УТВЕРЖДАЮ
Директор
ГАУ АО «Управление ИКТ АО»

_____ Матвеев Д.В.

«26» августа 2022 года

ТЕХНИЧЕСКИЕ УСЛОВИЯ

на подключение внешних пользователей и информационных систем
к автоматизированной информационной системе управления
финансово-хозяйственной деятельностью органов государственной власти,
иных государственных органов и государственных учреждений
Архангельской области

Оглавление

ВВЕДЕНИЕ

Настоящие технические условия (далее - технические условия, ТУ) определяют требования и условия, а также устанавливают порядок подключения внешних пользователей и информационных систем к автоматизированной информационной системе управления финансово-хозяйственной деятельностью органов государственной власти, иных государственных органов и государственных учреждений Архангельской области (далее - АИС ФХД).

Настоящие технические условия разработаны в соответствии с Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Постановлением Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», нормативными правовыми актами, техническими и методическими документами ФСТЭК России и ФСБ России в области обеспечения информационной безопасности и защиты персональных данных.

Требования технических условий распространяются на исполнительные органы государственной власти Архангельской области и иные государственные органы, подведомственные им учреждения и организации, в том числе государственные учреждения Архангельской области, подключенные или подключаемые к АИС ФХД.

1. ОСНОВНЫЕ ПОЛОЖЕНИЯ

1.1. Описание АИС ФХД

АИС ФХД предназначена для централизованного ведения бухгалтерского учета и кадрового документооборота служащих и работников исполнительных органов государственной власти и государственных учреждений Архангельской области.

Основными целями создания АИС ФХД являются:

обеспечение прозрачности, открытости и подотчетности финансово-хозяйственной деятельности органов государственной власти, иных государственных органов и государственных учреждений Архангельской области;

повышение качества и достоверности, оперативное формирование бухгалтерской (бюджетной) и управленческой отчетности;

повышение качества финансового менеджмента организаций сектора государственного управления за счет формирования единого информационно-аналитического пространства;

формирование и развитие единой методологии и технологического обеспечения управления финансово-хозяйственной деятельности органов государственной власти, иных государственных органов и государственных учреждений Архангельской области.

АИС ФХД обеспечивает выполнение следующих задач:

ввод и хранение информации в объеме, необходимом для оформления первичных учетных документов и формирования регистров бухгалтерского учета;

регистрация входящих первичных учетных документов;

оформление исходящих первичных учетных документов (формирование в бумажном и/или электронном виде);

хранение сформированных первичных документов в электронном виде в информационной базе;

формирование регистров учета по учетным данным с получением твердых копий на бумажном носителе на типовых бланках;

формирование регистров учета, стандартных и специализированных отчетов с различной группировкой и иерархией представления данных;

формирование регламентированной бухгалтерской, налоговой и статистической отчетности;

формирование типовой аналитической отчетности о финансово-хозяйственной деятельности;

электронный обмен данными в форматах Федерального казначейства, УФЭБС, с использованием стандарта «1С:Предприятие – Клиент банк», настраиваемый механизм обмена информацией с казначейскими системами;

электронный документооборот с ИФНС, ПФР, ФСС и ФСГС посредством подключения к соответствующим сервисам данных органов и выгрузки формализованных отчетов по защищенным получающей стороной каналам связи с обратной отправкой подтверждения;

возможность обмена данными между подсистемами, в части отражения начислений, удержаний, налогов и взносов в бухгалтерском и бюджетном учете;

возможность управления процессом ведения бухгалтерского учета и подготовки отчетности по децентрализованной схеме – ведение учета непосредственно в органах государственной власти, иных государственных органах и государственных учреждениях.

Передача данных в АИС ФХД 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 АИС ФХД, а также защита информации при ее передаче в АИС ФХД 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 АИС ФХД, являются протоколы семейства TCP/IP. Для организации АИС ФХД 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 АИС ФХД, внешних пользователей и информационных систем

Субъектами отношений, возникающих в связи с формированием и функционированием АИС ФХД (далее - участники информационного взаимодействия АИС ФХД), являются:

1) государственное автономное учреждение Архангельской области "Управление информационно-коммуникационных технологий Архангельской области" (далее - оператор АИС ФХД);

2) исполнительные органы государственной власти Архангельской области и иные государственные органы, подведомственные им учреждения и организации, в том числе государственные учреждения Архангельской области (далее - пользователи АИС ФХД);

3) организация, обеспечивающая техническое сопровождение прикладного программного обеспечения АИС ФХД, определенная по результатам конкурсных процедур в соответствии с Федеральным законом от 18 июля 2011 г. № 223-ФЗ (далее - подрядная организация).

