УТВЕРЖДАЮ

Исполняющий обязанности директора КОГБУ «Центр стратегического развития информационных ресурсов и систем управления»

_____/Д.В. Охапкин

«30» июня 2017 г.

КОГБУ «Центр стратегического развития информационных ресурсов и систем управления»

Регламент защищённой сети региональной системы межведомственного электронного взаимодействия Кировской области

Содержание

1. Введение

1.1. Обзорная информация

Настоящий Регламент определяет механизмы и условия использования подсистемы информационного обмена в защищённой сети региональной системы межведомственного электронного взаимодействия Кировской области и предоставления доступа к ней, включая обязанности Участников РСМЭВ и Оператора РСМЭВ, протоколы работы, принятые форматы данных, основные организационно-технические мероприятия, необходимые для безопасной работы ПСИОЗС РСМЭВ.

1.2. Идентификация Регламента

Наименование документа: «Регламент защищённой сети региональной системы межведомственного электронного взаимодействия Кировской области».

Версия: 4.1.

Дата: ___.___.2017

Объектный идентификатор: 98477432.425520.001-3.2-И.

1.3. Публикация Регламента

Настоящий Регламент распространяется:

В электронной форме:

из репозитария Оператора РСМЭВ по адресу http://10.0.112.30 ;

(URL с указанием протокола)

через E-mail от отправителя VasilevichiIV@csr43.ru ;

(адрес электронной почты отправителя)

В бумажной форме:

через 61000, г. Киров, ул. Карла Маркса, д. 54 (почтовый адрес Оператора РСМЭВ)

Копии Регламента, предназначенные для распространения в электронной форме из репозитория Оператора РСМЭВ, распространяются в виде двух файлов, один из которых содержит электронный образ Регламента в формате pdf, а другой - электронную цифровую подпись уполномоченного лица Оператора РСМЭВ к файлу электронного образа Регламента.

Копии Регламента, предназначенные для распространения в электронной форме через E-mail, распространяются виде двух файлов, один из которых содержит электронный образ Регламента в формате pdf, а другой - электронную цифровую подпись уполномоченного лица Оператора РСМЭВ к файлу электронного образа Регламента. Область применения Регламента

Настоящий Регламент предназначен служить соглашением, налагающим обязательства по всем вовлеченным сторонам, а также средством официального уведомления и информирования всех сторон о взаимоотношениях, возникающих в процессе предоставления и использования подсистемы информационного обмена в защищённой сети региональной системы межведомственного электронного взаимодействия Кировской области.

Настоящий Регламент устанавливает общие принципы защищённого электронного взаимодействия между КОГБУ "Центр стратегического развития информационных ресурсов и систем управления", исполнительными органами государственной власти Кировской области, органами местного самоуправления, государственными и муниципальными учреждениями, многофункциональными центрами, иными органами и организациями, участвующими в предоставлении государственных и муниципальных услуг и исполнении государственных и муниципальных функций в электронной форме.

1.4. Срок действия Регламента

Настоящий Регламент вступает в силу со дня его публикации.

Срок действия Регламента - 6 лет.

Если Оператор РСМЭВ официально не уведомит Участников РСМЭВ о прекращении действия Регламента, Регламент автоматически пролонгируется на следующие 6 лет.

Официальное уведомление о прекращении действия Регламента осуществляется способами, определенными в разделе 1.3 данного Регламента.

1.5. Порядок внесения изменений в Регламент

Изменения в настоящий Регламент вносятся по инициативе Оператора РСМЭВ. Оператор вправе в одностороннем порядке вносить изменения в Регламент.

При внесении изменений в настоящий Регламент Оператор РСМЭВ обязан довести характер изменений, новую версию Регламента до Участников РСМЭВ.

Уведомление о планируемой дате ввода в действие новой версии Регламента осуществляется способами, определенными в разделе 1.3 данного Регламента, а также путем размещения информационного сообщения на официальном сайте Оператора РСМЭВ в защищенной сети РСМЭВ http://10.0.112.30 .

В процессе ввода в действие изменений настоящего Регламента информационный обмен осуществляется в соответствии с предыдущей версией Регламента. Мероприятия по реализации изменений не могут быть основанием потери или отсрочки обработки электронных сообщений в соответствии с предыдущей версией Регламента. После ввода в эксплуатацию измененной версии данного Регламента обмен электронными сообщениями в соответствии с предыдущей версией данного Регламента прекращается.

1.6. Контактная информация

Кировское областное государственное бюджетное учреждение “Центр стратегического развития информационных ресурсов и систем управления”

Почтовый адрес: 61000, г. Киров, ул. Карла Маркса, д. 54

E-mail: csr@csr43.ru

Телефон/факс: 27-97-00/ 27-97-05

Контактные телефоны Службы поддержки 27-97-19, 27-97-30, 27-97-18

E-mail Службы поддержки VasilevichIV@csr43.ru

GanichevAV@csr43.ru

LebedevaOV@csr43.ru

2. Общие положения

Регламент защищённой сети региональной системы межведомственного электронного взаимодействия Кировской области разработан в соответствии с требованиями Федерального закона от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных», Федерального закона от 06.04.2011 №63-ФЗ «Об электронной подписи», Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, утвержденной приказом Федерального агентства правительственной связи и информации при Президенте Российской Федерации (ФАПСИ) от 13.06.2001 №152, Типовых требований по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных, утверждёнными руководством 8 Центра ФСБ России 21.02.2008 № 149/6/6-622, Приказа от 27.12.2010г. №190 Министерства связи и массовых телекоммуникаций Российской Федерации “ Об утверждении технических требований к взаимодействию информационных систем в единой системе межведомственного электронного взаимодействия” и других нормативных правовых актов Российской Федерации в области защиты информации.

3. Перечень сокращений

Перечень используемых сокращений в настоящем документе приведён в таблице №1.

Таблица №1 – Перечень сокращений

№ п/п	Сокращение	Расшифровка
1	АРМ	- автоматизированное рабочее место
2	ЗЭВ	- защищённое электронное взаимодействие
3	ОС	- операционная система
4	ПО	- программное обеспечение
5	РД	- руководящий документ
6	РСМЭВ	- региональная система межведомственного электронного взаимодействия Кировской области
7	ЭС	- электронное сообщение
8	СЗИ	- средство защиты информации
9	СКЗИ	- средство криптографической защиты информации
10	ФСБ	- Федеральная служба безопасности
11	ФСТЭК	- Федеральная служба по техническому и экспортному контролю
12	ПСИОЗС РСМЭВ	- подсистема информационного обмена защищенной сети региональной системы межведомственного электронного взаимодействия Кировской области
13	ЗСРСМЭВ	- защищенная сеть региональной системы межведомственного электронного взаимодействия Кировской области

4. Термины и определения

Регламент - Регламент защищённой сети региональной системы межведомственного электронного взаимодействия Кировской области.

Оператор РСМЭВ - КОГБУ "Центр стратегического развития информационных ресурсов и систем управления", на которое возложены функции управления инфраструктурой РСМЭВ.

Участник РСМЭВ - исполнительные органы государственной власти Кировской области, органы местного самоуправления Кировской области, государственные и муниципальные учреждения Кировской области, многофункциональные центры, иные органы и организации, участвующие в предоставлении государственных и муниципальных услуг и исполнении государственных и муниципальных функций в электронной форме.

Защищённая сеть РСМЭВ – программно-технический комплекс, реализующий, защищённую с помощью СКЗИ, инфраструктуру сети передачи данных РСМЭВ.

Автоматизированное рабочее место – программно-технический комплекс, предназначенный для автоматизации определенного вида деятельности.

Администратор Участника – сотрудник Участника, отвечающий за эксплуатацию средств криптографической защиты информации на стороне Участника, необходимых для защищенного информационного обмена в региональной системе межведомственного электронного взаимодействия Кировской области.

Администратор Оператора РСМЭВ – сотрудник отдела информационного обеспечения Оператора РСМЭВ, назначенный приказом директора ответственным за эксплуатацию средств криптографической защиты информации на стороне Оператора РСМЭВ, необходимых для защищенного информационного обмена в региональной системе межведомственного электронного взаимодействия Кировской области.

Ключевая информация – специальным образом организованная совокупность данных, предназначенная для осуществления криптографической защиты информации и позволяющая организовать защищенный информационный обмен в региональной системе межведомственного электронного взаимодействия Кировской области.

Носитель ключевой информации – материальный носитель, содержащий закрытые ключи электронной цифровой подписи или ключи шифрования, или набор персональных ключей.

Пользователь Участника – сотрудник Участника, уполномоченный использовать средства шифрования при работе с ПСИОЗС РСМЭВ.

Средства криптографической защиты информации – программно-аппаратные средства, осуществляющее криптографическое преобразование информации для обеспечения ее безопасности.

Подсистема информационного обмена защищенной сети региональной системы межведомственного электронного взаимодействия Кировской области – совокупность программных и технических средств, а также организационных мер, обеспечивающих функционирование процесса защищённого с помощью СКЗИ информационного обмена между Участниками РСМЭВ.

Электронное сообщение (ЭС) – любая информация, представленная в электронно-цифровой форме и передаваемая по защищённым каналам связи РСМЭВ.

5. Организация информационного обмена

Оператор РСМЭВ и Участники РСМЭВ осуществляют обмен ЭС, содержащими информацию ограниченного доступа, в рамках ПСИОЗС РСМЭВ по телекоммуникационным каналам связи.

Обмен ЭС и их шифрование, подтверждение целостности и подлинности документа осуществляется в соответствии Приказом от 27.12.2010г. №190 Министерства связи и массовых телекоммуникаций Российской Федерации “Об утверждении технических требований к взаимодействию информационных систем в единой системе межведомственного электронного взаимодействия”, руководствами пользователей на технические средства и средства защиты, обеспечивающие обмен, и документацией на СКЗИ.

Участники РСМЭВ и Оператор РСМЭВ должны обеспечить защиту от несанкционированного доступа к ЭС и непреднамеренного уничтожения и/или искажения ЭС.

При работе с информацией ограниченного доступа в рамках ПСИОЗС РСМЭВ Оператор РСМЭВ и Участники РСМЭВ руководствуются нормативными правовыми актами Российской Федерации в области защиты информации, настоящим Регламентом, а также методическими рекомендациями, письмами и указаниями Оператора РСМЭВ.

5.1. Порядок подключения к защищенной сети

Для подключения к защищенной сети передачи данных РСМЭВ Участнику РСМЭВ необходимо:

1) заключить Соглашение о присоединении Участника РСМЭВ к защищённой сети региональной системы межведомственного электронного взаимодействия Кировской области по форме согласно Приложению №1 к настоящему Регламенту (далее - Соглашение);

2) выбрать схему подключения рабочих мест к защищенной сети;

3) выполнить требования информационной безопасности;

4) предоставить документы Оператору РСМЭВ для подключения в соответствии с пунктом 7 настоящего Регламента;

5) получить от Оператора РСМЭВ ключевую информацию, а также информацию, необходимую для инициализации подключения;

6) инициализировать и ввести в эксплуатацию СКЗИ, проверить подключение к РСМЭВ.

Схемы подключения к РСМЭВ, их описание, технические особенности и порядок выбора представлены в Приложении №2. Выбор схемы подключения зависит от следующих условий:

– количество подключаемых рабочих мест;

– имеющиеся финансовые ресурсы;

– наличие технических возможностей подключения, в том числе доступа в Интернет;

– возможность выполнения требований по безопасности в соответствии с пунктом 6 настоявшего Регламента.

6. Требования к обеспечению безопасности в информационной системе Участника РСМЭВ

Средства криптографической защиты информации и помещения, в которых они установлены, Участника РСМЭВ, используемые для подключения к ЗСРМСЭВ, должны удовлетворять техническим условиям подключения, приведённых в Приложении №3.

Участник, заключивший Соглашение, подготавливает помещение, в котором будут функционировать СКЗИ, и несет ответственность за соответствие этих помещений требованиям по размещению, охране и режиму. Участник РСМЭВ обеспечивает установку и настройку программно-технических средств защиты информации, и настройку СКЗИ в соответствии с эксплуатационной документацией. Полный перечень мероприятий, выполнение которых обеспечивает защищенность информации при подключении Участника РСМЭВ к защищенной сети, приведен в Протоколе оценки соответствия требованиям информационной безопасности для выбранной схемы подключения: Приложение №4 (для схемы 1), Приложение №5 (для схемы 2), Приложение №6 (для схемы 3), Приложение №7 (для схемы 4) и Приложение №8 (для схемы 5).

В случае невозможности выполнить указанные мероприятия Участник РСМЭВ может привлечь стороннюю организацию, имеющие лицензии ФСТЭК России на деятельность по технической защите информации и лицензию ФСБ России, разрешающую деятельность по техническому обслуживанию шифровальных (криптографических) средств.

7. Регистрация Участника РСМЭВ в подсистеме информационного обмена защищенной сети региональной системы межведомственного электронного взаимодействия Кировской области

Регистрация Участников РСМЭВ осуществляется в ПСИОЗС РСМЭВ после заключения Соглашения между Оператором РСМЭВ и Участником РСМЭВ и подачи заявки.

7.1. Оформление заявки и подтверждение готовности к подключению к ЗСРСМЭВ

Подтверждение готовности Соискателя подключения является основанием для его подключения к защищенной сети РСМЭВ, в том числе проведения первичной инициализации средств шифрования.

Для подтверждения готовности Участник РСМЭВ направляет Оператору РСМЭВ следующий пакет документов, указанный в Таблице 2.

