следующим направлениям:

Информация о сетевых соединениях:

- схема сети, информационные потоки;

- системное сетевое программное обеспечение, в т.ч. наименование, полная версия;

- типы применяемого сетевого оборудования, версии прошивок операционных систем маршрутизаторов, коммутаторов, систем управления сетевым оборудованием на всех уровнях;

- использование встроенных средств защиты информации (наличие криптографических протоколов и специального канального оборудования для шифрования критичного трафика) на всех уровнях.

Информация об используемых сетевых и автономных АРМ Заказчика:

- количество, тип, место установки и назначение;

- аппаратные платформы, аппаратное обеспечение, фирма-производитель, фирма-поставщик, описание;

- операционные системы, в т.ч. наименование, полная версия, полные версии заплат (patch, service pack);

- использование штатных (приобретенных) сертифицированных средств защиты от НСД.

Информация о программном обеспечении АРМ в МФЦ ММР:

- перечень специальных систем (системы управления базами данных, электронный документооборот, системы с привязкой к конкретным серверам и пользовательским рабочим местам);

- перечень прикладных программ сторонних производителей с привязкой к конкретным серверам и пользовательским рабочим местам;

- перечень прикладных программ собственной разработки с привязкой к конкретным серверам и пользовательским рабочим местам;

- сертификаты и документация производителя;

- специальные возможности прикладного программного обеспечения;

- наличие критичных для организации процессов электронной обработки и передачи данных.

**Определение степени участия персонала Заказчика в обработке ПДн и характера взаимодействия персонала между собой**

Определение степени участия персонала в обработке ПДн и характер взаимодействия персонала между собой проводятся на основе:

- анализа внутренних нормативных документов заказчика, регулирующих работу с ПДн;

- анализа должностных инструкций сотрудников, имеющих доступ к ПДн;

- интервьюирования сотрудников.

**Требования к содержанию отчета о результатах обследования текущего состояния ИСПДн**

Отчет должен содержать:

- результаты анализа внутренних документов, регламентирующих порядок обработки и защиты ПДн;

- результаты анализа состава и структуры ИСПДн, используемых в них средств защиты;

- результаты степени участия персонала в обработке ПДн и характера взаимодействия персонала между собой;

- вывод по результатам обследования.

**Требования к содержанию рекомендаций по созданию СЗПДн**

Рекомендации по устранению выявленных несоответствий должны содержать:

- рекомендации по устранению выявленных недостатков СЗПДн;

- рекомендации по введению новых и внесению изменений в существующую документацию, регламентирующую обеспечение защиты ПДн;

- рекомендации по созданию системы защиты ПДн, обеспечивающей нейтрализацию выявленных угроз с использованием методов и способов защиты ПДн, предусмотренных для соответствующего класса ИСПДн;

- рекомендации по обучению персонала, имеющему доступ к ИСПДн и СЗПДн.

**Требования к порядку разработки требований по обеспечению безопасности ПДн при обработке в ИСПДн**

Разработка требований по обеспечению безопасности ПДн при обработке в ИСПДн должна включать следующие подэтапы:

- классификация ИСПДн;

- разработка частной модели угроз безопасности ИСПДн в соответствии с «Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» на основе «Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных»;

- разработка требований к СЗПДн.

Классификация ИСПДн включает: определение характеристик ИСПДн на основе собранной информации, присвоение класса ИСПДн в соответствии с правилами классификации типовых ИСПДн, разработку проекта Распоряжения о классификации ИСПДн.

Подэтап разработки частной модели угроз безопасности ПДн в ИС включает: составление общего перечня угроз безопасности ПДн содержащего данные по угрозам безопасности ПДн, обрабатываемых в ИСПДн, определение актуальности угроз безопасности из Перечня и разработку собственно частной модели угроз безопасности ПДн.

Подэтап разработки требований к СЗПДн включает: определение технических требований к СЗПДн на основе информации о классе ИСПДн и частной модели угроз безопасности ПДн, разработку Плана мероприятий по созданию СЗПДн, разработку требований к составу и содержанию организационно-распорядительной документации, регламентирующей СЗПДн, разработку перечня сертифицированных средств защиты информации, удовлетворяющих требованиям к СЗПДн и позволяющих реализовать мероприятия по созданию СЗПДн.

**Требования к разработке организационно-регламентирующей документации**

На данном этапе разрабатывается документация, регламентирующая: порядок сбора, хранения, обработки, передачи ПДн в составе ИСПДн, порядок доступа в помещения, в которых размещены средства обработки ПДн, порядок организации выполнения услуг по классификации ИСПДн, действия администраторов и пользователей, учет носителей информации, порядок контроля за соблюдением условий  использования  средств  защиты информации, порядок эксплуатации СЗИ в составе СЗПДн и т.д.

