«ТЕХНИЧЕСКИЕ УСЛОВИЯ НА ПОДКЛЮЧЕНИЕ ГОСУДАРСТВЕННЫХ УЧРЕЖДЕНИЙ И ОРГАНИЗАЦИЙ К ЗАЩИЩЕННОЙ СЕТИ ПЕРЕДАЧИ ДАННЫХ АДМИНИСТРАЦИИ ГУБЕРНАТОРА АРХАНГЕЛЬСКОЙ ОБЛАСТИ И ПРАВИТЕЛЬСТВА АРХАНГЕЛЬСКОЙ ОБЛАСТИ»

Листов 18

г. Архангельск, 2013

Инв. № подл. | Подпись и дата | Взам. инв. № | Инв. № дубл. | Подпись и дата

СОГЛАСОВАНО

Директор

государственного автономного учреждения Архангельской области «Управление информационно-коммуникационных технологий Архангельской области»

_____ ***Л.О. Эмке***

«14» октября 2013 г.

УТВЕРЖДАЮ

Директор

департамента информационных технологий администрации Губернатора Архангельской области и Правительства Архангельской области

_____ ***И.А. Иванов***

«___» _____ 2013 г.

«ТЕХНИЧЕСКИЕ УСЛОВИЯ НА ПОДКЛЮЧЕНИЕ ГОСУДАРСТВЕННЫХ УЧРЕЖДЕНИЙ И ОРГАНИЗАЦИЙ К ЗАЩИЩЕННОЙ СЕТИ ПЕРЕДАЧИ ДАННЫХ АДМИНИСТРАЦИИ ГУБЕРНАТОРА АРХАНГЕЛЬСКОЙ ОБЛАСТИ И ПРАВИТЕЛЬСТВА АРХАНГЕЛЬСКОЙ ОБЛАСТИ»

ЛИСТ УТВЕРЖДЕНИЯ

Листов ЛУ 1

РАЗРАБОТАНО

Директор

общества с ограниченной ответственностью «Центр Комплексной Безопасности»

Лицензия ФСТЭК на деятельность по технической защите информации № 1730 от 02 ноября 2011 г. Действительна до 02 ноября 2016 г..

_____ *С.П. Кирчигин*

«10» сентября 2013 г.

Изм.	Лист	№ документа	Подпись	Дата	90249648.425760.001.ТУ	Лист 2

Подпись и дата | Инв. № дубл. | Взам. инв. № | Подпись и дата | Инв. № подл.

ВВЕДЕНИЕ

Настоящие технические условия определяют требования и условия, а также устанавливают порядок подключения автоматизированных информационных систем государственных учреждений и организаций, иных уполномоченных организаций (далее-внешние АИС) к Защищенной сети передачи данных (далее-ЗСПД) администрации Губернатора Архангельской области и Правительства Архангельской области. ЗСПД обеспечивает телекоммуникационный и сетевой уровень функционирования Архангельской региональной системы межведомственного электронного взаимодействия, а также других информационных систем в сфере предоставления государственных и муниципальных услуг. Администрация Губернатора Архангельской области и Правительство Архангельской области является оператором ЗСПД, ответственная за обеспечение и эксплуатацию информационных систем в сфере предоставления государственных и муниципальных услуг

Настоящие технические условия разработаны в соответствии с Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27 июля 2010 года № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», Постановлением Правительства РФ от 01 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказом Минкомсвязи от 27 декабря 2010 года № 190 «Об утверждении технических требований к взаимодействию информационных систем в единой системе межведомственного электронного взаимодействия», нормативными правовыми актами, техническими и методическими документами ФСТЭК России и ФСБ России в области обеспечения информационной безопасности и защиты персональных данных.

Требования технических условий устанавливают состав, содержание, а также порядок выполнения работ по подключению внешних АИС к ЗСПД, состав программно-технических средств, в том числе средств защиты информации, необходимых для организации защищенного взаимодействия внешних АИС и функционирующими информационными системами на базе ЗСПД администрации Губернатора Архангельской области и Правительства Архангельской области.