Таблица 2 – Пакет документов

№ п/п	Наименование документа	Цель документа	Оформление документа
1	Соглашение о присоединении Участника РСМЭВ к защищённой сети региональной системы межведомственного электронного взаимодействия Кировской области	Заявить о согласии Участника РСМЭВ выполнять условия настоящего регламента и нести ответственность	Документ оформляется по форме, представленной в Приложении №1, и подписывается руководителем Участника РСМЭВ

№ п/п	Наименование документа	Цель документа	Оформление документа
2	Заявка на подключение	Заявить о готовности Участника РСМЭВ к подключению	Документ оформляется по форме, представленной в Приложении №9, и подписывается руководителем Участника РСМЭВ
2	Анкета	Предоставляет основные организационные сведения о Участнике РСМЭВ	Документ оформляется по форме, представленной по форме №10
3	Копия приказа о назначении лица, ответственного за осуществление защищенного взаимодействия с РСМЭВ	Предоставить свидетельство назначения сотрудника, ответственного за осуществление взаимодействия с РСМЭВ, с указанием его ФИО, должности, обязанностей и ответственности	Копия заверяется подписью руководителя и печатью Участника РСМЭВ
4	Сведения, необходимые для регистрации	Предоставить сведения о СЗИ, универсальных АРМ и их пользователях	Сведения в виде копий документов и справки в

№ п/п	Наименование документа	Цель документа	Оформление документа
	Участников РСМЭВ в защищенной сети	для регистрации, и идентификации в защищенной сети РСМЭВ	соответствии с Приложением №11
5	Протокол оценки соответствия требованиям безопасности	Подтвердить соответствие выполненных условий Участником РСМЭВ требованиям информационной безопасности для выбранной схемы подключения	Документы выполняется по форме, представленной в Приложении №4, Приложении №5, Приложении №6, Приложении №7, Приложении №8

Протокол оценки соответствия заполняют и подписывают ответственные за свой участок сотрудники.

Если организация привлекает для выполнения мероприятий стороннюю организацию, то Протокол в графе, соответствующей выполняемым мероприятиям, подписывается представителем этой организации.

Все указанные документы утверждаются и подписываются руководителем организации.

Весь пакет документов о готовности Участника РСМЭВ изготавливается в двух экземплярах. Один хранится у Участника РСМЭВ подключения в Деле по учету документации по взаимодействию с РСМЭВ. Другой экземпляр подшивается и ведется Оператором РСМЭВ в деле Участника.

Ответственность за достоверность сведений, представленных в Протоколе, несет руководитель организации-Участника РСМЭВ.

После предоставления Участников РСМЭВ документов, указанных в Таблице 2, Оператора РСМЭВ проводит экспертизу представленной документации и выносит решение о возможности или невозможности подключения:

в случае принятия положительного решения в течение трех рабочих дней производит регистрацию Участника, генерирует дистрибутив ключей шифрования для сетевого узла ЗСРСМЭВ, записывает сформированный дистрибутив на предоставленный носитель ключевой информации, после чего уведомляет Участника о готовности дистрибутива ключей сетевого узла ЗСРСМЭВ по телефону, указанному в Акте готовности.

в случае отказа в регистрации уведомляет об этом Участника с указанием причины отказа и выявленных нарушениях. Участник РСМЭВ должен устранить несоответствия и после этого подать повторное заявление на подключение к РСМЭВ.

Администратор Оператора РСМЭВ проводит инструктаж лица ответственного за информационную безопасность Участника РСМЭВ правилам эксплуатации СКЗИ в рамках ЗСРСМЭВ. Пользователи Участника РСМЭВ допускаются к самостоятельной работе с СКЗИ после прохождения инструктажа, проводимого лицом ответственным за информационную безопасность, на местах.

7.2. Порядок получения носителей ключевой информации

В случае принятия Оператором РСМЭВ положительного решения о подключении Участника к РСМЭВ, последнему предоставляется ключевая информация, а также информация, необходимая для инициализации СКЗИ.

В случае личного присутствия Ответственного Пользователя Участника РСМЭВ выдается носитель ключевой информации с дистрибутивом ключей для сетевого узла ЗСРСМЭВ (далее – носитель ключевой информации). Пользователь Участника РСМЭВ подписывает Акт

приема-передачи инициализирующей информации СКЗИ (форма Акта приведена в Приложении №12).

В случае, если Участник РСМЭВ направляет доверенное лицо (форма доверенности приведена в Приложении №13) для получения инициализирующей ключевой информации, представитель Пользователя Участника РСМЭВ предоставляет доверенность Администратору Оператора РСМЭВ. Администратор Оператора РСМЭВ выдает носитель ключевой информации в запечатанном конверте и два экземпляра Акта приема-передачи инициализирующей информации СКЗИ. Ответственный пользователь Участника при получении конверта с носителям ключевой информации и сертификатом сетевого узла, проверяет целостность конверта, вскрывает его, после чего собственноручно расписывается в обоих экземплярах акта приема-передачи инициализирующей ключевой информации СКЗИ, и один экземпляр оправляет на адрес Оператора РСМЭВ любым доступным способом (лично, курьер, заказное письмо).

Акт приема-передач и ключевой и инициализирующей информации является официальным документом, разрешающим подключение Участника РСМЭВ к защищенной сети. По подписании Акта приема/передачи Участник РСМЭВ авторизуется защищенной сети РСМЭВ и в дальнейшем несет ответственность за безопасность своего подключения.

8. Порядок работы с ключевой информацией

8.1. Общие положения

Срок действия ключей администратора сетевого узла составляет 1 (один) год.

В качестве носителей ключевой информации используются материальные носители.

Носители ключевой информации относятся к материальным носителям, содержащим информацию ограниченного доступа. При обращении с ними должны выполняться требования нормативных правовых документов, регламентирующих порядок обращения с информацией ограниченного доступа.

Учет носителей ключевой информации осуществляется Администратором Оператора РСМЭВ.

Ответственные пользователи Участника РСМЭВ, имеющие доступ к носителям ключевой информации, несут персональную ответственность за безопасность ключевой информации на них и обязаны обеспечивать её сохранность, неразглашение и нераспространение.

Не позднее, чем через 3 (три) дня с момента прекращения срока действия ключа администратора сетевого узла, он должен быть уничтожен, о чём составляется акт уничтожения ключевой информации.

8.2. Требования по организации хранения и использования носителей ключевой информации

Порядок хранения и использования носителей ключевой информации с ключами сетевого узла должен исключать возможность несанкционированного доступа к ним.

Во время работы с носителями ключевой информации доступ к ним посторонних лиц должен быть исключен.

Категорически запрещается производить несанкционированное копирование носителей ключевой информации, знакомить или передавать носители ключевой информации лицам, к ним не допущенным, выводить закрытые ключи на дисплей или принтер, устанавливать носитель ключевой информации в считывающее устройство других компьютеров, оставлять носитель ключевой информации без присмотра на рабочем месте, записывать на носитель ключевой информации посторонние файлы.

9. Проверка и ввод подключения к защищенной сети РСМЭВ в эксплуатацию

Участник информационного взаимодействия РСМЭВ осуществляет первичную инициализацию СКЗИ и ввод в эксплуатацию подключения к защищенной сети РСМЭВ.

Факт проверки подключения к защищенной сети оформляется Протоколом проверки СКЗИ (Приложение №14), который подписывается ответственным за СКЗИ сотрудником, или комиссией, проводившей проверку.

При положительном результате проверки оформляется Акт о вводе в эксплуатацию СКЗИ (Приложение №15). Акт подписывается сотрудниками, осуществившими ввод СКЗИ в эксплуатацию. В случае привлечения сторонней организации-Лицензиата Акт о вводе в эксплуатацию также подписывается представителем этой организации.

При отрицательном результате проверки Участник своими силами или при помощи технической поддержки Оператора РСМЭВ определяет причину невозможности подключения.

При невозможности устранить причину Участником выполняется процедура отключения от защищенной сети (п.12).

10. Порядок осуществления контроля защищенности

Для поддержания уровня защищенности сети передачи данных РСМЭВ Участники информационного взаимодействия осуществляют периодический контроль соответствия реализуемых мероприятий требованиям информационной безопасности.

Периодичность проведения контроля устанавливается не реже 1 раза в год.

Процедура контроля инициируется Оператором РСМЭВ в форме письма, содержащего требование выполнить контроль в установленные сроки. По умолчанию, если не указано в письме, срок для осуществления контроля составляет 14 календарных дней с момента получения письма.

При осуществлении контроля Участник информационного взаимодействия должен выполнить шаги:

– оценить соответствие реализуемых мероприятий требованиям действующего Регламента защищенной сети;

– провести корректирующие действия по результатам оценки;

– сообщить о результатах контроля Оператору РСМЭВ, предоставив справку о проведенном контроле и отчетную документацию;

– актуализировать параметры подключения совместно с Оператором РСМЭВ.

Участник оценивает состав и содержание реализуемых мероприятий, руководствуясь Протоколом проверки соответствия требованиям информационной безопасности и Методическими рекомендациями.

По результатам проведенной оценки Участник, если необходимо, выполняет мероприятия по устранению выявленных несоответствий и повторяет процедуру контроля.

По результатам контроля Участник предоставляет Оператору РСМЭВ пакет отчетной документации. Цель предоставления отчетной документации

— подтверждение соответствия и актуализация сведений об Участнике РСМЭВ и выполняемых им мероприятиях.

Перечень предоставляемых документов аналогичен документам, предоставляемым при подключении (п.7.1), за исключением Заявки.

Вместо Заявки Участником информационного взаимодействия подается Справка о проведении контроля, оформляемая по форме, представленной в Приложении №16. Справка подписывается руководителем Участника информационного взаимодействия.

Порядок подачи и оформления документов аналогичен п.7.1. Сведения, не претерпевшие изменений, могут не предоставляться, о чем указывается в тексте справки.

По предоставлении Участником справки о проведении контроля и отчетной документации Оператор РСМЭВ:

– актуализирует дело Участника;

– проводит экспертизу документации Участника;

– выполняет изменения параметров и состава подключения Участника;

– добавляет абонентские пункты по процедуре в соответствии с п.7.1.;

– удаляет абонентские пункты из защищенной сети.

В случае, если Участник не предоставил справку и отчетную документацию в установленный срок, Оператор уведомляет его повторно с требованием предоставить справку и отчетную документацию в срок 7 календарных дней.

В случае не предоставления справки и отчетной документации Участником после повторного запроса Оператор выполняет отключение Участника (п.12) от защищенной сети РСМЭВ до урегулирования данной ситуации.

11. Порядок взаимодействия сторон

11.1. Замена ключей шифрования сетевого узла ЗСРСМЭВ

В ЗСРСМЭВ производятся следующие замены используемой ключевой информации:

- плановая смена ключей;
- внеплановая смена ключей по инициативе Участника;
- внеплановая смена при компрометации.

Плановая замена ключей в ЗСРСМЭВ производится периодически, не реже одного раза в год. Формирование ключей сетевого узла при плановой смене ключей осуществляется по инициативе Оператора РСМЭВ.

Замена ключей по инициативе Участника РСМЭВ возможна в любой момент. Данная замена обязательна при смене ответственного пользователя узла передачи данных Участника РСМЭВ, при выходе из строя носителя ключевой информации.

При компрометации ключей узла передачи данных Участник РСМЭВ незамедлительно прекращает его использование и сообщает о факте компрометации Администратор Оператора РСМЭВ.

Формирование дистрибутивов ключей при внеплановой смене ключей осуществляется на основании предоставленной в письменной форме заявления на внеплановую смену к настоящему Регламенту и копии приказа о назначении Ответственного пользователя и Пользователя Участника РСМЭВ, ранее выданные ключи шифрования должны быть уничтожены. По факту уничтожения составляется акт по форме приведённой в Приложении 17. Акт составляется в 2-х экземплярах один передаётся Оператору РСМЭВ.

Отзыв ключей сетевого узла без дальнейшего формирования ключей сетевого узла осуществляется при расторжении Соглашения.

11.2. Порядок решения инцидентов информационной безопасности

Инцидентом информационной безопасности считается нежелательное событие информационной безопасности, которое привело к нарушению конфиденциальности, целостности или доступности информации, обрабатываемой в РСМЭВ.

При обнаружении инцидента информационной безопасности сотрудник, ответственный за осуществление защищенного взаимодействия с РСМЭВ, проводит мероприятия по изоляции ситуации, в которой возник инцидент, и незамедлительно информирует Оператора РСМЭВ с указанием объема, сроков и причины нарушения безопасности информации, а также информацию об устройствах сети, задействованных в инциденте.

Изоляция ситуации означает ограничение доступа в помещения, к скомпрометированным АРМ, абонентским пунктам со стороны Оператора, периферийным устройствам, средствам защиты информации, идентификаторам, сетевым устройствам, крипто-маршрутизаторам, а также сохранение устройств в рабочем состоянии — все необходимые действия по обеспечению объективного расследования.

Под руководством Оператора РСМЭВ создается комиссия, которая совместно с Участником проводит расследование обстоятельств инцидента и оценивает последствия инцидента.

Комиссия вырабатывает мероприятия по устранению последствий инцидента (коррекция), а также по недопущению таких инцидентов в будущем (корректирующее действие).

Участник обязан выполнить указанные комиссией мероприятия и пройти внеплановый контроль в соответствии с п.10.

11.3. Порядок разрешения конфликтных ситуаций и споров

Конфликтные ситуации и споры разрешаются Оператором РСМЭВ и Участниками РСМЭВ в рабочем порядке путем переговоров или по итогам работы комиссии по разрешению конфликтной ситуации (далее - Комиссия).

В случае, если конфликтная ситуация не была разрешена в рабочем порядке, инициатор должен в течение трёх рабочих дней после возникшей конфликтной ситуации направить предложение о создании Комиссии. Предложение о создании Комиссии должно содержать информацию о предполагаемом месте, дате и времени сбора Комиссии, список предлагаемых представителей инициатора с указанием фамилий, имён, отчеств, должностей, их контактной информации. Предложение составляется на бумажном носителе, подписывается руководителем инициатора и передаётся другому участнику разрешения конфликтной ситуации в установленном порядке, обеспечивающем подтверждение вручения корреспонденции.