АИС ФХД включает совокупность содержащейся в базах данных информации, а также информационные технологии и технические средства, обеспечивающие взаимодействие информационных систем участников информационного взаимодействия.

В базах данных АИС ФХД содержатся сведения о бухгалтерском учете, заработной плате и кадровом документообороте исполнительных органов государственной власти Архангельской области и иных государственных органов, подведомственных им учреждений и организаций, в том числе государственных учреждений Архангельской области, подключенных к АИС ФХД.

АИС ФХД является информационной системой, обрабатывающей персональные данные 3-го уровня защищенности.

2. ОРГАНИЗАЦИЯ ЗАЩИЩЕННОГО ВЗАИМОДЕЙСТВИЯ

2.1. Последовательность действий

Исполнительному органу государственной власти Архангельской области или иному государственному органу, подведомственному ему учреждению или организации, в том числе государственному учреждению Архангельской области, планирующему подключение к АИС ФХД необходимо:

2.1.1. Заключить соглашение об использовании АИС ФХД с оператором АИС ФХД по форме, представленной в приложении к ТУ.

2.1.2. Выбрать одну из типовых схем организации защищенного взаимодействия, описанных в пункте 2.2, и согласовать ее с оператором АИС ФХД.

2.1.3. Осуществить закупку СЗИ, совместимых с используемыми СЗИ в АИС ФХД, обеспечить их установку, настройку, разработку и утверждение необходимых организационно-распорядительных документов, а также аттестацию и подключение автоматизированной системы или автоматизированного рабочего места к АИС ФХД в соответствии с пунктами 2.3.-2.5., разделом 3.

2.2. Типовые схемы организации защищенного взаимодействия

Организация подключения пользователей к АИС ФХД должна соответствовать требованиям Федерального закона от 27 июля 2006 г. № 152-ФЗ "О персональных данных", Постановления Правительства Российской Федерации от 1 ноября 2012 г. № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных", приказа ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», приказа ФСБ России от 10 июля 2014 г. № 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 защищенности", а также 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 АИС ФХД при их передаче по сетям связи общего пользования должна быть обеспечена посредством организации защищенного взаимодействия между АИС ФХД и внешними автоматизированными системами или автоматизированными рабочими местами.

Для обеспечения безопасности информации до выполнения работ по подключению внешних АРМ или АС к АИС ФХД должна быть выбрана одна из следующих типовых схем защищенного взаимодействия:

2.2.1. Схема № 1 - взаимодействие одного или нескольких АРМ, оборудованных сертифицированными по требованиям безопасности информации ФСТЭК России и ФСБ России персональными средствами защиты информации (далее - СЗИ) и средствами криптографической защиты информации (далее - СКЗИ), а также наличие действующего аттестата соответствия требованиям по безопасности информации.

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

Структурная схема подключения автоматизированного рабочего места представлена на рисунке 1, автоматизированной системы - на рисунке 2.

В случае невозможности использования ни одной из типовых схем по согласованию с оператором АИС ФХД допускается реализация подключения по индивидуальной схеме.

До начала выполнения работ по подключению к АИС ФХД исполнительный орган государственной власти Архангельской области или иной государственный орган, подведомственное ему учреждение или организация, в том числе государственное учреждение Архангельской области, должны согласовать схему защищенного взаимодействия с оператором АИС ФХД.

2.3. Требования к реализации типовых схем защищенного взаимодействия

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

2.3.1.1. Для организации взаимодействия с АИС ФХД должно быть использовано одно или несколько специализированных АРМ,

оборудованных сертифицированными по требованиям безопасности информации ФСТЭК России и ФСБ России персональными СЗИ и СКЗИ.

2.3.1.2. Подключаемые АРМ должны иметь действующие аттестаты соответствия требованиям информационной безопасности, подтверждающие принятие мер, необходимых для обеспечения не ниже 3 уровня защищенности персональных данных.