СОДЕРЖАНИЕ

1. ОСНОВНЫЕ ПОЛОЖЕНИЯ

1.1 Описание ЗСПД

Защищенная сеть передачи данных построена на основе Архангельской региональной системы межведомственного электронного взаимодействия (далее-АРСМЭВ), организатором и оператором которой является администрация Губернатора Архангельской области и Правительства Архангельской области, а также других информационных систем в сфере предоставления государственных и муниципальных услуг.

АРСМЭВ обеспечивает межведомственное информационное взаимодействие при предоставлении в электронной форме государственных услуг, муниципальных услуг и иных услуг, сведения о которых размещаются в государственной информационной системе Архангельской области "Архангельский региональный портал государственных и муниципальных услуг" (далее - государственные и муниципальные услуги).

Обладателем информации, содержащейся в региональной системе, является Архангельская область.

Основными функциями АРСМЭВ являются:

- обеспечение передачи запросов, иных документов и сведений, необходимых для получения государственных и муниципальных услуг и поданных заявителями через порталы, в подключенные к ней информационные системы органов и организаций, обязанных предоставить испрашиваемые государственные и муниципальные услуги;

- обеспечение обмена электронными сообщениями между органами и организациями, информационные системы которых подключены к АРСМЭВ, при предоставлении государственных и муниципальных услуг и исполнении государственных и муниципальных функций в электронной форме;

- обеспечение передачи на порталы запросов, иных документов и сведений, обработанных в информационных системах органов и организаций, а также информации о ходе и результатах выполнения запросов о предоставлении государственных и муниципальных услуг и исполнении государственных и муниципальных функций в электронной форме.

Передача данных в АРСМЭВ обеспечивается за счет использования каналов и сетей доступа операторов связи, предоставляющих услуги доступа к сети Интернет, и возможностей передачи данных непосредственно в сети Интернет.

Логическая изоляция и выделение АРСМЭВ, а также защита информации

при ее передаче в АРСМЭВ по открытым каналам осуществляются за счет использования технологии виртуальных частных сетей - VPN, реализованной на базе продуктов семейства ViPNet компании ОАО «ИнфоТеКС».

Основными сетевыми телекоммуникационными протоколами, используемыми в АРСМЭВ, являются протоколы семейства TCP/IP. Для организации АРСМЭВ используется телекоммуникационное и сетевое оборудование различных производителей, а в качестве криптографических средств, обеспечивающих защиту каналов связи - Программно-аппаратный комплекс/программный комплекс «ViPNet Координатор» и «ViPNet Клиент»

1.2 Характеристика АРСМЭВ и внешних систем

Региональная система функционирует в соответствии с техническими требованиями к взаимодействию информационных систем в единой системе межведомственного электронного взаимодействия.

Информационное взаимодействие с оператором единой системы межведомственного электронного взаимодействия осуществляется в порядке, установленном нормативными правовыми актами Российской Федерации.

Субъектами отношений, возникающих в связи с формированием и функционированием региональной системы (далее - участники информационного обмена региональной системы), являются:

1.2.1. оператор региональной системы;

1.2.2. исполнительные органы государственной власти Архангельской области, осуществляющие с использованием государственных информационных систем Архангельской области, операторами которых они являются, или с использованием Архангельской региональной системы исполнения регламентов предоставление:

- государственных услуг Архангельской области;

- сведений, находящихся в их распоряжении и являющихся необходимыми для предоставления государственных, муниципальных услуг, органам, предоставляющим государственные услуги, органам, предоставляющим муниципальные услуги, организациям, участвующим в предоставлении государственных и муниципальных услуг, или многофункциональным центрам предоставления государственных и муниципальных услуг;

- в государственную информационную систему о государственных и муниципальных платежах сведений, находящихся в их распоряжении и являющихся необходимыми для уплаты денежных средств физическими и юридическими лицами за государственные и муниципальные услуги, а также

иных платежей, являющихся источниками формирования бюджетов бюджетной системы Российской Федерации;