Не позднее, чем на третий рабочий день после получения предложения о создании комиссии должна быть сформирована Комиссия. Комиссия формируется на основании совместного приказа Оператора РСМЭВ и Участника РСМЭВ, в котором устанавливаются состав Комиссии, время и место её работы.

Комиссия в двухнедельный срок проводит разбор конфликтной ситуации и по итогам работы составляет акт, в котором в обязательном порядке указываются суть конфликта, виновная сторона и сроки устранения причин возникновения конфликтной ситуации.

В случае невозможности разрешения конфликтной ситуации в рабочем порядке и по итогам работы Комиссии конфликтная ситуация разрешается в судебном порядке в соответствии с законодательством Российской Федерации.

12. Порядок отключения от защищенной сети

Отключение Участника РСМЭВ в целом или отдельных АРМ Участника РСМЭВ может потребоваться в ситуациях:

- предоставление Участником сведений об изменениях;
- прекращение или приостановление деятельности Участника;
- наступление инцидента информационной безопасности;
- другие ситуации.

Для проведения отключения в штатной ситуации Участник подает Оператору РСМЭВ Запрос об отключении АРМ с указанием идентификационных данных АРМ или сети, данных пользователей (при необходимости) и причины отключения.

Оператор РСМЭВ рассматривает Запрос Участника и выполняет все необходимые меры по его отключению от защищенной сети.

Повторное подключение АРМ выполняется согласно п.5.1.

Приложение №1. Типовая форма соглашения

Соглашение № _____

о присоединении Участника РСМЭВ

к защищённой сети региональной системы межведомственного электронного взаимодействия Кировской области

г. Киров «____» _____ 20__ г.

Кировское областное государственное бюджетное учреждение "Центр стратегического развития информационных ресурсов и систем управления", в лице директора _____ действующего на основании Устава, именуемый в дальнейшем «Оператор», с одной стороны и _____

(наименование юридического лица)

в лице _____,
действующего на основании _____, именуемый в дальнейшем «Участник», с другой стороны, а вместе именуемые «Стороны», заключили настоящее Соглашение о нижеследующем:

1. ПРЕДМЕТ СОГЛАШЕНИЯ

1.2 Участник и Оператор осуществляют информационный обмен электронными сообщениями в рамках защищённой сети региональной системы межведомственного электронного взаимодействия Кировской области (далее - ЗСРСМЭВ).

1.2. Стороны признают, что полученные ими электронные сообщения, заверенные электронной подписью уполномоченных представителей, юридически эквивалентны полученным документам на бумажных носителях, заверенных соответствующими подписями и оттиском печатей сторон на основании Федерального закона от 06 апреля 2011 года № 63-ФЗ «Об

электронной подписи» и соответствующих доверенностей на право подписание документов, выданных уполномоченным представителям.

1.3. Стороны признают, что использование в ЗСРСМЭВ средств защиты информации, которые реализуют сетевую защиту, шифрование и электронную подпись, достаточно для обеспечения конфиденциальности информационного взаимодействия Сторон, а также для подтверждения того, что:

- электронное сообщение исходит от Стороны, его передавшей (подтверждение авторства документа);

- электронное сообщение не претерпело изменений при информационном взаимодействии сторон (подтверждение целостности и подлинности документа);

- электронный документ, содержащийся в сообщении, юридически эквивалентен документу на бумажном носителе.

1.4. Для работы в ЗСРСМЭВ стороны руководствуются действующим законодательством Российской Федерации и нормативными документами Оператора, в том числе Регламентом защищённой сети региональной системы межведомственного электронного взаимодействия Кировской области (далее - Регламент).

2. ТЕХНИЧЕСКИЕ УСЛОВИЯ

2.1. Участник за свой счет оплачивает услуги поставщиков средств защиты информации, приобретает, устанавливает и обеспечивает работоспособность средств защиты информации, необходимых для подключения к ЗСРСМЭВ.

2.2. Участник оплачивает средства связи и каналы связи, необходимые для работы в ЗСРСМЭВ.

2.3. Передачу Участнику ключевой информации осуществляет Оператор.

Виды деятельности по выработки ключевой информации, требующие лицензирования осуществляется Оператор или уполномоченное им лицо – организация, имеющая лицензию на данный вид деятельности.

Уполномоченное лицо на основании заключенного договора с Оператором осуществляет:

- изготовление ключевых документов;

- создание реквизитов доступа для Участника;

- приостановление и возобновление действия реквизитов доступа для Участника;

- аннулирование реквизитов доступа для Участника;

- ведение реестра реквизитов доступа для Участника;

- проверка уникальности реквизитов доступа для Участника в реестре и в архиве;

- подтверждение реквизитов доступа для Участника.

3. ПОРЯДОК ОСУЩЕСТВЛЕНИЯ ОБМЕНА ЭЛЕКТРОННЫМИ СООБЩЕНИЯМИ

3.1. Каждая сторона имеет право в электронной форме передавать другой стороне электронные документы по взаимной договоренности.

3.2. Обмен электронными документами, их подпись и проверка достоверности осуществляется в соответствии с руководствами пользователей на средства защиты, обеспечивающие такой обмен.

3.3. Отправленные электронные документы и полученные Извещения сохраняются и могут быть перенесены на любые носители.

3.4. Стороны должны обеспечить защиту от несанкционированного доступа и непреднамеренного уничтожения и (или) искажения учетных данных, содержащихся в электронных журналах учета электронных документов.

3.5. Хранение подписанных электронных документов.

3.5.1. Все подписанные электронные документы должны храниться каждым Участником не менее 3-х лет.

3.5.2. Электронные архивы подлежат защите от несанкционированного доступа и непреднамеренного уничтожения и (или) искажения.

4. ПРАВА И ОБЯЗАННОСТИ СТОРОН

4.1. Оператор принимает на себя следующие права и обязанности:

4.1.1. Зарегистрировать Участника в ЗСРСМЭВ, в соответствии с Регламентом.

4.1.2. Обеспечить функционирование всего необходимого оборудования со стороны Оператора, необходимого для обмена электронными сообщениями с Участником.

4.1.3. Приостановить обмен электронными сообщениями с Участником при получении от него сообщения о компрометации его ключей шифрования и электронной подписи.

4.1.4. При изменении требований к передаваемым электронным сообщениям ЗСРСМЭВ Оператор обязуется известить Участника об изменениях в установленные законодательством Российской Федерации сроки.

4.1.5. Проинформировать Участника и Уполномоченное лицо о компрометации ключей шифрования других Участников.

4.2. Участник принимает на себя следующие права и обязанности:

4.2.1. Для обеспечения контроля, правил эксплуатации средств защиты, обеспечить доступ уполномоченных представителей Оператора на объекты, на которых будет производиться установка и дальнейшее сопровождение средств защиты информации.

4.2.2. Соблюдать правила работы в ЗСРСМЭВ и требования эксплуатационной документации на средства защиты информации, а также нормативных документов Оператора.

4.2.3. Содержать в исправном состоянии компьютеры, которые подключены к ЗСРСМЭВ, принимать организационные меры для предотвращения несанкционированного доступа к данным компьютерам и

установленному на них программному обеспечению и средствам защиты информации, а также в помещения, в которых они установлены.

4.2.4. Не допускать появления в компьютерной среде, где функционирует ЗСРСМЭВ, компьютерных вирусов и программ, направленных на ее разрушение;

4.2.5. Без согласования с Оператором не вносить никаких изменений в технические и программные средства ЗСРСМЭВ, установленные у Участника.

4.2.6. Прекращать использование скомпрометированного ключа шифрования и немедленно информировать Оператора о факте компрометации ключа.

4.2.7. В связи с тем, что эксплуатируемые по настоящему Соглашению программы и технологии, а также данные, образующиеся в результате работы программного обеспечения, содержат конфиденциальную информацию, пользователь системы обязуется всеми доступными ему способами предотвращать ее разглашение, связанное с работой в ЗСРСМЭВ.

4.2.8. Срок поддержания архивов определяется законодательством Российской Федерации, а в случае возникновения споров - до их разрешения. Стороны несут ответственность за целостность и достоверность своих электронных архивов.

4.3. Стороны обязуются при осуществлении передачи электронных сообщений в ЗСРСМЭВ руководствоваться правилами и техническими требованиями, установленными Оператором и действующим законодательством Российской Федерации.

4.4. Сторона, для которой создалась невозможность исполнения обязательств по настоящему Соглашению, должна немедленно известить об этом другую Сторону. Обмен электронными сообщениями на время действия этих обстоятельств приостанавливается.

4.5. При возникновении споров, связанных с принятием или непринятием электронного сообщения стороны обязаны исполнять требования Регламента.

5. ОТВЕТСТВЕННОСТЬ СТОРОН

5.1. Стороны несут ответственность за использование информации в соответствии с законодательством Российской Федерации.

5.2. Оператор не несет ответственности за ущерб, возникший вследствие принятия электронных сообщений в случае компрометации ключей шифрования Участника, в случае получения информации о компрометации ключей шифрования Участника после принятия электронного документа к исполнению.

5.3. Оператор не несет ответственности за ущерб, возникший в результате:

- неправильного заполнения Участником электронных сообщений в ЗСРСМЭВ;

- разглашения Участником паролей или доступности третьим лицам ключей шифрования.

5.4. Участник несет ответственность за сохранность программного обеспечения системы, архивов открытых ключей и электронных сообщений, размещенных на своих компьютерах.

5.5. Если одна из Сторон предъявляет другой Стороне претензии по электронному сообщению при наличии подтверждения другой Стороны о получении такого сообщения, а другая Сторона не может представить архивную копию спорного электронного сообщения вследствие нарушения требований к хранению архива, то виновной признается Сторона, не представившая архивную копию спорного сообщения.

6. ПОРЯДОК СМЕНЫ КЛЮЧЕЙ ШИФРОВАНИЯ И ЭЛЕКТРОННОЙ ПОДПИСИ

6.1. Порядок смены ключей, в том числе в случае их компрометации и обмена открытыми ключами определяется Регламентом.

6.2. Порядок отзыва реквизитов доступа для Участника определяется Регламентом.

7. ПОРЯДОК РАЗРЕШЕНИЯ КОНФЛИКТНЫХ СИТУАЦИЙ И СПОРОВ

7.1. В случае возникновения спора или разногласий в течение 3-х рабочих дней с момента возникновения таковых, создается комиссия из представителей сторон и заинтересованных лиц для разрешения вопросов путем переговоров.

7.2. При не урегулировании в процессе переговоров спорных вопросов по исполнению, изменении и расторжении договора, споры разрешаются в Арбитражном суде Кировской области в порядке, установленном действующим законодательством РФ.

8. ПРОЧИЕ УСЛОВИЯ

8.1. Настоящее Соглашение вступает в силу с момента его подписания и является бессрочным.

8.2. Изменения и дополнения в настоящее Соглашение могут вноситься только в письменном виде по взаимному согласию Сторон.

8.3. В случае нарушения одной из сторон обязательств, предусмотренных данным Соглашением, другая Сторона вправе в одностороннем порядке расторгнуть настоящее Соглашение, уведомив об этом в письменном виде другую сторону.

8.4. Настоящее Соглашение составляется в двух экземплярах, по одному для каждой Стороны.

8.5. Расторжение настоящего Соглашения не влияет на обязательства Сторон по исполнению электронного документа, принятых до даты расторжения Соглашения.

8.6. При изменении наименования, адреса, банковских реквизитов или реорганизации стороны информируют друг друга в письменном виде в трех дневный срок.

9. ЮРИДИЧЕСКИЕ АДРЕСА И РЕКВИЗИТЫ СТОРОН

Оператор	Участник
Кировское областное государственное бюджетное учреждение «Центр стратегического развития информационных ресурсов и систем управления» Юридический адрес: 610000, г. Киров, ул. К. Маркса 54 Почтовый адрес: 610000, г. Киров, ул. К. Маркса 54 ИНН 4345311251 КПП 434501001 Банковские реквизиты: Л/с 03813008062 в УФК по Кировской области (Департамент финансов Кировской области л\счет 02402002360(КОГБУ «Центр стратегического развития информационных ресурсов и систем управления»)) Р/с 40201810900000100015 в ГРКЦ Банка России по Кировской области г. Киров БИК 0433044001;	
И.о. директора _____/ _____.	_____ _____/ _____
М.П.	М.П.

Приложение №2. Схемы подключения

Предполагается пять схем подключения к защищенной сети РСМЭВ. Они представлены на рисунке 2.1.