2.3.1.3. В системе защиты ПДн подключаемого АРМ должны использоваться СЗИ и СКЗИ, совместимые со средствами применяемыми в АИС ФХД, в частности СКЗИ «ViPNet» версии 4.х, СЗИ "Dallas Lock" версии 8.х, средством антивирусной защиты " Kaspersky", в том числе для создания единого контура защиты АИС ФХД. СЗИ "Dallas Lock" и " Kaspersky" должны быть подключены к серверам безопасности.

2.3.1.4. Для организации защищенного канала связи с АИС ФХД должно быть использовано СКЗИ, сертифицированное по классу криптографической защиты не ниже КС2. Подключение АРМ к АИС ФХД должно быть реализовано только посредством данного СКЗИ. В случае регистрации СКЗИ в защищенной сети ViPNet отличной от сети № 1623, производится процедура установления межсетевого взаимодействия такой сети с сетью № 1623, администрирование которой осуществляет оператор АИС ФХД.

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

2.3.1.6. 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.

2.3.1.7. Схема подключения, сетевые настройки АРМ и дополнительные настройки установленных СЗИ и СКЗИ должны соответствовать требованиям ТУ и ЭД на АРМ, СЗИ и СКЗИ, в отдельном случае схема подключения согласовывается с оператором АИС ФХД.

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

2.3.2. Требования к реализации **схемы № 2** защищенного взаимодействия.

2.3.2.1. Подключаемая АС должна иметь действующий аттестат соответствия требованиям информационной безопасности, подтверждающий принятие мер, необходимых для обеспечения не ниже 3 уровня защищенности персональных данных.

2.3.2.2. В системе защиты ПДн подключаемой АС должны использоваться СЗИ и СКЗИ, совместимые со средствами применяемыми в АИС ФХД, в частности СКЗИ «ViPNet» версии 4.х, СЗИ "Dallas Lock" версии 8.х, антивирусным средством "Kaspersky", в том числе для создания единого контура защиты АИС ФХД. СЗИ "Dallas Lock" и " Kaspersky" должны быть подключены к серверам безопасности.

2.3.2.3. Для организации защищенного канала связи с АИС ФХД должно быть использовано СКЗИ, сертифицированное по классу криптографической защиты не ниже КС2. Подключение АС к АИС ФХД должно быть реализовано только посредством данного СКЗИ. В случае регистрации СКЗИ в защищенной сети ViPNet отличной от сети № 1623, производится процедура установления межсетевого взаимодействия такой сети с сетью № 1623, администрирование которой осуществляет оператор АИС ФХД.

2.3.2.4. Для обеспечения безопасного межсетевого взаимодействия в АС должно быть использовано средство межсетевого экранирования (МЭ), имеющее сертификат соответствия требованиям документа «Требования к межсетевым экранам» (ФСТЭК России, 2016), профили защиты межсетевых экранов типов А, Б или В не ниже шестого класса защиты.

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

2.3.2.6. Схема подключения СКЗИ и средств МЭ, а также необходимые для их корректного функционирования настройки должны быть выполнены в соответствии с требованиями ТУ и ЭД на АРМ, СЗИ и СКЗИ, либо предварительно согласованы с оператором АИС ФХД.

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

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

2.3.2.9 Доступ к АИС ФХД должен быть предоставлен только АРМ, участвующим в работе АИС ФХД.

2.4. Требования по информационной безопасности

2.4.1. В соответствии с Приказом ФСТЭК от 18 февраля 2013 г. № 21 на внешних объектах информатизации - автоматизированных рабочих местах, автоматизированных системах, необходимо обеспечить уровень

защищённости персональных данных не ниже 3, в том числе путем принятия организационных и технических мер защиты информации, в состав которых входят:

идентификация и аутентификация субъектов доступа и объектов доступа;

управление доступом субъектов доступа к объектам доступа;

защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные;

регистрация событий безопасности;

антивирусная защита;

контроль (анализ) защищенности персональных данных;

защита среды виртуализации (в случае использования технологии виртуализации);

защита технических средств;

защита информационной системы, ее средств, систем связи и передачи данных;

управление конфигурацией информационной системы и системы защиты персональных данных.