1.2.3. федеральные органы исполнительной власти, органы государственных внебюджетных фондов, осуществляющие предоставление государственных услуг с использованием государственных информационных систем Российской Федерации, операторами которых они являются, или с использованием Архангельской региональной системы исполнения регламентов;

1.2.4. местные администрации муниципальных образований Архангельской области, органы местных администраций муниципальных образований Архангельской области, осуществляющие с использованием муниципальных информационных систем Архангельской области, операторами которых они являются, или с использованием Архангельской региональной системы исполнения регламентов предоставление:

- муниципальных услуг, государственных услуг Архангельской области, переданных для осуществления органам местного самоуправления;

- сведений, находящихся в их распоряжении и являющихся необходимыми для предоставления государственных, муниципальных услуг, органам, предоставляющим государственные услуги, органам, предоставляющим муниципальные услуги, организациям, участвующим в предоставлении государственных и муниципальных услуг, или многофункциональным центрам предоставления государственных и муниципальных услуг;

- в государственную информационную систему о государственных и муниципальных платежах сведений, находящихся в их распоряжении и являющихся необходимыми для уплаты денежных средств физическими и юридическими лицами за государственные и муниципальные услуги, а также иных платежей, являющихся источниками формирования бюджетов бюджетной системы Российской Федерации;

1.2.5. организации, осуществляющие с использованием информационных систем, операторами которых они являются, или с использованием Архангельской региональной системы исполнения регламентов:

- участие в предоставлении государственных, муниципальных или иных услуг;

- предоставление в государственную информационную систему о государственных и муниципальных платежах сведений, находящихся в их распоряжении и являющихся необходимыми для уплаты денежных средств физическими и юридическими лицами за государственные и муниципальные

услуги, а также иных платежей, являющихся источниками формирования бюджетов бюджетной системы Российской Федерации.

Региональная система включает совокупность содержащейся в базах данных информации, а также информационные технологии и технические средства, обеспечивающие взаимодействие информационных систем участников информационного обмена региональной системы.

В базах данных региональной системы содержатся сведения:

- об используемых участниками информационного обмена региональной системы программных и технических средствах, обеспечивающих возможность доступа через региональную систему к их информационным системам (далее - электронные сервисы);

- об истории движения в региональной системе электронных сообщений при предоставлении государственных и муниципальных услуг в электронной форме.

В функционирующих на безе ЗСПД информационных системах, отнесенные ко 2 и 3 классам уровней защиты обрабатываются сведения субъектов персональных данных (далее-ПДн), а также общедоступные и обезличенные ПДн в зависимости от конкретной информационной системы.

Доступ к обрабатываемым сведениям, содержащим обезличенные персональные и общедоступные данные, из-за пределов ЗСПД организован посредством веб-сайта pgu.dvinaland.ru, обращение к которому осуществляется через сеть международного информационного обмена Интернет.

2. ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ

2.1 Требования к организации подключения

Организация подключения внешней АИС к ЗСПД должна соответствовать требованиям приказа ФСТЭК России от 11.02.2013 г. № 17 « Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и приказа Минкомсвязи России от 27 декабря 2010 г. № 190 «Об утверждении технических требований к взаимодействию информационных систем в единой системе межведомственного электронного взаимодействия», требований иных нормативных технических и методических документов ФСТЭК России и ФСБ России в области обеспечения безопасности и защиты информации, а также настоящих ТУ.

Безопасность сведений ограниченного доступа, обрабатываемых в функционирующих на базе ЗСПД администрации Губернатора Архангельской

области и Правительства Архангельской области, при их передаче по сетям связи общего пользования должна быть обеспечена посредством организации защищенного взаимодействия между функционирующими на базе ЗСПД ИС и подключаемой внешней АИС.

Для обеспечения безопасности информации до выполнения работ по подключению внешней АИС к ЗСПД должна быть выбрана одна из следующих схем защищенного взаимодействия:

2.1.1. Схема № 1 - взаимодействие АИС, состоящей из одного специализированного АРМ, оборудованного сертифицированными по требованиям безопасности информации ФСТЭК России и ФСБ России средств защиты информации (далее-СЗИ) и средств криптографической защиты информации (далее-СКЗИ), а также наличие оценки эффективности принятых мер по обеспечению безопасности персональных данных.