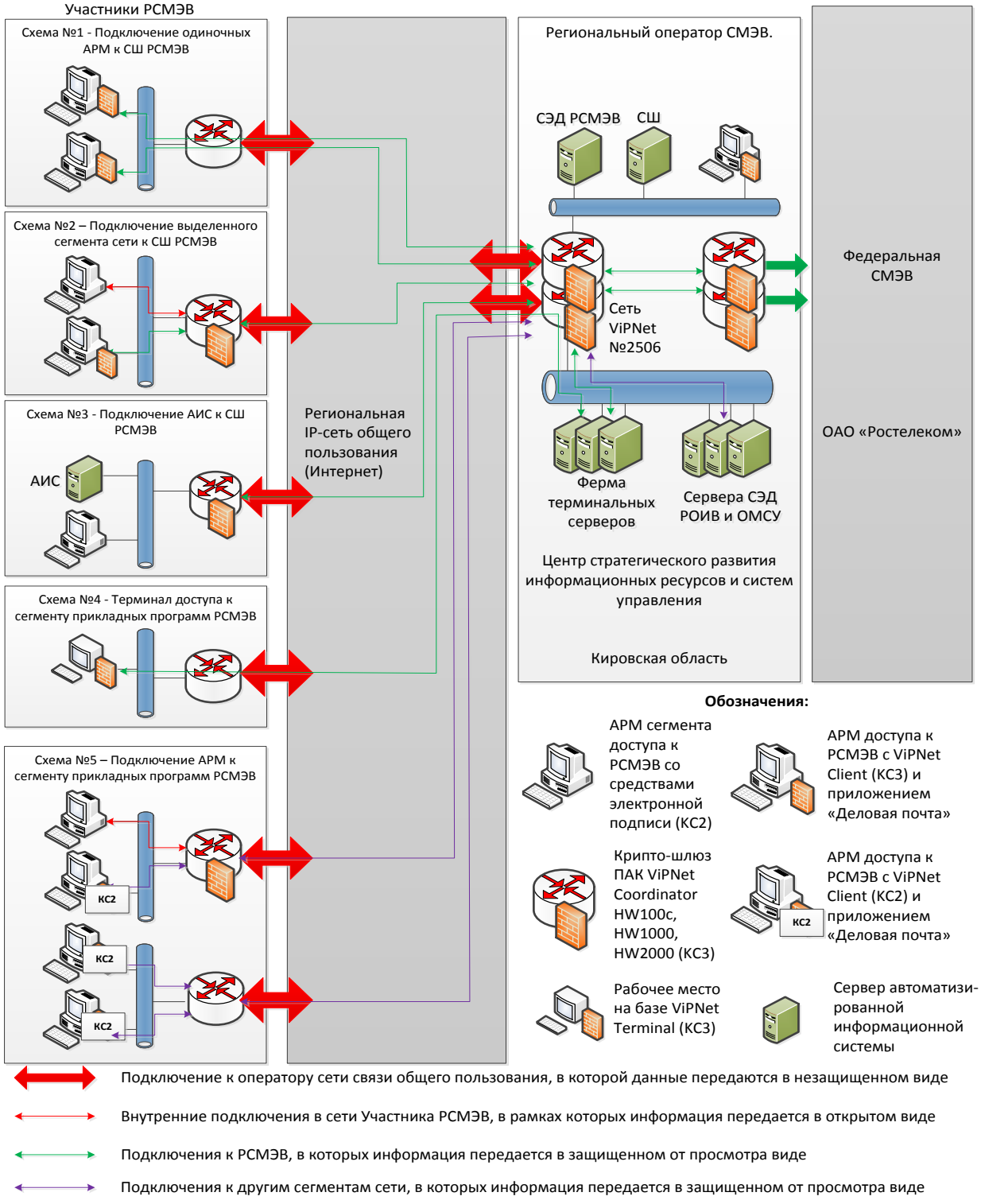

Рисунок 2.1 – Схемы подключения к защищенной сети РСМЭВ

Общее описание схем подключения

Схемы 1-3 предназначены для подключения информационных систем РОИВ и ОМСУ, к сервисной шине РСМЭВ, схемы 4-5 рассчитаны на обеспечение требований информационной безопасности при подключении к сегменту прикладных систем РСМЭВ.

Выделенные для РСМЭВ компьютеры должны быть предназначены исключительно для доступа к информационному ресурсу РСМЭВ и не должны иметь доступа к другим информационным ресурсам. В VIPNet Coordinator HW, VIPNet Terminal, ViPNet Client данные ограничения обеспечиваются при начальной инициализации СКЗИ и не могут быть отменены.

Если организация желает на этих же рабочих местах работать с другими информационными ресурсами, то она должна обеспечить мероприятия по защите информации во всех совмещаемых информационных ресурсах по уровню требований не ниже уровня требований к АРМ РСМЭВ (схема №1) или требований к схеме №3.

Для успешного подключения по всем схемам к защищенной сети достаточно наличия у организации подключения к сети Интернет.

На рабочих местах применяются сертифицированные средства защиты информации от несанкционированного доступа, обеспечивающие контроль целостности, контроль доступа, регистрацию событий безопасности, средства антивирусной защиты, соответствующие требованиям по безопасности автоматизированных информационных систем класса 1Г, а также сертифицированные СКЗИ.

Ниже приведены особенности предлагаемых схем и рекомендации по их подключению.

Схема №1 – подключение одиночных автоматизированных мест к сервисной шине РСМЭВ

По данной схеме предполагается подключение локальной информационной системы к защищенной сети РСМЭВ посредством СКЗИ ViPNet Client (КС3).

Данный вариант применяется при количестве рабочих мест менее 5.

В этой схеме СКЗИ, входящее в состав ViPNet Client (КС3), может применяться для электронной подписи.

Требования к мероприятиям, выполняемым для схемы №1, приведены в Приложении 4

Схема №2 – подключение выделенного сегмента сети к сервисной шине РСМЭВ

Данная схема является рекомендуемой для подключения ведомственных информационных систем РОИВ И ОМСУ размещённых в выделенном сегменте локально-вычислительной сети РОИВ И ОМСУ..

По данной схеме подключается выделенный сегмент локально-вычислительной сети посредством крипто-маршрутизатора ViPNet Coordinator (КС3).

По данной схеме выполняются следующие действия:

1) Компьютеры, предназначенные для работы в РСМЭВ, выделяются в отдельный сегмент сети.

2) На периметре этого сегмента сети устанавливается крипто-маршрутизатор ViPNet Coordinator HW100, HW1000 или HW2000 в различных возможных конфигурациях, в том числе, обеспечивающих отказоустойчивость. Выбор крипто-маршрутизатора выполняется на основе его характеристик, приведенных ниже.

3) На компьютерах предусматриваются использование СКЗИ для электронной подписи по уровню защищенности не ниже КС2.

4) Выполняются мероприятия согласно протоколу, приведенному в Приложении 5.

Схема №3 – подключение АИС организации к сервисной шине РСМЭВ

Данная схема выбирается, если организация имеет сложную автоматизированную информационную систему, а организация выделенных сегментов или АРМ для подключении к РСМЭВ в системе приводит к нарушению алгоритмов её работы.

С точки зрения безопасности по данной схеме выполняются действия:

1) В технологический процесс имеющейся автоматизированной системы добавляется и испытывается интерфейс для связи с сервисной шиной РСМЭВ. Добавление и испытание данного интерфейса проводится в соответствии с регламентом АИС РСМЭВ Кировской области.

2) На периметре этой системы устанавливается крипто-маршрутизатор ViPNet Coordinator HW100c или HW1000 в зависимости от потребности организации к производительности соединения, количества узлов сети, которые должны иметь доступ в РСМЭВ и его надежности.

3) Автоматизированная система аттестуется по требованиям безопасности для ИСПДн уровня защищённости 3 или защищённых автоматизированных систем класса 1Г или государственных информационных систем класса защищённости 3.

4) Дополнительные мероприятия, обязательные к выполнению для этой схемы, приведены в протоколе в Приложении 6.

Схема №4 – подключение терминалов к сегменту прикладных систем РСМЭВ

По данной схеме осуществляется подключение законченного решения ViPNet Terminal к сегменту терминальных серверов РСМЭВ.

В терминальном сеансе пользователи получают все необходимые приложения для работы с РСМЭВ и других задач, реализуемых в защищенной сети региона.

Данный вариант применяется при количестве рабочих мест менее 5.

В случае необходимости использования средств электронной подписи при подключении к сегменту прикладных систем РСМЭВ необходимо использовать схему №5.

Требования к мероприятиям, выполняемым для схемы №4, приведены в Приложении 7.

Схема №5 – подключение выделенного сегмента сети, либо одиночных АРМ к сегменту прикладных систем РСМЭВ.

Данная схема является рекомендуемой для применения в целях подключений ведомственных сетей либо отдельных АРМ к “Системе оказания услуг Кировской области”, а также организации сегментов ведомств на базе ресурсов Оператора. Таких сегментов может быть несколько по решению Оператора.

По данной схеме сегмент либо ведомственная сеть подключается посредством крипто-маршрутизатора ViPNet Coordinator (минимальный требуемый класс защищенности КС2), либо одиночные АРМ с установленным СКЗИ ViPNet Client (КС2).

При этом на отдельные АРМ за криптомаршрутизатором могут ставиться ViPNet Client (КС2).

При подключении по данной схеме с использованием криптомаршрутизатора ViPNet Coordinator выполняются следующие требования:

1) Компьютеры, предназначенные для работы с сегментом прикладных систем РСМЭВ, выделяются в отдельный сегмент сети.

2) На периметре этого сегмента сети устанавливается крипто-маршрутизатор ViPNet Coordinator в различных возможных конфигурациях, в том числе, обеспечивающих отказоустойчивость.

3) Выполняются мероприятия согласно протоколу, приведенному в Приложении 8.

При подключении по данной схеме без использования криптомаршрутизатора ViPNet Coordinator выполняются следующие требования:

1) На компьютеры, предназначенные для работы с сегментом прикладных систем РСМЭВ, устанавливается СКЗИ ViPNet Client (КС2).

2) Выполняются мероприятия согласно протоколу, приведенному в Приложении 8.

Характеристики ПАК ViPNet Coordinator HW

Ниже в таблице приведены основные характеристики крипто-маршрутизаторов ПАК ViPNet Coordinator HW.

№	Характерстика	HW100c	HW1000
1)	Количество защищаемых (туннелируемых) IP-адресов	10	Не ограничено
2)	Максимальная производительность шифрования, Мбит/с	20	280
3)	Возможность отказоустойчивости	нет	Да
4)	Количество портов Ethernet	4x10/100/1000 Мбит/с	4x10/100/1000 Мбит/с
5)	Размеры	187x130x52 мм (ШхВхГ)	19” Rack 1U для монтажа в стойку
6)	Функция маршрутизатора пограничной сети	Да	Да
7)	Возможность установки ViPNet Client за крипто-шлюзом	Да	Да
8)	Возможность взаимодействия с другими сетями ViPNet	Да	Да
9)	Возможность применения «Деловой почты»	Да	Да

Увеличение числа мест для крипто-шлюзов ViPNet Coordinator HW100c

Если организация приобрела криптошлюз HW100c, а количество рабочих мест превышает заданное для него ограничение, то возможно приобретение рабочих мест ViPNet Client, которые будут соединяться с защищенной сетью РСМЭВ через имеющийся у организации криптошлюз.

При наличии в организации своей сети ViPNet

Если организация уже имеет развернутую собственную сеть ViPNet, то обязательными условиями для подключения к РСМЭВ такой сети являются наличие у пограничного ViPNet Coordinator:

– сертификата соответствия СКЗИ по требованиям безопасности на уровень КС3;

– функции маршрутизатора пограничной сети и жесткого диска (модели HW100c, HW1000).

Приложение №3. Технические условия подключения к ЗСРСМЭВ.

1. Общие требования по обеспечению безопасности информационных систем при взаимодействии с системой межведомственного электронного взаимодействия

Подсистема информационной безопасности каждой информационной системы, подключаемой к РСМЭВ, должна обеспечивать установленные законодательством Российской Федерации уровни защищенности информации, обрабатываемой в этой системе.

Каналы связи, используемые информационными системами для взаимодействии с сервисной шиной РСМЭВ, выходящие за пределы контролируемых зон участников взаимодействия, должны быть защищены с помощью сертифицированных средств криптографической защиты информации, удовлетворяющих установленным требованиям к средствам криптографической защиты информации класса не ниже КС3.

Каналы связи, используемые для взаимодействии с сегментом прикладных программ РСМЭВ, выходящие за пределы контролируемых зон участников взаимодействия, должны быть защищены с помощью сертифицированных средств криптографической защиты информации, удовлетворяющих установленным требованиям к средствам криптографической защиты информации класса не ниже КС2.

Подключение каналообразующего оборудования и СКЗИ к электрическим сетям должно подключатся через источники бесперебойного питания.

Доступ к электронным сервисам информационных систем участников взаимодействия должен осуществляться с использованием сертифицированных средств межсетевого экранирования.

Администрирование и сопровождение оборудования, обеспечивающего криптографическую защиту каналов связи, должно производиться только участником взаимодействия либо уполномоченными им лицами.

Доступ посторонних лиц ко всем техническим средствам системы взаимодействия, каналам связи и поддерживающим системам (электропитания, вентиляции, кондиционирования и т.п.) в контролируемой зоне участника взаимодействия должен быть исключен.

В целях обеспечения защиты информации, содержащейся в информационных системах, подключенных к РСМЭВ, участники информационного взаимодействия:

– обеспечивают при обслуживании информационных систем, подключенных к РСМЭВ, исполнение установленных требований по информационной, производственной, технологической и противопожарной безопасности;

– осуществляют контроль доступа посторонних лиц к техническим средствам и каналам связи в контролируемой зоне участника взаимодействия, включая время проведения ремонтных работ и уборки помещений;

– обеспечивают обслуживание информационных систем, подключенных к РСМЭВ, только лицами, имеющими право доступа к информации, содержащейся в указанных информационных системах;

– принимают необходимые и достаточные меры, исключающие доступ посторонних лиц к защищаемой (в т.ч. парольной и ключевой) информации, хранящейся на используемых и отчуждаемых носителях информации;

– осуществляют учет лиц, имеющих доступ к оконечному оборудованию, обеспечивающему криптографическую защиту каналов связи системы взаимодействия, расположенному в контролируемой зоне участника взаимодействия, а также лиц, имеющих возможность изменения

конфигурации информационных систем данного участника взаимодействия, подключенных к РСМЭВ.

В целях обеспечения полноценного функционирования РСМЭВ и подключенных к ней информационных систем каждый участник взаимодействия:

– обеспечивает возможность оперативного переключения на резервный канал с сохранением функций обеспечения безопасности информации для всех каналов связи, выход из строя которых может существенно повлиять на доступность информационных систем, подключенных к системе взаимодействия;

– обеспечивает возможность оперативной замены оборудования, обеспечивающего криптографическую защиту каналов связи, используемых участником взаимодействия для осуществления информационного обмена в рамках системы взаимодействия, в случае выхода такого оборудования из строя.