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

2.4.3. Меры по управлению доступом субъектов доступа к объектам доступа должны обеспечивать управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных на объекте информатизации правил разграничения доступа, а также обеспечивать контроль за соблюдением этих правил.

2.4.4. Меры по защите машинных носителей персональных данных (средств обработки (хранения) персональных данных, съемных машинных носителей персональных данных) должны исключать возможность несанкционированного доступа к машинным носителям и хранящимся на них персональным данным, а также несанкционированное использование съемных машинных носителей персональных данных.

2.4.5. Меры по регистрации событий безопасности должны обеспечивать сбор, запись, хранение и защиту информации о событиях

безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.

2.4.6. Меры по антивирусной защите должны обеспечивать обнаружение на объекте информатизации компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

2.4.7. Меры по контролю (анализу) защищенности персональных данных должны обеспечивать контроль уровня защищенности персональных данных, обрабатываемых в информационной системе, путем проведения систематических мероприятий по анализу защищенности объекта информатизации и тестированию работоспособности системы защиты персональных данных.

2.4.8. Меры по защите среды виртуализации должны исключать несанкционированный доступ к персональным данным, обрабатываемым в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры и (или) воздействие на них, в том числе к средствам управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системе хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам, а также системе резервного копирования и создаваемым ею копиям.

2.4.9. Меры по защите технических средств должны исключать несанкционированный доступ к стационарным техническим средствам, обрабатывающим персональные данные, средствам, обеспечивающим функционирование информационной системы (далее - средства обеспечения функционирования), и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий, а также защиту персональных данных, представленных в виде информативных электрических сигналов и физических полей.

2.4.10. Меры по защите объекта информатизации, ее средств, систем связи и передачи данных должны обеспечивать защиту персональных данных при взаимодействии объекта информатизации или его отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры

объекта информатизации и проектных решений, направленных на обеспечение безопасности персональных данных.

2.4.11. Меры по управлению конфигурацией объекта информатизации и системы защиты персональных данных должны обеспечивать управление изменениями конфигурации объекта информатизации и системы защиты персональных данных, анализ потенциального воздействия планируемых изменений на обеспечение безопасности персональных данных, а также документирование этих изменений.

2.4.12. К основным организационным мерам по информационной безопасности относятся:

реализация разрешительной системы допуска пользователей (обслуживающего персонала) к информационным ресурсам, автоматизированной системе, автоматизированным рабочим местам и связанным с ее использованием работам, документам;

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

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

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

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

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

проведение аттестационных испытаний информационных систем персональных данных по требованиям защиты информации (Аттестация выполняется организациями, имеющими лицензию ФСТЭК России на деятельность по технической защите конфиденциальной информации).

2.4.13. К основным техническим мерам по информационной безопасности относятся:

каналы связи, выходящие за пределы контролируемых зон, должны быть защищены с помощью СКЗИ;

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

доступ к АИС ФХД через сети общего пользования, включая сеть международного информационного обмена Интернет, должен производится с использованием защищенных каналов связи (программные и/или программно-аппаратные продукты линейки ViPNet с действующими сертификатами соответствия ФСБ России);

на серверном оборудовании и автоматизированных рабочих местах должны использоваться сертифицированные средства защиты от несанкционированного доступа (программные продукты линейки Dallas Lock версии 8.0-k и выше с действующими сертификатами соответствия ФСТЭК России);

на серверном оборудовании и автоматизированных рабочих местах должны использоваться сертифицированные средства антивирусной защиты (программные продукты линейки Kaspersky Endpoint Security с действующими сертификатами соответствия ФСТЭК России);

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

2.4.14. 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.

2.5. Требования к техническому и программному обеспечению автоматизированных рабочих мест пользователей

Автоматизированное рабочее место Участника должно соответствовать следующим требованиям.