2.1.2. Схема № 2 - взаимодействие с учетом наличия у подключаемой внешней АИС внутренних АРМ, с использованием сертифицированных по требованиям безопасности информации ФСТЭК России и ФСБ России СЗИ и СКЗИ, а также действующего аттестата соответствия требованиям по безопасности информации.

Структурная схема подключения автоматизированного рабочего места представлена на рисунке 1 и автоматизированной информационной системы на рисунке 2.

В соответствии с Приказом ФСТЭК от 11.02.2013 г. № 17 внешним автоматизированным информационным системам необходимо обеспечить 2, 3 и 4 уровни защищённости персональных данных. Все Пользователи (Участники) ЗСПД должны иметь представление об организационных, технических и программно-аппаратных требованиях, предъявляемых к данным классам защищенности, и выполнять их.

Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата

Изм.	Лист	№ документа	Подпись	Дата

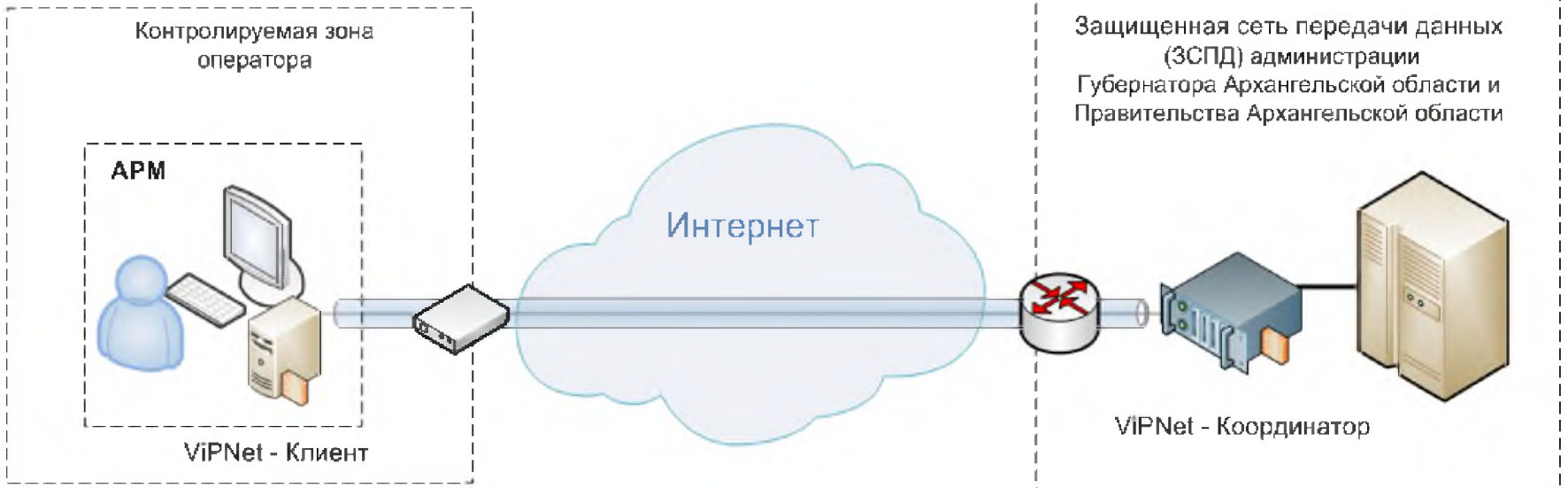

Рис.1 Структурная схема подключения АРМ (Схема №1)