Для выполнения требований по обеспечению безопасности информационных систем при взаимодействии с РСМЭВ необходимо реализовать систему информационной безопасности, состоящую из 6 подсистем:

– подсистема управления доступом;

– подсистема регистрации и учета;

– подсистема контроля целостности;

– подсистема межсетевого экранирования;

– подсистема антивирусной защиты;

– подсистема криптографической защиты;

2. Требования к средствам защиты информации и АРМ подключаемым к ЗСРСМЭВ

На АРМ Участника, которые подключены к СКЗИ, должно быть установлено и активировано антивирусное программное обеспечение с автоматической проверкой на вирусы и ежедневным обновлением.

Средства защиты информации, в том числе криптографические средств защиты информации, должны пройти в установленном законодательством Российской Федерации порядке процедуру оценки соответствия.

Средства защиты информации от несанкционированного доступа должны быть сертифицированы для использования в защищённых автоматизированных системах класса 1Г.

3. Требования к обеспечению сетевого взаимодействия

Должно обеспечиваться стабильное подключение к сети передачи данных (через сеть Ethernet, PPPoE через XDSL-подключение, PPP через ISDN, сеть мобильной связи GPRS или Wireless-устройства, сети MPLS или VLAN), пропускная способность не менее канала не менее 512 Кбит/с;

Должен обеспечиваться беспрепятственный пропуск сетевых пакетов к криптомаршрутизатору оператора РСМЭВ (а также к криптомаршрутизаторам участника взаимодействия при их наличии) по протоколу UDP на порт 55777 в обоих направлениях, с учетом политики ограничений Интернет-провайдера абонента.

При подключении к системе межведомственного электронного взаимодействия рекомендуется использовать средство межсетевого экранирования и криптографической защиты Vipnet Coordinator HW100C или HW1000

4. Требования по размещению средств защиты информации

Размещение, охрана и режим в помещениях, в которых размещены СКЗИ (далее - помещения), должны обеспечивать безопасность информации, СКЗИ, ключей шифрования и ЭП.

Помещения должны иметь прочные входные двери с замками, гарантирующими надежное закрытие помещений в нерабочее время. Окна помещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в помещения посторонних лиц, необходимо оборудовать металлическими решетками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в помещения.

Размещение и монтаж СКЗИ, а также другого оборудования, функционирующего с СКЗИ, в помещениях должны свести к минимуму возможность неконтролируемого доступа посторонних лиц к указанным средствам.

Режим охраны и порядок доступа в помещения устанавливает Участник. Установленный руководителем Участника режим охраны должен предусматривать периодический контроль технического состояния средств охранной и пожарной сигнализации и соблюдения режима охраны.

Расположение АРМ в помещении должно исключить возможность визуального просмотра информации с монитора. Окна (при наличии) должны быть закрыты шторами (жалюзи).

Для хранения носителей ключевой информации, эксплуатационной и технической документации, инсталлирующих СКЗИ носителей необходимо иметь достаточное число надежно запираемых шкафов (ящиков, хранилищ) индивидуального пользования, оборудованных приспособлениями для опечатывания замочных скважин. Ключи от этих хранилищ должны находиться у соответствующих пользователей СКЗИ. В случае отсутствия у пользователя СКЗИ индивидуального хранилища ключи шифрования и ЭП по окончании рабочего дня должны сдаваться лицу, ответственному за их хранение.

По окончании рабочего дня помещение и установленные в нём хранилища должны быть закрыты, хранилища опечатаны.

Приложение №4. Протокол оценки соответствия для Схемы №1 (форма)

УТВЕРЖДАЮ

Руководитель организации

_____/_____

«____» _____ _____ г.

ПРОТОКОЛ

оценки соответствия требованиям безопасности информации

№ п/п	Группа требований	Требование	Результат выполнения
1	Схема подключения		
1.1	Схема №1	АРМ доступа к РСМЭВ	☑
2	Организационные мероприятия		
2.1	Заведено дело по учету документации, связанной с подключением к РСМЭВ.		☐ Да ☐ Нет
2.2	Ответственные лица.		
2.2.1		Назначен приказом ответственный за режим в организации.	☐ Да ☐ Нет
2.2.2		Назначен приказом ответственный за защиту информации (администратор информационной безопасности).	☐ Да ☐ Нет
2.2.3		Назначен приказом ответственный за криптографическую защиту информации.	☐ Да ☐ Нет
2.2.4		Назначен приказом ответственный за	☐ Да ☐ Нет

№ п/п	Группа требований	Требование	Результат выполнения
		осуществление защищенного взаимодействия с РСМЭВ.	
2.3	Эксплуатация СКЗИ.		
2.3.1		Инструкция по обращению с СКЗИ.	☐ Да ☐ Нет
2.3.2		Наличие и ведение журнала учета средств криптографической защиты.	☐ Да ☐ Нет
2.3.3		Утвержден приказом список лиц, допущенных к работе с АРМ с использованием СКЗИ.	☐ Да ☐ Нет
2.3.4		Наличие сейфа для хранения съемных носителей с ключевой информацией.	☐ Да ☐ Нет
2.4	Наличие и ведение журналов.		
2.4.1		Заведен журнал учета идентификаторов, идентификаторы выданы и учтены	☐ Да ☐ Нет
2.4.2		Заведен журнал инструктажа, инструктажи ведутся	☐ Да ☐ Нет
		Заведен журнал учета носителей конфиденциальной информации, носители, в том числе носитель для получения инициализирующей информации ViPNet, учтены	☐ Да ☐ Нет
2.5	Квалификация ответственных лиц и пользователей.		
2.5.1		Проведено обучение администратора информационной безопасности в части эксплуатации средств КЗИ и средств защиты	☐ Да ☐ Нет

№ п/п	Группа требований	Требование	Результат выполнения
		информации от НСД.	
2.5.2		Проведено обучение пользователей в части эксплуатации АРМ с установленными средствами КЗИ и средствами защиты информации от НСД.	☐ Да ☐ Нет
3	Режимные мероприятия		
3.1	Режим доступа в помещение, в котором установлены рабочие места РСМЭВ, установлен: утвержден список лиц, допущенных к работе в помещениях, к обслуживанию помещений, посторонние лица допускаются только в присутствии допущенных, установлен порядок закрытия и открытия, установлен порядок обслуживания, установлен порядок действий в нештатных ситуациях. Режим учитывает невозможность неконтролируемого необнаруживаемого несанкционированного доступа.		☐ Да ☐ Нет
3.2	Наличие и ведение журнала учета ключей и средств доступа в помещения.		☐ Да ☐ Нет
3.3	Требования к помещениям, в которых установлены АРМ доступа к РСМЭВ.		
3.3.1		Входные двери помещений оборудованы внутренними замками, гарантирующими надежное закрытие дверей при выходе из помещения и в нерабочее время.	☐ Да ☐ Нет
3.4	Требования к помещениям, в которых установлены ПАК «ViPNet Coordinator HW»		

№ п/п	Группа требований	Требование	Результат выполнения
3.4.1		Входные двери помещений оборудованы внутренними замками, гарантирующими надежное закрытие дверей при выходе из помещения и в нерабочее время.	☐ Да ☐ Нет
3.4.2		Окна и двери должны быть оборудованы охранной сигнализацией, связанной с центральным пультом наблюдения за сигнализацией поста охраны.	☐ Да ☐ Нет
3.5	Требования к допуску и обслуживанию.		
3.5.1		В помещения допускаются сотрудники согласно утвержденному приказом перечню.	☐ Да ☐ Нет
3.5.2		Уборка помещения, обслуживание оборудования систем жизнеобеспечения осуществляется назначенным персоналом при выключенных мониторах в присутствии администратора безопасности.	☐ Да ☐ Нет
3.5.3		По окончании рабочего дня, помещения закрываются, опечатываются и сдаются под охрану.	☐ Да ☐ Нет
3.6	Приняты меры, исключающие возможность несанкционированного не обнаруживаемого изменения аппаратной части технических средств, на которых установлено СКЗИ (опечатывание системного блока и разъемов ПЭВМ).		☐ Да ☐ Нет
4	Технические мероприятия		
4.1	Организовано подключение к сети Интернет со		☐ Да ☐ Нет

№ п/п	Группа требований	Требование	Результат выполнения
	скоростью соединения не менее 512 Кбит/с.		
4.2	Вход на АРМ выполняется с использованием USB-токена.		☐ Да ☐ Нет
4.3	Применяется политика назначения и смены паролей (для входа в ОС, BIOS, при шифровании на пароле и т.д.), используются фильтры паролей.		☐ Да ☐ Нет
4.4	Состав технических средств каждого универсального АРМ.		
4.4.1		Сертифицированный отчуждаемый носитель ключевой информации (токен) – по одному на каждого пользователя-участника РСМЭВ.	☐ Да ☐ Нет
4.5	Состав программного обеспечения каждого универсального АРМ.		
4.5.1		Лицензионная операционная система Windows XP/Vista/7/8 (только одна ОС на ПЭВМ), включая установочный комплект.	☐ Да ☐ Нет
4.5.2		Лицензионное антивирусное программное обеспечение, сертифицированное ФСТЭК России с проверкой на НДВ, включая установочный комплект.	☐ Да ☐ Нет
4.5.3		Лицензионное сертифицированное ФСТЭК России СЗИ от НСД, включая установочный комплект.	☐ Да ☐ Нет
4.5.4		Лицензионное сертифицированное ФСБ РФ СКЗИ «ViPNet CSP КС3», включая установочный комплект.	☐ Да ☐ Нет

№ п/п	Группа требований	Требование	Результат выполнения
4.6	Настройка ОС и СЗИ.		
4.6.1		Исключена возможность применения измененных или отладочных версий ОС, таких как, Debug/Checked Build.	☐ Да ☐ Нет
4.6.2		Исключена возможность установки средства отладки и трассировки ПО.	☐ Да ☐ Нет
4.6.3		Регулярно устанавливаются пакеты обновления безопасности ОС (Service Packs, Hot fix и т.п.), обновляются антивирусные базы.	☐ Да ☐ Нет
4.6.4		Установка и настройка СЗИ от НСД и средств КЗИ выполнена в соответствии с эксплуатационной документацией и правилами пользования.	☐ Да ☐ Нет
Примечания			

Представители комиссии:

Ответственный за режим _____ _____

Администратор безопасности _____ _____

Ответственный за СКЗИ _____ _____

Ответственный за осуществление
защищенного взаимодействия с РСМЭВ _____ _____

Приложение №5. Протокол оценки соответствия для Схемы №2 (форма)

УТВЕРЖДАЮ

Руководитель организации

_____/_____

«____» _____ _____ г.

ПРОТОКОЛ

оценки соответствия требованиям безопасности информации

№ п/п	Группа требований	Требование	Результат выполнения
1	Схема подключения		
1.1	Схема №2	Сегмент доступа к СЭД РСМЭВ	☑
2	Организационные мероприятия		
2.1	Заведено дело по учету документации, связанной с подключением к РСМЭВ.		☐ Да ☐ Нет
2.2	Ответственные лица.		
2.2.1		Назначен приказом ответственный за режим в организации.	☐ Да ☐ Нет
2.2.2		Назначен приказом ответственный за защиту информации (администратор информационной безопасности).	☐ Да ☐ Нет
2.2.3		Назначен приказом ответственный за криптографическую защиту информации.	☐ Да ☐ Нет
2.2.4		Назначен приказом ответственный за	☐ Да ☐ Нет

№ п/п	Группа требований	Требование	Результат выполнения
		осуществление защищенного взаимодействия с РСМЭВ.	
2.3	Эксплуатация СКЗИ.		
2.3.1		Инструкция по обращению с СКЗИ.	☐ Да ☐ Нет
2.3.2		Наличие и ведение журнала учета средств криптографической защиты.	☐ Да ☐ Нет
2.3.3		Утвержден приказом список лиц, допущенных к работе с АРМ с использованием СКЗИ.	☐ Да ☐ Нет
2.3.4		Наличие сейфа для хранения съемных носителей с ключевой информацией.	☐ Да ☐ Нет
2.4	Наличие и ведение журналов.		
2.4.1		Заведен журнал учета идентификаторов, идентификаторы выданы и учтены	☐ Да ☐ Нет
2.4.2		Заведен журнал инструктажа, инструктажи ведутся	☐ Да ☐ Нет
2.4.3		Заведен журнал учета носителей конфиденциальной информации, носители, в том числе носитель для получения инициализирующей информации ViPNet, учтены	☐ Да ☐ Нет
2.5	Квалификация ответственных лиц и пользователей.		
2.5.1		Проведено обучение администратора информационной безопасности в части эксплуатации средств КЗИ и средств защиты информации от НСД.	☐ Да ☐ Нет

№ п/п	Группа требований	Требование	Результат выполнения
2.5.2		Проведено обучение пользователей в части эксплуатации АРМ с установленными средствами КЗИ и средствами защиты информации от НСД.	☐ Да ☐ Нет
3	Режимные мероприятия		
3.1	Режим доступа в помещение, в котором установлены рабочие места РСМЭВ, установлен: утвержден список лиц, допущенных к работе в помещениях, к обслуживанию помещений, посторонние лица допускаются только в присутствии допущенных, установлен порядок закрытия и открытия, установлен порядок обслуживания, установлен порядок действий в нештатных ситуациях. Режим учитывает невозможность неконтролируемого необнаруживаемого несанкционированного доступа.		☐ Да ☐ Нет
3.2	Наличие и ведение журнала учета ключей и средств доступа в помещения.		☐ Да ☐ Нет
3.3	Требования к помещениям, в которых установлены АРМ доступа к РСМЭВ.		
3.3.1		Входные двери помещений оборудованы внутренними замками, гарантирующими надежное закрытие дверей при выходе из помещения и в нерабочее время.	☐ Да ☐ Нет
3.4	Требования к помещениям, в которых установлены ПАК «ViPNet Coordinator HW»		
3.4.1		Входные двери помещений оборудованы внутренними замками, гарантирующими	☐ Да ☐ Нет