В результате выполнения услуг по этапу должны быть разработаны проекты следующих документов:

- положение по организации и выполнения услуг по обеспечению безопасности ПДн при их обработке в ИСПДн;

- требования по обеспечению безопасности ПДн при обработке в ИСПДн;

- инструкции персоналу ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн;

- рекомендации (инструкции) по использованию программных и аппаратных средств защиты информации.

- требования к порядку ввода в действие СЗПДн и Системы защиты сети обработки персональных данных

**Ввод в действие СЗПДн должен включать следующие подэтапы:**

-оценку мероприятий по защите от НСД к ПДн при их обработке в ИСПДн;

- оценку мероприятий по защите информации от утечки по техническим каналам;

- разработку и утверждение отчетных документов.

Оценка мероприятий по защите от НСД к ПДн при их обработке в ИСПДн включает оценку реализации следующих функций:

- управление доступом;

- регистрацию и учет;

- обеспечение целостности;

- контроль отсутствия недекларированных возможностей;

- антивирусную защиту;

- обеспечение безопасного межсетевого взаимодействия ИСПДн;

- анализ защищенности;

- обнаружение вторжений.

Оценка мероприятий по защите информации от утечки по техническим каналам включает:

- проверку соответствия СВТ требованиям стандартов Российской Федерации по электромагнитной совместимости, безопасности, санитарным нормам, предъявляемым к видеодисплейным терминалам;

- оценку нарушений безопасности функционирования ИСПДн и СЗПДн от угроз неатропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера;

- оценку размещения средств вычислительной техники с точки зрения защищенности ПДн от  перехвата с помощью оптических (оптико-электронных) средств.

**Аттестация требований безопасности информации ИСПДн должна включать:**

Анализ и оценка исходных данных и документации по СЗПДн, анализ организационной структуры Заказчика. Проверка условий размещения, монтажа и эксплуатации технических средств, изучение технологического процесса обработки, передачи и хранения информации, анализ информационных потоков, определение состава использованных для обработки, передачи и хранения информации технических средств.

Испытания отдельных технических и программных средств ИСПДн, средств и систем защиты информации на соответствие требованиям защиты информации по утвержденным и согласованным с заявителем методикам испытаний с использованием экспертных методов и инструментальных средств.

Комплексные испытания ИСПДн на соответствие требованиям по защите информации (с попытками реализации НСД к защищаемой информации по различным сценариям, имитирующим действия нарушителей ИБ).

Подготовка отчетной документации — протоколов испытаний и заключения по результатам аттестационных испытаний и Аттестата соответствия по требованиям безопасности информации.

# **Порядок приемки работ**

Для проверки выполнения заданных функций системы, соответствия создаваемой системы требованиям технического задания, должны быть проведены приемочные испытания.

По результатам приемочных испытаний должен быть разработан «Акт приемочных испытаний».

Для проведения испытаний создается комиссия, в которую входят все заинтересованные сотрудники Заказчика и представители Исполнителя.

Результаты испытаний отражают в протоколе проведения испытаний

# **Требования к документированию**

Требования к методическому обеспечению СЗПДн определяются:

* нормативно-правовыми актами и стандартами РФ в области информационной безопасности и защиты информации;
* нормативно-распорядительными и методическими документами ФСБ России, ФСТЭК России, Министерства информационных технологий и связи России;
* источниками нормативно-справочной информации государственных органов исполнительной власти;
* ведомственными документами;
* регламентами информационного взаимодействия с внешними государственными организациями.

# **Требования к составу разрабатываемых документов по СЗПДн**

В процессе проектирования должны быть определены требования к составу, структуре и порядку взаимодействия административного персонала обслуживающего СЗПДн.

Внутренняя нормативная и организационно-распорядительная документация представлена в составе, указанном ниже.

На этапе разработки комплекта нормативной и организационно-распорядительной документации дополнительно должны быть разработаны проекты следующих документов:

* инструкция администратора ИБ ИСПДн;
* инструкция администратора ИСПДн;
* инструкция по организации антивирусной защиты ИСПДн;
* инструкция по резервному копированию защищаемой информации в ИСПДн;
* инструкция по порядку проведения проверок состояния защиты ПДн;
* инструкция пользователя ИСПДн;
* регламент учета средств защиты, документации и электронных носителей ПДн;
* приказ о вводе в промышленную эксплуатацию СЗПДн в ИСПДн;
* приказ о допуске сотрудников к обработке ПДн;
* приказ о назначении администратора ИБ ИСПДн;
* приказ о создании комиссии для определения уровня защищенности ИСПДн;
* приказ о создании комиссии по контролю защищенности ПДн;
* приказ о создании комиссии по уничтожению ПДн;
* приказ о назначении ответственного за обеспечение безопасности ПДн;
* приказ об утверждении мест хранения материальных носителей ПДн;
* план внутренних проверок состояния защиты ПДн;
* план мероприятий по защите ПДн;
* порядок парольной защиты в ИСПДн;
* акт классификации ИСПДн;
* положение по организации и проведению работ по обработке и защите ПДн, обрабатываемых в ИСПДн;
* журнал регистрации письменных запросов граждан на доступ к своим персональным данным;
* журнал учета носителей ПДн;
* журнал учета посетителей.