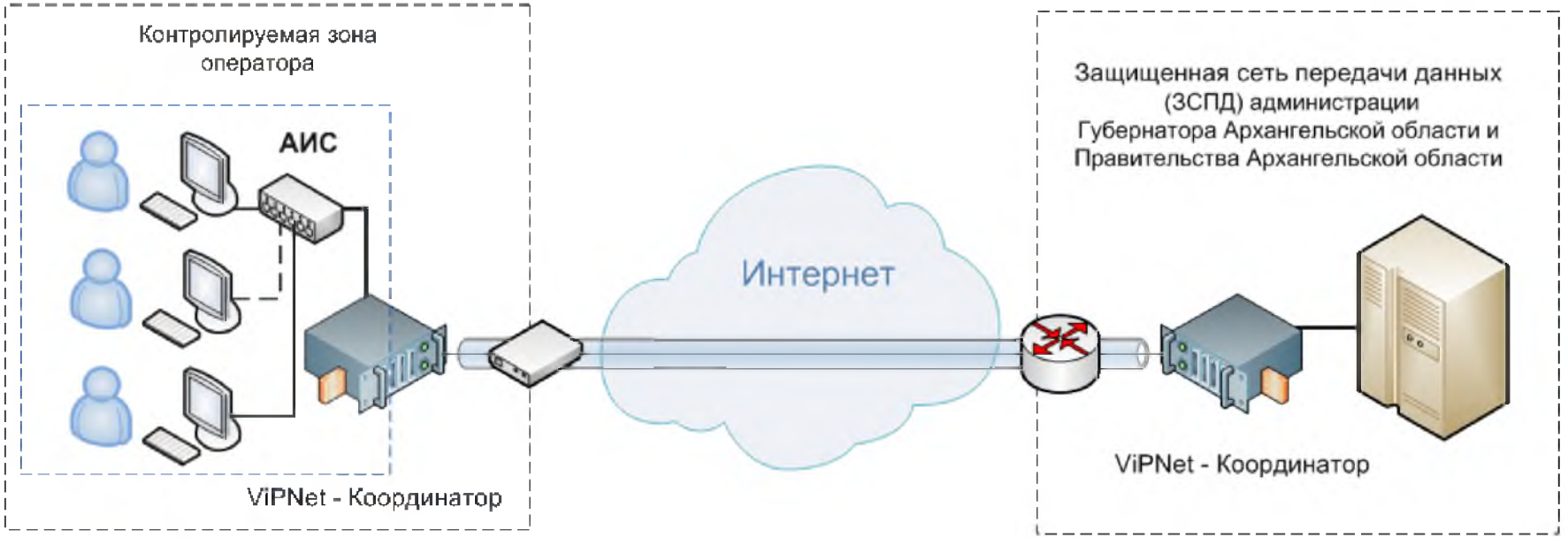

Рис.2 Структурная схема подключения АИС (Схема №2)

90249648.425760.001.ТУ

Лист
11

2.2 Требования к реализации защищенного взаимодействия

*2.2.1. Требования к реализации **схемы №1** защищенного взаимодействия.*

2.2.1.1. Для организации взаимодействия с функционирующими на базе ЗСПД должно быть использовано специализированное АРМ, оборудованное сертифицированными по требованиям безопасности информации ФСТЭК России и ФСБ России СЗИ и СКЗИ.

2.2.1.2. Помещение для размещения специализированного АРМ должно удовлетворять требованиям ТУ и эксплуатационной документации (ЭД) на используемые в реализации типовой схемы №1 АРМ, СЗИ и СКЗИ.

2.2.1.3. Специализированное АРМ должно быть подключено только к информационно-телекоммуникационным сетям, используемым для связи с ЗСПД. Подключение специализированного АРМ к другим АИС и к другим локальным вычислительным сетям не допускается.

2.2.1.4. Установка, монтаж, запуск и первоначальная настройка специализированного АРМ должны проводиться в заданном помещении в соответствии с требованиями ТУ и ЭД на АРМ, СЗИ и СКЗИ.

2.2.1.5. Схема подключения, сетевые настройки АРМ и дополнительные настройки установленных СЗИ и СКЗИ должны соответствовать типовым требованиям п.2.1.1., в отдельном случае схема подключения согласовывается с государственным автономным учреждением Архангельской области «Управление информационно-коммуникационных технологий Архангельской области» (далее-ГАУ АО «Управление ИКТ АО»).