№ п/п	Группа требований	Требование	Результат выполнения
		надежное закрытие дверей при выходе из помещения и в нерабочее время.	
3.4.2		Окна и двери должны быть оборудованы охранной сигнализацией, связанной с центральным пультом наблюдения за сигнализацией поста охраны.	☐ Да ☐ Нет
3.5	Требования к допуску и обслуживанию.		
3.5.1		В помещения допускаются сотрудники согласно утвержденному приказом перечню.	☐ Да ☐ Нет
3.5.2		Уборка помещения, обслуживание оборудования систем жизнеобеспечения осуществляется назначенным персоналом при выключенных мониторах в присутствии администратора безопасности.	☐ Да ☐ Нет
3.5.3		По окончании рабочего дня, помещения закрываются, опечатываются и сдаются под охрану.	☐ Да ☐ Нет
3.6	Приняты меры, исключающие возможность несанкционированного не обнаруживаемого изменения аппаратной части технических средств, на которых установлено СКЗИ (опечатывание системного блока и разъемов ПЭВМ и ПАК «ViPNet Coordinator HW»).		☐ Да ☐ Нет
4	Технические мероприятия		
4.1	Сетевой сегмент доступа к РСМЭВ является изолированным сетевым сегментом		☐ Да ☐ Нет
4.3	Организовано подключение к сети Интернет со скоростью		☐ Да ☐ Нет

№ п/п	Группа требований	Требование	Результат выполнения
	соединения не менее 512 Кбит/с.		
4.4	Вход на АРМ выполняется с использованием USB-токена.		☐ Да ☐ Нет
4.5	Применяется политика назначения и смены паролей (для входа в ОС, BIOS, при шифровании на пароле и т.д.), используются фильтры паролей.		☐ Да ☐ Нет
4.6	Состав технических средств каждого универсального АРМ.		
4.6.1		Сертифицированный отчуждаемый носитель ключевой информации (токен) – по одному на каждого пользователя-участника РСМЭВ.	☐ Да ☐ Нет
4.7	Состав технических средств сетевого сегмента.		
4.7.1		ПАК «ViPNet Coordinator» HW100(a/b/c)/1000 КСЗ.	☐ Да ☐ Нет
4.8	Состав программного обеспечения каждого универсального АРМ.		
4.8.1		Лицензионная операционная система Windows XP/Vista/7/8 (только одна ОС на ПЭВМ), включая установочный комплект.	☐ Да ☐ Нет
4.8.2		Лицензионное антивирусное программное обеспечение, сертифицированное ФСТЭК России с проверкой на НДВ, включая установочный комплект.	☐ Да ☐ Нет
4.8.3		Лицензионное сертифицированное ФСТЭК России СЗИ от НСД, включая установочный комплект.	☐ Да ☐ Нет

№ п/п	Группа требований	Требование	Результат выполнения
4.8.4		Лицензионное сертифицированное ФСБ РФ СКЗИ «ViPNet CSP КС2», включая установочный комплект.	☐ Да ☐ Нет
4.9	Настройка ОС и СЗИ.		
4.9.1		Исключена возможность применения измененных или отладочных версий ОС, таких как, Debug/Checked Build.	☐ Да ☐ Нет
4.9.2		Исключена возможность установки средства отладки и трассировки ПО.	☐ Да ☐ Нет
4.9.3		Регулярно устанавливаются пакеты обновления безопасности ОС (Service Packs, Hot fix и т.п.), обновляются антивирусные базы.	☐ Да ☐ Нет
4.9.4		Установка и настройка СЗИ от НСД и средств КЗИ выполнена в соответствии с эксплуатационной документацией и правилами пользования.	☐ Да ☐ Нет
Примечания			
*			

Представители комиссии:

Ответственный за режим _____ _____

Администратор безопасности _____ _____

Ответственный за СКЗИ _____ _____

Ответственный за осуществление
защищенного взаимодействия с РСМЭВ _____ _____

Приложение №6. Протокол оценки соответствия для Схемы №3 (форма)

УТВЕРЖДАЮ

Руководитель организации

_____/_____

«____» _____ _____ г.

ПРОТОКОЛ

оценки соответствия требованиям безопасности информации

№ п/п	Группа требований	Требование	Результат выполнения
1	Схема подключения		
1.1	Схема №3	АИС с подключением к сервисной шиной РСМЭВ	☑
2	Организационные мероприятия		
2.1	Заведено дело по учету документации, связанной с подключением к РСМЭВ.		☐ Да ☐ Нет
2.2	Назначен приказом ответственный за осуществление защищенного взаимодействия с РСМЭВ.		☐ Да ☐ Нет
3	Требования по аттестации АИС		
3.1	АИС имеет действующий аттестат соответствия требованиям информационной безопасности по одному из классов:		
3.1.		Информационная система персональных	☐ Да ☐ Нет

№ п/п	Группа требований	Требование	Результат выполнения
1		данных – уровня защищённости 3 и выше	
3.1.2		Автоматизированная система – 1Г.	☐ Да ☐ Нет
3.1.3		Государственная информационная система – класса защищённости 3 и выше	☐ Да ☐ Нет
3.2	В технологическом процессе аттестованной АИС предусмотрено взаимодействие с сервисной шиной РСМЭВ через сети связи общего пользования по защищенному каналу с уровнем защищенности не ниже КС3.		☐ Да ☐ Нет
4	Технические мероприятия		
4.1	Организовано подключение к сети Интернет со скоростью соединения не менее 512 Кбит/с.		☐ Да ☐ Нет
Примечания			
*			

Представители комиссии:

Ответственный за режим _____ _____

Администратор безопасности _____ _____

Ответственный за СКЗИ _____ _____

Ответственный за осуществление защищенного взаимодействия с РСМЭВ _____ _____

Приложение №7. Протокол оценки соответствия для Схемы №4 (форма)

УТВЕРЖДАЮ

Руководитель организации

_____/_____

«____» _____ _____ г.

ПРОТОКОЛ

оценки соответствия требованиям безопасности информации

№ п/п	Группа требований	Требование	Результат выполнения
1	Схема подключения		
1.1	Схема №4	Терминал доступа к СЭД РСМЭВ	☑
2	Организационные мероприятия		
2.1	Заведено дело по учету документации, связанной с подключением к РСМЭВ.		☐ Да ☐ Нет
2.2	Ответственные лица.		
2.2.1		Назначен приказом ответственный за режим в организации.	☐ Да ☐ Нет
2.2.2		Назначен приказом ответственный за защиту информации (администратор информационной безопасности).	☐ Да ☐ Нет
2.2.3		Назначен приказом ответственный за криптографическую защиту информации.	☐ Да ☐ Нет
2.2.4		Назначен приказом ответственный за	☐ Да ☐ Нет

№ п/п	Группа требований	Требование	Результат выполнения
		осуществление защищенного взаимодействия с РСМЭВ.	
2.3	Эксплуатация СКЗИ.		
2.3.1		Инструкция по обращению с СКЗИ.	☐ Да ☐ Нет
2.3.2		Наличие и ведение журнала учета средств криптографической защиты.	☐ Да ☐ Нет
2.3.3		Утвержден приказом список лиц, допущенных к работе с терминалом с использованием СКЗИ.	☐ Да ☐ Нет
2.3.4		Наличие сейфа для хранения съемных носителей с ключевой информацией.	☐ Да ☐ Нет
2.4	Наличие и ведение журналов.		
2.4.1		Заведен журнал учета идентификаторов, идентификаторы выданы и учтены.	☐ Да ☐ Нет
2.4.2		Заведен журнал инструктажа, инструктажи ведутся.	☐ Да ☐ Нет
		Заведен журнал учета носителей конфиденциальной информации, носители, в том числе носитель для получения инициализирующей информации ViPNet, учтены.	☐ Да ☐ Нет
2.5	Квалификация ответственных лиц и пользователей.		
2.5.1		Проведено обучение администратора информационной безопасности в части эксплуатации средств КЗИ и средств защиты	☐ Да ☐ Нет

№ п/п	Группа требований	Требование	Результат выполнения
		информации от НСД.	
2.5.2		Проведено обучение пользователей в части эксплуатации терминала с установленными средствами КЗИ.	☐ Да ☐ Нет
3	Режимные мероприятия		
3.1	Режим доступа в помещение, в котором установлены рабочие места РСМЭВ, установлен: утвержден список лиц, допущенных к работе в помещениях, к обслуживанию помещений, посторонние лица допускаются только в присутствии допущенных, установлен порядок закрытия и открытия, установлен порядок обслуживания, установлен порядок действий в нештатных ситуациях. Режим учитывает невозможность неконтролируемого необнаруживаемого несанкционированного доступа.		☐ Да ☐ Нет
3.2	Наличие и ведение журнала учета ключей и средств доступа в помещения.		☐ Да ☐ Нет
3.3	Требования к помещениям, в которых установлены терминалы доступа к РСМЭВ.		
3.3.1		Входные двери помещений оборудованы внутренними замками, гарантирующими надежное закрытие дверей при выходе из помещения и в нерабочее время.	☐ Да ☐ Нет
3.3.2		Окна (при необходимости) и двери должны быть оборудованы охранной сигнализацией, связанной с центральным пультом наблюдения за сигнализацией поста охраны.	☐ Да ☐ Нет

№ п/п	Группа требований	Требование	Результат выполнения
3.4	Требования к допуску и обслуживанию.		
3.4.1		В помещения допускаются сотрудники согласно утвержденному приказом перечню.	☐ Да ☐ Нет
3.4.2		Уборка помещения, обслуживание оборудования систем жизнеобеспечения осуществляется назначенным персоналом при выключенных мониторах в присутствии администратора безопасности.	☐ Да ☐ Нет
3.4.3		По окончании рабочего дня, помещения закрываются, опечатываются и сдаются под охрану.	☐ Да ☐ Нет
3.5	Приняты меры, исключающие возможность несанкционированного не обнаруживаемого изменения аппаратной части технических средств, на которых установлено СКЗИ (опечатывание системного блока и разъемов терминалов доступа).		☐ Да ☐ Нет
4	Технические мероприятия		
4.1	Организовано подключение к сети Интернет со скоростью соединения не менее 512 Кбит/с.		☐ Да ☐ Нет
4.2	Вход на терминал выполняется с использованием USB-токена.		☐ Да ☐ Нет
4.3	Применяется политика назначения и смены паролей (для входа в ОС, BIOS, при шифровании на пароле и т.д.), используются фильтры паролей.		☐ Да ☐ Нет
4.4	Состав технических средств каждого терминала доступа.		

№ п/п	Группа требований	Требование	Результат выполнения
4.4.1		Программно-аппаратный комплекс ViPNet Terminal (вариант исполнения №4).	☐ Да ☐ Нет
4.4.2		Сертифицированный отчуждаемый носитель ключевой информации (токен) – по одному на каждого пользователя-участника РСМЭВ.	☐ Да ☐ Нет
Примечания			
*			

Представители комиссии:

Ответственный за режим _____ _____

Администратор безопасности _____ _____

Ответственный за СКЗИ _____ _____

Ответственный за осуществление
защищенного взаимодействия с РСМЭВ _____ _____

Приложение №8. Протокол оценки соответствия для Схемы №5 (форма)

УТВЕРЖДАЮ

Руководитель организации

_____/_____

«____» _____ _____ г.