2.5.1. Требования к аппаратному обеспечению:

– x86-совместимый процессор с количеством ядер 2 и более;

– объем оперативной памяти – не менее 4 Гбайт (рекомендуется 8 Гбайт);

– свободное место на жестком диске – не менее 500 Мбайт (рекомендуется 1 Гбайт);

– сетевой интерфейс или модем;

– пропускная способность канала связи для взаимодействия с серверной частью из расчета на одно автоматизированное рабочее место (далее – АРМ) не менее 1 (рекомендуется 2) Mbit/сек;

2.5.2. Требования к программному обеспечению:

– 32/64-разрядная операционная система;

– операционная система Windows 10 или операционная система из реестра Российского программного обеспечения (reestr.minsvyaz.ru/reestr/):

Astra Linux Special Edition,

Astra Linux Common Edition,

Альт Рабочая станция,

РЕД ОС.

2.6. 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:

одно рабочее место: минимальная (рекомендуемая) скорость передачи данных - 1 (2) Мбит/с;

от 2 до 5 ПК: минимальная (рекомендуемая) скорость передачи данных - 2 (4) Мбит/с;

от 6 до 10 ПК: минимальная (рекомендуемая) скорость передачи данных - 4 (8) Мбит/с;

2.6.2. между локально-вычислительной сетью Участника информационного взаимодействия и сетью общего пользования должны быть установлены криптошифровальные устройства с функцией межсетевого экрана, к которым предъявляются следующие требования:

- должны быть из линейки ViPNet (обусловлено тем, что АИС ФХД размещена в защищенной сети, построенной по технологии ViPNet) и иметь действующие сертификаты соответствия ФСБ России и ФСТЭК России.

2.6.3. В зависимости от масштабов подключаемой сети Участника информационного взаимодействия выбираются соответствующие пограничные криптошлюзы ViPNet Coordinator или программные средства ViPNet Client.

2.6.4. При необходимости удаленного подключения к АРМ пользователей применяется программное обеспечнеие удаленного мониторинга и управления, внесенного в Единый реестр российских программ для электронных вычислительных машин и баз данных (https://reestr.digital.gov.ru/reestr).

3. ПРАВИЛА ПРИЕМКИ

3.1 Общие положения

Для осуществления приемки подключения внешних АРМ или АС к АИС ФХД 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 внешних АРМ или АС к АИС ФХД. Данные испытания должны быть проведены ответственными исполнителями со стороны подключаемых АРМ или АС 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 ФХД с аттестованными АРМ или АС должны быть выполнены следующие проверки:

3.2.1.1. проверка наличия у подключаемых АРМ или АС 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 подключаемых АРМ или АС и АИС ФХД.

Результаты проведенных проверок должны быть зафиксированы в отдельном протоколе испытаний, составляемом ответственными исполнителями со стороны подключаемых АРМ или АС.

3.3 Периодические испытания

Данные испытания предназначены для периодического контроля заданных при подключении внешних АРМ или АС к АИС ФХД показателей.

Результаты проведенных проверок должны быть зафиксированы в отдельном протоколе периодических испытаний, составляемом ответственными исполнителями со стороны подключаемых АРМ или АС.

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

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

Протоколы приёмочных испытаний и протоколы периодических испытаний, подписанные ответственными за проведение данных испытаний лицами, должны быть предоставлены для проверки оператору АИС ФХД в течение 5 рабочих дней по факту получения соответствующего запроса от оператора АИС ФХД.

В случае выявления нарушений требований настоящих ТУ, оператор АИС ФХД немедленно производит отключение соответствующих внешних АРМ или АС от АИС ФХД.

5. ОПРЕДЕЛЕНИЯ, ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АС	-	Автоматизированная информационная система
АРМ	-	Автоматизированное рабочее место
АИС ФХД	-	Автоматизированная информационная система управления финансово-хозяйственной деятельностью органов государственной власти, иных государственных органов и государственных учреждений Архангельской области
ИСПДн	-	Информационная система персональных данных
ИФНС	-	Инспекция федеральной налоговой службы
МЭ	-	Межсетевое экранирование
ПАК	-	Программно-аппаратный комплекс
ПДн	-	Персональные данные
ПФР	-	Пенсионный фонд Российской Федерации
РД	-	Руководящий документ
СЗИ	-	Средство защиты информации
СКЗИ	-	Средство криптографической защиты информации
ТУ	-	Технические условия
УФЭБС	-	Унифицированные форматы электронных банковских сообщений
ФСБ России	-	Федеральная служба безопасности
ФСГС	-	Федеральная служба государственной статистики
ФСС	-	Фонд социального страхования Российской Федерации
ФСТЭК России	-	Федеральная служба по техническому и экспортному контролю
ЭД	-	Эксплуатационная документация
VPN	-	Виртуальная частная (защищенная) сеть