2.2.1.6. Эксплуатация специализированного АРМ должна осуществляться в соответствии с требованиями ЭД на АРМ и используемые СЗИ и СКЗИ.

*2.2.2. Требования к реализации **схема № 2** защищенного взаимодействия.*

2.2.2.1. Подключаемая АИС должна иметь действующий аттестат соответствия требованиям информационной безопасности ФСТЭК 2 класса защищенности.

2.2.2.2. В системе защиты ПДн подключаемой АИС должны использоваться СЗИ и СКЗИ, совместимые со средствами применяемыми в ЗСПД, в частности ПАК «VipNet Координатор» версии 3.х. Для организации защищенного канала связи с ЗСПД должно быть использовано СКЗИ, сертифицированное или имеющее положительное заключение ФСБ России, с классом криптографической защиты не ниже КС3. Подключение АИС к ЗСПД должно быть реализовано только посредством данного СКЗИ.

2.2.2.3. Для обеспечения безопасного межсетевого взаимодействия с АИС ЗСПД должно быть использовано средство межсетевого экранирования

(МЭ), имеющее сертификат соответствия требованиям РД «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» ФСТЭК России не ниже 3 класса защищенности.

2.2.2.4. Помещения для размещения технических средств СКЗИ и средств МЭ должны удовлетворять требованиям ТУ и ЭД на данные средства.

2.2.2.5. Схема подключения СКЗИ и средств МЭ, а также необходимые для их корректного функционирования настройки должны быть выполнены в соответствии с инструкцией по подключению к сети ЗСПД, либо предварительно согласованы с ГАУ АО «Управление ИКТ АО».

2.2.2.6. Установка, монтаж, запуск и первоначальная настройка СКЗИ и средства МЭ должны быть проведены в заданных помещениях в соответствии с требованиями ТУ и ЭД на данные средства.

2.2.2.7. Эксплуатация СКЗИ и средств МЭ должна осуществляться в соответствии с требованиями эксплуатационной документации на данные средства.

2.3 Специальные требования

К проведению работ по установке, монтажу и настройке СКЗИ и СЗИ должны допускаться исполнители, имеющие соответствующий уровень квалификации, из числа сотрудников организаций, обладающих необходимыми лицензиями ФСТЭК России и ФСБ России на осуществление данных видов деятельности

Все используемые для организации защищенного взаимодействия СЗИ должны иметь действующий сертификат соответствия ФСТЭК России требованиям РД «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия не декларированных возможностей» не ниже 4 уровня контроля.

2.4 Требования по информационной безопасности

К основным организационным требованиям по информационной безопасности относятся:

2.4.1 реализация разрешительной системы допуска пользователей (обслуживающего персонала) к информационным ресурсам, информационной системе и связанным с ее использованием работам, документам;

2.4.2 ограничение доступа пользователей в помещения, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также хранятся носители информации;

2.4.3 разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;

2.4.4 регистрация действий пользователей и обслуживающего персонала, контроль несанкционированного доступа и действий пользователей, обслуживающего персонала и посторонних лиц;

2.4.5 учет и хранение съемных носителей информации и их обращение, исключающее хищение, подмену и уничтожение;

2.4.6 организация физической защиты помещений и собственно технических средств, позволяющих осуществлять обработку персональных данных;

2.4.7 проведение аттестационных испытаний информационных систем персональных данных по требованиям защиты информации (Аттестация выполняется компаниями, имеющими лицензию ФСТЭК России «Техническая защита конфиденциальной информации»).