До этапа аттестации должна быть разработана документация в составе:

* акт обследования (аналитически отчет) информационной системы ПДн;
* перечень технических и программных средств разрешенных к эксплуатации на объекте  информатизации;
* перечень защищаемых информационных ресурсов объекта информатизации;
* матрица доступа пользователей к ресурсам объекта информатизации;
* схема границ контролируемой зоны;
* частная модель угроз персональных данных
* акт определения уровня защищенности ИСПДн;
* технический паспорт объекта информатизации;
* техническое задание на создание системы защиты информационной системы объекта информатизации;
* акт установки средств защиты.
* приказ «О назначении комиссии по подготовке к аттестации ИС»;
* приказ «О вводе ИС в промышленную эксплуатацию»;

По результатам аттестации должна быть разработана документация в составе:

* программа и методики аттестационных испытаний;
* протоколы аттестационных испытаний объекта информатизации;
* заключение по результатам аттестационных испытаний объекта информатизации;
* аттестат соответствия;

# **Дополнительные требования**

В процессе работы возможно изменение состава (перечня) и наименования документов, при обосновании таких изменений требованиями нормативных или методических документов и согласовании таких изменений с заказчиком.

Разработанные проекты документов должны соответствовать требованиям действующего законодательства Российской Федерации.

Сторона, получившая конфиденциальную информацию, обязана использовать ее исключительно в целях выполнения настоящего технического задания, охранять ее конфиденциальность, если иное прямо не установлено законом.

# **Требования к участникам размещения заказа**

наличие у Исполнителя лицензий:

* лицензии ФСТЭК России на право осуществления деятельности по технической защите конфиденциальной информации;
* Лицензия ФСБ России на осуществление разработки, производства, распространения шифровальных (криптографических) средств, защищённых с использованием шифровальных (криптографических) средств, выполнения работ, оказания услуг в области шифрования информации, технического обслуживания шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя).
* Сертификат ИСО 9001:2008 – международная система управления качеством
* Свидетельство об аккредитации в области персональных данных

1. **Заключительные положения**

8.1. Технологические работы должны проводиться специалистами Исполнителя, сертифицированными по системе «1С», в соответствии с требованиями разработчика «1С» (<http://its.1c.ru/db/aboutits#content:2:1>). В противном случае информационно-технологическое сопровождение (1С:ИТС) не может быть осуществлено.

8.2. Обучение и консультирование пользователей должно производиться на рабочих местах сотрудников Заказчика по заявкам Заказчика или лица, им уполномоченного.

8.3. Все работы должны быть выполнены в соответствии с действующим законодательством РФ, регламентирующим данный вид деятельности.

1. **Требования по объему гарантий качества работ: 100%.**

На основании ст. 1225-1233 ГК РФ услуги оказываются специалистами, сертифицированными по системе «1С:Предприятие» и владеющими текущими настройками эксплуатируемых в МФЦ информационных систем.

**Минимально необходимый набор сертификатов для выполнения работ**

Сертификат «1С:Специалист» по платформе «1С:Предприятие» 8, - 2шт.

Сертификат «1С:Профессионал» по конфигурации «1С:Документооборот 8» - 2 шт.

1. **Требования по сроку гарантий качества на результаты работ:**

Исполнитель берет на себя гарантийные обязательства в течение срока действия контракта по устранению выявленных недочетов.

1. **Порядок сдачи и приемки результатов работ:**

Акты (накладные) приемки-сдачи работ (услуг, товаров, Права) составляются после оказания каждого этапа (части этапа) работ.

1. **Требования по техническому обучению Исполнителем персонала заказчика работе на подготовленных объектах:**

в результате обучения специалисты Заказчика должны уметь самостоятельно работать в системе в рамках назначенных им ролей.

1. **Требования по объему гарантий качества работ**:

В гарантийный период все услуги оказываются за счет Исполнителя, время реакции на заявку – не более 30 минут.

1. **Требования по сроку гарантий качества на результаты работ**:

Срок гарантии на программные элементы системы – в течение срока действия контракта.