ПРОТОКОЛ

оценки соответствия требованиям безопасности информации

№ п/п	Группа требований	Требование	Результат выполнения
1	Схема подключения		
1.1	Схема №5	Сегмент доступа к СЭД РОИВ и ОМСУ:	☑
2	Организационные мероприятия		
2.1	Заведено дело по учету документации, связанной с подключением к СЭД РОИВ и ОМСУ.		☐ Да ☐ Нет
2.2	Ответственные лица.		
2.2.1		Назначен приказом ответственный за режим в организации.	☐ Да ☐ Нет
2.2.2		Назначен приказом ответственный за защиту информации (администратор информационной безопасности).	☐ Да ☐ Нет
2.2.3		Назначен приказом ответственный за криптографическую защиту информации.	☐ Да ☐ Нет
2.2.4		Назначен приказом ответственный за	☐ Да ☐ Нет

№ п/п	Группа требований	Требование	Результат выполнения
		осуществление защищенного взаимодействия с СЭД РОИВ и ОМСУ .	
2.3	Эксплуатация СКЗИ.		
2.3.1		Инструкция по обращению с СКЗИ.	☐ Да ☐ Нет
2.3.2		Наличие и ведение журнала учета средств криптографической защиты.	☐ Да ☐ Нет
2.3.3		Утвержден список лиц, допущенных к работе с СКЗИ.	☐ Да ☐ Нет
2.3.4		Наличие сейфа для хранения съемных носителей с ключевой информацией.	☐ Да ☐ Нет
2.4	Наличие и ведение журналов.		
2.4.1		Заведен журнал учета идентификаторов, идентификаторы выданы и учтены.	☐ Да ☐ Нет
2.4.2		Заведен журнал инструктажа, инструктажи ведутся.	☐ Да ☐ Нет
		Заведен журнал учета носителей конфиденциальной информации, носители, в том числе носитель для получения инициализирующей информации ViPNet, учтены.	☐ Да ☐ Нет
2.5	Квалификация ответственных лиц и пользователей.		
2.5.1		Проведено обучение (инструктаж) администратора информационной безопасности в части эксплуатации средств КЗИ и средств защиты информации от НСД.	☐ Да ☐ Нет

№ п/п	Группа требований	Требование	Результат выполнения
2.5.2		Проведено обучение пользователей в части эксплуатации АРМ с установленными средствами КЗИ.	☐ Да ☐ Нет
3	Режимные мероприятия		
3.1	Режим доступа в помещение, в котором установлены СКЗИ, установлен: утвержден список лиц, допущенных к работе в помещениях, к обслуживанию помещений, посторонние лица допускаются только в присутствии допущенных, установлен порядок закрытия и открытия, установлен порядок обслуживания, установлен порядок действий в нештатных ситуациях. Режим учитывает невозможность неконтролируемого необнаруживаемого несанкционированного доступа.		☐ Да ☐ Нет
3.2	Наличие и ведение журнала учета ключей и средств доступа в помещения.		☐ Да ☐ Нет
3.3	Требования к помещениям, в которых установлены СКЗИ		
3.3.1		Входные двери помещений оборудованы внутренними замками, гарантирующими надежное закрытие дверей при выходе из помещения и в нерабочее время.	☐ Да ☐ Нет
3.3.2		Окна и двери должны быть оборудованы охранной сигнализацией, связанной с центральным пультом наблюдения за сигнализацией поста охраны.	☐ Да ☐ Нет
3.3.3		Помещение оборудуется средствами вентиляции и кондиционирования воздуха,	☐ Да ☐ Нет

№ п/п	Группа требований	Требование	Результат выполнения
		обеспечивающими соблюдение установленных параметров температурно-влажностного режима, вентиляции и очистки воздуха (для ПАК «ViPNet Coordinator HW»).	
3.4	Требования к допуску и обслуживанию.		
3.4.1		В помещения допускаются сотрудники согласно утвержденному перечню.	☐ Да ☐ Нет
3.4.2		Уборка помещения, обслуживание оборудования систем жизнеобеспечения осуществляется назначенным персоналом при выключенных мониторах в присутствии сотрудников, допущенных к работе в помещении.	☐ Да ☐ Нет
3.4.3		По окончании рабочего дня помещения с установленными СКЗИ закрываются, опечатываются и сдаются под охрану.	☐ Да ☐ Нет
4	Технические мероприятия		
4.1	Организовано подключение к сети Интернет со скоростью соединения не менее 512 Кбит/с.		☐ Да ☐ Нет
4.2	Пользователи сегмента сети имеют доступ к ресурсам ЛВС и Интернет (разрешено)		☐ Да ☐ Нет
4.3	Применяется политика назначения и смены паролей (для входа в ОС, BIOS, при шифровании на пароле и т.д.), используются фильтры паролей.		☐ Да ☐ Нет
4.4	Состав программно-технических средств сетевого сегмента.		

№ п/п	Группа требований	Требование	Результат выполнения
4.4.1		ViPNet Coordinator HW100c/1000	☐ Да ☐ Нет
4.4.2		ViPNet Client КС2	☐ Да ☐ Нет
4.5	Состав программного обеспечения каждого АРМ.		
4.5.1		Лицензионная операционная система Windows XP Pro/Vista Business/7 Профессиональная/8 (только одна ОС на ПЭВМ), включая установочный комплект.	☐ Да ☐ Нет
4.5.2		Лицензионное антивирусное программное обеспечение: Kaspersky Endpoint Security, DrWeb Enterprise Suite, ESET Nod32.	☐ Да ☐ Нет
4.5.3		Лицензионное сертифицированное ФСБ РФ средство электронной подписи: при необходимости для использования в СЭД. Класс защищенности КС1.	☐ Да ☐ Нет
4.6	Настройка ОС и СЗИ на АРМ.		
4.6.1		Исключена возможность применения измененных или отладочных версий ОС, таких как, Debug/Checked Build.	☐ Да ☐ Нет
4.6.2		Исключена возможность установки средства отладки и трассировки ПО.	☐ Да ☐ Нет
4.6.3		Регулярно устанавливаются пакеты обновления безопасности ОС (Service Packs, Hot fix и т.п.), обновляются антивирусные базы.	☐ Да ☐ Нет
4.6.4		Установка и настройка средств КЗИ	☐ Да ☐ Нет

№ п/п	Группа требований	Требование	Результат выполнения
		выполнена в соответствии с эксплуатационной документацией и правилами пользования.	
Примечания			
*			

Представители комиссии:

Ответственный за режим _____ _____

Администратор безопасности _____ _____

Ответственный за СКЗИ _____ _____

Ответственный за осуществление защищенного взаимодействия с РСМЭВ _____ _____

Приложение №9. Заявка на подключение к защищенной сети передачи данных РСМЭВ (форма)

На официальном бланке организации

Оператору РСМЭВ
Кировской области

№Исх от «___»_____20__г.

ЗАЯВКА

_____
(наименование участника информационного взаимодействия)

на подключение к защищенной сети передачи данных
РСМЭВ Кировской области

В целях реализации взаимодействия при обеспечении предоставления (исполнения) государственных (муниципальных) услуг (функций) в электронной форме прошу предоставить подключение к защищенной сети передачи данных РСМЭВ Кировской области.

Информирую Вас о нашем согласии с условиями подключения, изложенными в Регламенте защищенной сети Региональной системы межведомственного электронного взаимодействия Кировской области (далее Регламент).

_____
(наименование участника информационного взаимодействия)

принимает на себя обязательства по выполнению положений Регламента и несет ответственность за качество их выполнения.

Информируем Вас о проведении всех подготовительных мероприятий, необходимых для подключения к защищенной сети передачи данных РСМЭВ.

В подтверждение заявки и в целях обеспечения подключения прилагаю следующие документы:

1. Анкета _____
(наименование участника информационного взаимодействия)

– на __ листах в __ экз.;

2. Копия приказа о назначении лица, ответственного за осуществление защищенного взаимодействия _____
_____
(наименование участника информационного взаимодействия)

в РСМЭВ – на __ листах в __ экз.;

3. Перечень сведений для подключения к сети передачи данных для схемы № __ – на __ листах в __ экз.;

4. Протокол оценки соответствия _____
_____
(наименование участника информационного взаимодействия)

требованиям информационной безопасности для схемы № __ – на __ листах в __ экз.

Ответственность за достоверность предоставляемых сведений оставляю за собой.

Руководитель _____/_____

М.П.

Приложение №10. Анкета Участника защищенной сети РСМЭВ (форма)

АНКЕТА (ФОРМА)

Участника защищенной сети РСМЭВ Кировской области

«___»_____20__года

1. Сведения об Участнике информационного взаимодействия				
1.1.Полное Наименование Участника				
1.2. Краткое наименование Участника				
1.3. Почтовый адрес				
1.4. Юридический адрес				
2. Сведения об ответственных лицах Участника, контактная информация				
2.1. Лицо, ответственное за осуществление защищенного взаимодействия		Рабочий тел-н	Мобильный тел-н	E-mail
ФИО				
2.2. Лицо, ответственное за информационную безопасность		Рабочий тел-н	Мобильный тел-н	E-mail
ФИО				
2.3. Лицо, ответственное за технические средства подключения		Рабочий тел-н	Мобильный тел-н	E-mail
ФИО				
3. Сведения об объекте подключения				
3.1. Адрес объекта подключения				
3.2. Этаж				
3.3. Помещение				

Руководитель _____/_____

МП

Приложение №11. Сведения, предоставляемые при подключении к РСМЭВ

Сведения для схемы №1.

№ п/п	Наименование	Сведения
1	Полное наименование РОИВ или ОМСУ.	
2	Место нахождения (адрес) – населенный пункт, улица, дом.	
4	Количество АРМ, включаемых в защищенную сеть.	
5	Серийные номера ViPNet Client	
6	Условия подключения ViPNet к внешней сети.	[ ] Без межсетевого экрана [ ] Через МЭ с динамической трансляцией адресов [ ] Через МЭ со статической трансляцией адресов

Перечень пользователей ViPNet Client (пример)

№	Фамилия	Имя	Отчество	Должность	Отдел	E-mail	Телефон
1.	Петров	Василий	Иванович	Инспектор	ИО	pvi00101@mail.ru	66-66-66

Таблица привязки АРМ и пользователей (пример)

№ п/п	АРМ	Пользователь (ли)
1	АРМ1	Петров В.И.
2	АРМ2	Сидорова А.А. Иванова К.С.
3	АРМ3	Софронов А.В.
…	…	…
4	АРМ4	Степанова Т.В. Попова Л.А.

Важно! В схеме №1 применяются рабочие места на базе ViPNet Client (КС3), в которых доступна «Деловая почта» - система, позволяющая выполнять защищенный обмен документами между участниками сети и использовать электронную подпись. Поэтому для применения ViPNet Client пользователи АРМ должны быть идентифицированы и привязаны к конкретным АРМ.
Для этого предоставляется перечень пользователей и таблица привязки АРМ и пользователей.

Сведения для схемы №2.

№ п/п	Наименование	Сведения
1	Полное наименование РОИВ или ОМСУ.	
2	Место нахождения (адрес) – населенный пункт, улица, дом.	
3	Количество АРМ, включаемых в защищенную сеть.	
4	Статические IP-адреса всех АРМ, включаемых в защищенную сеть.	
5	Серийные номера ViPNet Client (при их использовании)	
6	Условия подключения ViPNet к внешней сети.	[ ] Без межсетевого экрана [ ] Через МЭ с динамической трансляцией адресов [ ] Через МЭ со статической трансляцией адресов
Сведения о ПАК ViPNet Coordinator HW		
7	Наименование изделия	
8	Модификация изделия	
9	Лицензионный номер ПАК	
10	Учетный номер по ФСТЭК	
11	Учетный номер СКЗИ	
12	IP-адрес и маска сети внутреннего сетевого интерфейса ПАК	
13	IP-адрес и маска сети внешнего сетевого интерфейса ПАК	
14*	Внутренний IP-адрес МЭ	
15*	IP-адрес МЭ, через который осуществляется доступ к ПАК со стороны внешних узлов (внешний адрес МЭ)	
16*	Номер порта, который задан в настройках МЭ для обеспечения доступа к координатору со стороны внешних узлов (по умолчанию UDP55777)	

***** - указывается при подключении ПАК через межсетевой экран (МЭ). В роли МЭ обычно выступает ADSL-модем.

Сведения для схемы №3.

Для подключения по схеме №3 обязательно предоставление:

1. Технологического процесса обработки информации в АИС организации с обязательным наличием связи между АИС и сервисной шиной РСМЭВ.
2. Технического паспорта на АИС.
3. Аттестата соответствия АИС организации в качестве ИСПДн по требованиям безопасности для класса К1.
4. Следующих дополнительных сведений:

№ п/п	Наименование	Сведения
1	Полное наименование РОИВ или ОМСУ.	
2	Место нахождения (адрес) – населенный пункт, улица, дом.	
3	Количество АРМ, включаемых в защищенную сеть.	
4	Статические IP-адреса всех АРМ, включаемых в защищенную сеть.	
5	Условия подключения ViPNet к внешней сети.	[ ] Без межсетевого экрана [ ] Через МЭ с динамической трансляцией адресов [ ] Через МЭ со статической трансляцией адресов
Сведения о ПАК ViPNet Coordinator HW		
5	Наименование изделия	
6	Модификация изделия	
7	Лицензионный номер ПАК	
8	Учетный номер по ФСТЭК	

Сведения для схемы №4.

№	Наименование	Сведения
1	Полное наименование РОИВ или ОМСУ	
2	Место нахождения (адрес) – населенный пункт, улица, дом.	
3	Количество пользователей, регистрируемых на терминале доступа.	
Сведения о ПАК «ViPNet Terminal»		
4	Наименование изделия	ПАК «ViPNet Terminal КС3»
5	Модификация изделия	Исполнение №4
6	Лицензионный номер ПАК	
7	Учетный номер по ФСТЭК	
8	Учетный номер по ФСБ (номер СКЗИ)	
9	Условия подключения ПАК «ViPNet Terminal» к внешней сети.	[ ] Без межсетевого экрана [ ] Через МЭ с динамической трансляцией адресов [ ] Через МЭ со статической трансляцией адресов
10	IP-адрес и маска сети сетевого интерфейса терминала доступа.	
11	IP-адрес шлюза по умолчанию.	
12*	Внутренний IP-адрес МЭ.	
13*	IP-адрес МЭ, через который осуществляется доступ к терминалу со стороны внешних узлов (внешний адрес МЭ).	
14*	Номер порта, который задан в настройках МЭ для обеспечения доступа к терминалу со стороны внешних узлов (по умолчанию UDP55777).	

***** - указывается при подключении терминала доступа через МЭ. В роли МЭ обычно выступает ADSL-модем (или иное сетевое устройство, предоставляющее доступ к сети Интернет).

Сведения о пользователях, регистрируемых на терминале доступа.

№	Фамилия	Имя	Отчество	Должность	Отдел	E-mail
1						
2						

Сведения для схемы №5.