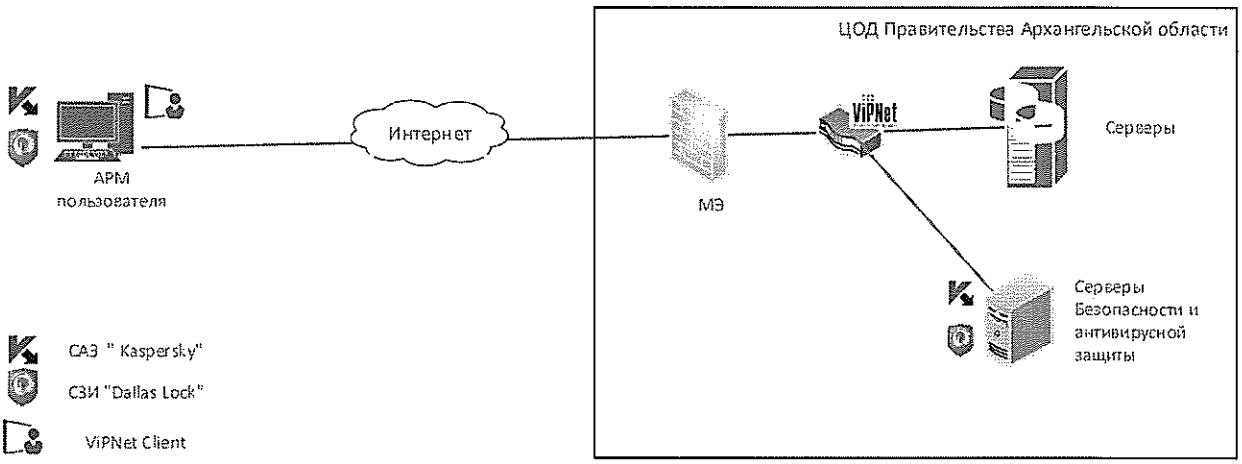

Рисунок 1. Схема подключение одного или нескольких АРМ.

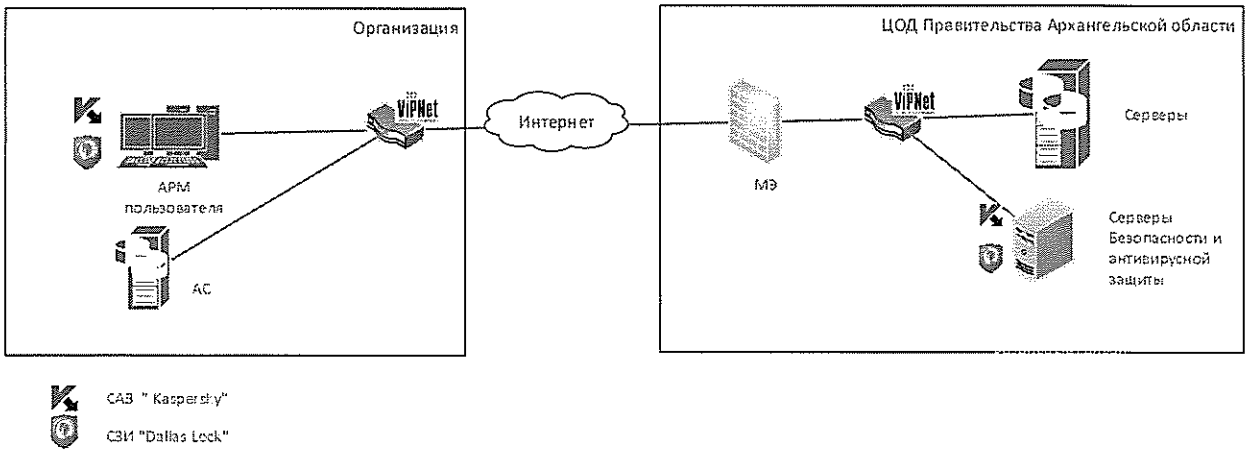

Рисунок 2. Схема подключения АС и АРМ с использованием координатора.