2.5 Технические требования по информационной безопасности

Основные технические требования по информационной безопасности:

2.5.1 каналы связи, выходящие за пределы контролируемых зон, должны быть защищены с помощью средств криптографической защиты информации, удовлетворяющие установленным требованиям (в соответствии приказу Минкомсвязи от 27.12.10 №190);

2.5.2 объекты информатизации должны быть аттестованы по требованиям безопасности информации в соответствии с методическими документами Федеральной службы по техническому и экспортному контролю (ФСТЭК России);

2.5.3 доступ к АРСМЭВ через сети общего пользования, включая сеть международного информационного обмена Интернет, должен производится с использованием защищенных каналов связи (Программные продукты линейки ViPNet сертификат ФСБ России № СФ/115-1285 от 27 февраля 2009 года на соответствие требованиям ФСБ России);

2.5.4 на серверном оборудовании и автоматизированных рабочих местах должны использоваться сертифицированные средства антивирусной защиты;

2.5.5 каналы передачи данных, выходящие за пределы контролируемой зоны, должны быть включены через межсетевые экраны с целью управления доступом, фильтрации сетевых пакетов и трансляции сетевых адресов для скрытия структуры информационной системы;

2.5.6 должны использоваться сертифицированные средства защиты информации, при выполнении следующих функций:

2.5.7 централизованное управление системой защиты персональных данных информационной системы;

2.5.8 периодический анализ безопасности установленных межсетевых экранов на основе имитации внешних атак на информационные системы;

2.5.9 активный аудит безопасности информационной системы на предмет обнаружения в режиме реального времени несанкционированной сетевой активности;

2.5.10 управление доступом к защищаемым персональным данным информационной сети;

2.5.11 аутентификация взаимодействующих информационных систем и проверка подлинности пользователей и целостности передаваемых данных.

2.6. Требования к реализации защищенного взаимодействия

Требования к организации защищенного VPN-канала.

Организация защищенного канала строится на базе сети общего пользования, включая сеть международного информационного обмена Интернет. К организации защищенного канала предъявляются следующие требования:

2.6.1. наличие минимум одного подключения к сети общего пользования Интернет со следующей скоростью доступа:

2.6.2. одно рабочее место: минимальная (рекомендуемая) скорость передачи данных – 256 (512) Кбит/с;

2.6.3. от 2 до 5 ПК: минимальная (рекомендуемая) скорость передачи данных - 512 (1024) Кбит/с;

2.6.4. от 6 до 150 ПК: минимальная (рекомендуемая) скорость передачи данных - 2 (20) Мбит/с;

2.6.5. более 150 ПК: минимальная (рекомендуемая) скорость передачи данных - 10 (32) Мбит/с.

2.6.6. между локально-вычислительной сетью Участника АРСМЭВ и сетью общего пользования должны быть установлены крипто-шифровальные устройства с функцией межсетевого экрана, к которым предъявляются следующие требования:

- должны быть из линейки VipNet (обусловлено тем, что АРСМЭВ вместе с центральным узлом простроено на базе VipNet: защищенная сеть);

- должны иметь сертификаты Федеральной службы по техническому и экспортному контролю (ФСТЭК) по требованиям к межсетевым экранам по 3

классу, отсутствию не декларируемых возможностей по 3 уровню, иметь оценочный уровень доверия не ниже 4+ и возможностью использования в автоматизированных системах до класса 1Г включительно;

- иметь сертификат Федеральной службы безопасности Российской Федерации (ФСБ России) по требованиям к средствам криптографической защиты информации не ниже КС3;

- использовать протоколы туннелирования с инкапсуляцией любого IP-трафика приложений в IP#241 и UDP;

- алгоритм шифрования должен соответствовать ГОСТ 28147-89 (256 бит).

В зависимости от масштабов подключаемой сети Участника ЗСПД выбираются соответствующие пограничные криптошлюзы или программные средства:

- 1-2 рабочих места: VipNet Client;

- 3-10 рабочих места: VipNet-координатор HW-100C;

неограниченное число пользователей: VipNet HW1000.

3. ПРАВИЛА ПРИЕМКИ

3.1 Общие положения

Для осуществления приемки подключения внешней АРМ или АИС к ЗСПД устанавливаются следующие категории контрольных испытаний:

- приемо-сдаточные испытания;

- периодические испытания.

3.2 Приемо-сдаточные испытания

Приемо-сдаточные испытания проводятся непосредственно после завершения работ по подключению внешней АИС к ЗСПД. Данные испытания должны быть проведены ответственными исполнителями со стороны подключаемой АИС совместно с представителями организации, осуществлявших установку, монтаж и настройку СКЗИ и СЗИ.

По завершению испытаний должен быть составлен совместный акт сдачи-приемки работ с обязательной отметкой о соответствии требованиям настоящих ТУ.

3.2.1. Проверка организации схемы защищенного взаимодействия .

При проведении приемо-сдаточных испытаний подключения по схеме защищенного взаимодействия АИС ЗСПД с аттестованной АИС должны быть выполнены следующие проверки:

3.2.1.1. проверка наличия у подключаемой АИС действующего аттестата соответствия;

3.2.1.2. проверка комплектности СЗИ и СКЗИ, используемых для организации защищенного взаимодействия, в соответствии с ТУ и ЭД на данные средства;

3.2.1.3. проверка наличия у СЗИ и СКЗИ, используемых для организации защищенного взаимодействия, действующих сертификатов соответствия;

3.2.1.4. проверка выполнения требований и рекомендаций по размещению технических средств СЗИ и СКЗИ;

3.2.1.5. проверка корректности подключения и настроек СЗИ и СКЗИ, используемых для организации защищенного взаимодействия, в соответствии с схемой подключения и необходимыми настройками, а также требованиями ТУ и ЭД на данные средства;

3.2.1.6. проверка наличия защищенного канала связи между подключаемой АИС и ЗСПД.

Результаты проведенных проверок должны быть зафиксированы в отдельном протоколе испытаний, составляемом ответственными исполнителями со стороны подключаемой АИС.

3.3 Периодические испытания

Данные испытания предназначены для периодического контроля заданных при подключении внешней АИС к АИС ЗСПД показателей.

Результаты проведенных проверок должны быть зафиксированы в отдельном протоколе периодических испытаний, составляемом ответственными исполнителями со стороны подключаемой АИС.

Состав и содержание проверок должны соответствовать пункту 3.2 настоящих ТУ

Периодические испытания должны проводиться не реже одного раза в год.

4. КОНТРОЛЬ РЕАЛИЗАЦИИ ПОДКЛЮЧЕНИЯ К ЗСПД

Ответственность за соблюдение требований настоящих ТУ, а так же за соблюдение требований к эксплуатации СЗИ, используемых в выбранной схеме подключения лежит на владельцах подключаемых АИС.

Протоколы приёмочных испытаний и протоколы периодических испытаний, подписанные ответственными за проведение данных испытаний лицами, должны быть предоставлены для проверки в государственное автономное учреждение Архангельской области

«Управление информационно-коммуникационных технологий Архангельской области» в течение 5 рабочих дней по факту получения соответствующего запроса из ГАУ АО «Управление ИКТ АО».

В случае выявления нарушений требований настоящих ТУ, ГАУ АО «Управление ИКТ АО» немедленно производит отключение соответствующей внешней АИС от ЗСПД.

5. ОПРЕДЕЛЕНИЯ, ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АИС	*Автоматизированная информационная система*
АРМ	*Автоматизированное рабочее место*
ЗСПД	*Защищенная сеть передачи данных*
ИСПДн	*Информационная система персональных данных*
МЭ	*Межсетевое экранирование*
ПАК	*Программно-аппаратный комплекс*
ПДн	*Персональные данные*
РД	*Руководящий документ*
АРСМЭВ	*Региональная система межведомственного электронного взаимодействия*
СЗИ	*Средство защиты информации*
СКЗИ	*Средство криптографической защиты информации*
ТУ	*Технические условия*
ФСБ	*Федеральная служба безопасности*
ФСТЭК	*Федеральная служба по техническому и экспортному контролю*
ЭД	*Эксплуатационная документация*

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ.

Изм.	*Номера листов (страниц)*				*Всего листов (страниц) в докум.*	*Номер докум.*	*Входящий № сопроводительного докум. и дата*	*Подпись*	*Дата*
	изменённых	*замененных*	*новых*	*аннулированных*					