№ п/п	Наименование	Сведения
1	Полное наименование РОИВ или ОМСУ.	
2	Место нахождения (адрес) – населенный пункт, улица, дом.	
3	Названия подключаемых сегментов	
4	Количество АРМ, включаемых в защищенную сеть.	
5	Статические IP-адреса всех АРМ, включаемых в защищенную сеть.	
6	Серийные номера ViPNet Client (при их использовании)	
7	Условия подключения ViPNet к внешней сети.	[ ] Без межсетевого экрана [ ] Через МЭ с динамической трансляцией адресов [ ] Через МЭ со статической трансляцией адресов
Сведения о ПАК ViPNet Coordinator HW (при его использовании)		
8	Наименование изделия	
9	Модификация изделия	
10	Лицензионный номер ПАК	
11	Учетный номер по ФСТЭК	
12	Учетный номер СКЗИ	
13	IP-адрес и маска сети внутреннего сетевого интерфейса ПАК	
14	IP-адрес и маска сети внешнего сетевого интерфейса ПАК	
15*	Внутренний IP-адрес МЭ	
16*	IP-адрес МЭ, через который осуществляется доступ к ПАК со стороны внешних узлов (внешний адрес МЭ)	
17*	Номер порта, который задан в настройках МЭ для обеспечения доступа к координатору со стороны внешних узлов (по умолчанию UDP55777)	

***** - указывается при подключении ПАК через межсетевой экран (МЭ). В роли МЭ обычно выступает ADSL-модем.

Перечень пользователей ViPNet Client (пример)

№	Фамилия	Имя	Отчество	Должность	Отдел	E-mail	Телефон
1.	Петров	Василий	Иванович	Инспектор	ИО	pvi00101@mail.ru	66-66-66

Таблица привязки АРМ и пользователей (пример)

№ п/п	**АРМ**	**Пользователь (ли)**
1	АРМ1	Петров В.И.
2	АРМ2	Сидорова А.А. Иванова К.С.
3	АРМ3	Софронов А.В.
4	АРМ4	Степанова Т.В. Попова Л.А.

Важно! В схеме №5 применяются рабочие места на базе ViPNet Client (КС2), в которых доступна «Деловая почта» - система, позволяющая выполнять защищенный обмен документами между участниками сети и использовать электронную подпись. Поэтому для применения ViPNet Client пользователи АРМ должны быть идентифицированы и привязаны к конкретным АРМ.
Для этого предоставляется перечень пользователей и таблица привязки АРМ и пользователей.

Приложение №12. Акт приема-передачи инициализирующей информации СКЗИ (форма)

Акт (ФОРМА)

приема-передачи инициализирующей информации

СКЗИ VipNet

«___» _____ 20___ г.

_____,

(наименование организации-лицензиата ФСБ, обслуживающего защищенную сеть РСМЭВ)

в лице _____, действующего на основании_____, именуемый в дальнейшем Оператор РСМЭВ с одной стороны и

_____,

в лице _____, действующего на основании Доверенности №____ от «___»_____20__г., именуемый в дальнейшем Участник информационного взаимодействия с другой стороны, именуемые в дальнейшем Стороны составили настоящий Акт о том, что:

_____,

(наименование организации-лицензиата ФСБ, обслуживающего защищенную сеть РСМЭВ)

в соответствии со Сведениями, приложенными Участником информационного взаимодействия к Заявке на подключение, изготовил и передал Участнику информационного взаимодействия информацию для первичной инициализации СКЗИ VipNet на носителе, а Участник информационного взаимодействия принял ее.

Акт составлен в двух идентичных экземплярах по одному для каждой из Сторон.

Оператор РСМЭВ	Участник информационного взаимодействия
_____	_____
_____	_____
_____	_____
_____/_____	_____/_____
«___»_____20__года	«___»_____20__года

Приложение №13. Доверенность на получение инициализирующей информации СКЗИ (форма)

ДОВЕРЕННОСТЬ (ФОРМА) № _____

Дата выдачи: «___»_____20__года

_____
(наименование участника информационного взаимодействия)
уполномочивает
_____
(фамилия, имя, отчество лица полностью)
паспорт серии _____ №_____ выдан
_____
_____ «___»_____ _____ г.
зарегистрированного по адресу:
_____
_____,
совершить от имени
_____
_____
(наименование участника информационного взаимодействия)
следующие действия:

1. Получить от _____,
(наименование организации-лицензиата ФСБ, обслуживающего защищенную сеть РСМЭВ)

инициализирующую информацию СКЗИ VipNet на носителе.

2. Подписать Акт приема-передачи инициализирующей информации СКЗИ VipNet, а также соответствующие документы, необходимые для исполнения поручений, определенных настоящей доверенностью *(удалить п.2 из доверенности в случае выдачи доверенности лицу, не относящемуся к перечню лиц, указанных в анкете участника защищенной сети РСМЭВ (ответственных лиц)).*

Настоящая доверенность действительна по «____» _____ 20__г.

Подпись уполномоченного представителя _____/_____

Подтверждаю:

Руководитель
_____/_____
МП

Приложение №14. Протоколы контрольной проверки СКЗИ (формы)

Протокол (Форма)
контрольной проверки
ПК «ViPNet Client»

«___» _____ 20___ г.

«ViPNet Client» установлен в _____
(наименование подразделения)
по адресу _____
в соответствии с эксплуатационно-технической документацией и введен в эксплуатацию в помещении №_____.

Акт о вводе в эксплуатацию №_____ от «___» _____ 20__ г.

Состав ПК VipNet Client:

Системный блок №_____.

Программный комплекс:

1. VipNet Client версия _____ сборка _____.
2. Дополнительное установленное оборудование (наименование, назначение, серийный номер и т.д.) указать
3. Дополнительное установленное ПО (антивирусное ПО, Прокси – сервер, ПЛ для удаленного администрирования и т.д. указать

_____
_____
_____

Состав и результаты проверок и контрольных тестов

№	Описание действий	Ожидаемый результат	Результат (+/-)	Примечания. Отметки об устранении
1	Загрузка ОС с отказом от ввода пароля ViPNet	Отказ в загрузке ОС		
2	Загрузка ОС с аутентификацией пользователя	Загрузка ОС и старт ПО ViPNet		Указать тип аутентификации
3	Проверка установленных режимов безопасности	Режимы безопасности соответствуют назначению СУ		
4	Проверка настроек ПО	Настройки ПО соответствуют требованиям ЭТД		
5	Аутентификация с паролем Администратора СУ	Переход ПО в режим работы Администратора СУ		
6	Контроль журнала событий ПО VipNet	Отсутствие попыток несанкционированного изменения режимов, настроек фильтров, отсутствие признаков НСД, аварийных завершений ПО		
7	Контроль журнала регистрации IP-пакетов	Отсутствие признаков сетевых атак, отсутствие информации о пропуске пакетов на запрещенные режимом (фильтрами) адреса (протоколы)		
8	Проверка связи с видимыми СУ защищенной сети	Наличие сообщений о доступности СУ		
9	Проверка связи с	Наличие сообщений о		

№	Описание действий	Ожидаемый результат	Результат (+/-)	Примечания. Отметки об устранении
	видимым СУ защищенной сети, для которого включен фильтр блокировки пакетов	недоступности СУ, информация в журнале о блокировании пакетов		
10	Проверка связи (ping nnn.nnn.nnn.nnn) с открытым не зарегистрированным адресом (во втором режиме)	Отсутствие ответа от узла. Информация в журнале о блокировке пакетов для данного адреса		
11	Настройка фильтра, блокирующего отдельный протокол (например, ICMP) для отдельного СУ защищенной сети, проверка соединения с СУ по данному протоколу (например, ping)	Отсутствие ответа от СУ, информация о блокировании пакетов по выбранному протоколу		
12	Настройка фильтра, запрещающего отдельный протокол (например, UDP) для всех СУ защищенной сети, проверка связи с СУ, для которого не настроено других фильтров, по данному	Наличие сообщений о недоступности СУ, информация в журнале о блокировании пакетов		

№	Описание действий	Ожидаемый результат	Результат (+/-)	Примечания. Отметки об устранении
	протоколу (например, проверка соединения)			
13	Настройка фильтра, разрешающего отдельный протокол (например, ICMP) для всех узлов открытой сети, проверка связи с любым узлом по данному протоколу (например, ping)	Наличие ответа от узла. Информация в журнале о пропуске пакетов для данного адреса		
14	Проверка связи по разрешенному протоколу для зарегистрированных открытых адресов (только для 2 режима безопасности)	Наличие соединения по данному протоколу		
15	Проверка связи по запрещенному протоколу для зарегистрированных открытых адресов	Отсутствие соединения по данному протоколу		
16	Отправка зашифрованного и подписанного письма адресатам ДП (При наличии установленного ПО ViPNet Клиент [Деловая Почта])	Отправка письма, получение квитанций о доставке (прочтении)		

№	Описание действий	Ожидаемый результат	Результат (+/-)	Примечания. Отметки об устранении
17	Контроль журналов автопроцессинга ДП (При наличии данного функционала на СУ)	Отсутствие сбоев в работе правил		

Администратор СКЗИ
(На основании договора
№____ от «___»_____20__г.)

_____/_____
«___» _____20___г.

Ответственный за защищенное взаимодействие с РСМЭВ

_____/_____
«___» _____20___г.

Протокол (Форма)

контрольной проверки

ПАК «ViPNet Coordinator HW»

«___» _____ 20___ г.

ПАК «ViPNet Coordinator HW» установлен в _____
_____
(наименование подразделения)

по адресу _____

в соответствии с эксплуатационно-технической документацией и введен в эксплуатацию в помещении №_____.

Акт о вводе в эксплуатацию №_____ от «___» _____ 20__ г.

Состав и результаты проверок и контрольных тестов

№	Описание действий	Ожидаемый результат	Результат (+/-)	Примечания. Отметки об устранении
1	Проверка состава программных и аппаратных средств	Состав и регистрационные номера аппаратных и программных средств, входящих в состав ПАК и дополнительно установленных, соответствуют акту о вводе в эксплуатацию		
2	Загрузка ОС с аутентификацией пользователя	Загрузка ОС и старт ПО ViPNet		Указать тип аутентификации
3	Проверка установленных	Режимы безопасности соответствуют		

№	Описание действий	Ожидаемый результат	Результат (+/-)	Примечания. Отметки об устранении
	режимов безопасности	назначению СУ		
4	Проверка настроек ПО	Настройки ПО соответствуют требованиям ЭТД		
5	Аутентификация с паролем Администратора СУ	Переход ПО в режим работы Администратора СУ		
6	Контроль журнала событий командного интерпретатора	Отсутствие попыток несанкционированного изменения режимов, настроек фильтров, отсутствие признаков НСД, аварийных завершений ПО		
7	Контроль журнала регистрации IP-пакетов	Отсутствие признаков сетевых атак, отсутствие информации о пропуске пакетов на запрещенные режимом (фильтрами) адреса (протоколы)		
8	Проверка связи с видимыми СУ защищенной сети	Наличие сообщений о доступности СУ		
9	Проверка связи с видимым СУ защищенной сети, для которого включен фильтр блокировки пакетов	Наличие сообщений о недоступности СУ, информация в журнале о блокировании пакетов		
10	Проверка связи (ping nnn.nnn.nnn.nnn) с открытым не зарегистрированн	Отсутствие ответа от узла. Информация в журнале о блокировке пакетов для данного адреса		

№	Описание действий	Ожидаемый результат	Результат (+/-)	Примечания. Отметки об устранении
	ым адресом			
11	Настройка фильтра, блокирующего отдельный протокол (например, ICMP) для отдельного СУ защищенной сети, проверка соединения с СУ по данному протоколу (например, ping)	Отсутствие ответа от СУ, информация о блокировании пакетов по выбранному протоколу		
12	Настройка фильтра, запрещающего отдельный протокол (например, UDP) для всех СУ защищенной сети, проверка связи с СУ, для которого не настроено других фильтров, по данному протоколу (например, проверка соединения)	Наличие сообщений о недоступности СУ, информация в журнале о блокировании пакетов		
13	Настройка фильтра, разрешающего отдельный протокол (например, ICMP)	Наличие ответа от узла. Информация в журнале о пропуске пакетов для данного адреса		

№	Описание действий	Ожидаемый результат	Результат (+/-)	Примечания. Отметки об устранении
	для всех узлов открытой сети, проверка связи с любым узлом по данному протоколу (например, ping)			
14	Проверка связи по разрешенному протоколу для зарегистрированных открытых адресов (только для 2 режима)	Наличие соединения по данному протоколу		
15	Проверка связи по запрещенному протоколу для зарегистрированных открытых адресов	Отсутствие соединения по данному протоколу		

Администратор СКЗИ
(На основании договора
№____ от «___»_____20__г.)

_____/_____
«___» _____20___г.

Ответственный за защищенное взаимодействие с РСМЭВ

_____/_____
«___» _____20___г.

Приложение №15. Акты ввода в эксплуатацию СКЗИ (формы)

УТВЕРЖДАЮ

Руководитель организации

_____/_____

«____» _____ _____ г.

Акт (ФОРМА)

о вводе в эксплуатацию ПК ViPNet Client

«___» _____ 20___ г.

Комиссия в составе: председателя комиссии _____,

членов комиссии _____

_____

и Администратора СКЗИ _____

составила акт о том, что ПК «ViPNet Client» установлен в _____

(наименование подразделения)

по адресу _____

в помещении №_____

в соответствии с эксплуатационно-технической документацией и введен в эксплуатацию.

Состав ПК «ViPNet Client»:

Системный блок № _____.

Программный комплекс:

VipNet Client версия _____сборка _____.

Дополнительное ПО (антивирусное ПО, Прокси-сервер, ПО для удаленного администрирования и т.д.) указать:

_____

_____

_____

Председатель комиссии	_____	_____	_____
	должность	Ф.И.О.	Подпись
Члены комиссии:	_____	_____	_____
	должность	Ф.И.О.	Подпись
	_____	_____	_____
	должность	Ф.И.О.	Подпись
	_____	_____	_____
	должность	Ф.И.О.	Подпись

УТВЕРЖДАЮ

Руководитель организации

_____/_____

«____» _____ _____ г.

Акт (ФОРМА)
о вводе в эксплуатацию
ПАК «ViPNet Coordinator HW»

«___» _____ 20___ г.

Комиссия в составе: председателя комиссии _____,
членов комиссии _____
_____
и Администратора ПАК «ViPNet Coordinator HW» _____ составила акт о том, что ПАК «ViPNet Coordinator HW» установлен в _____
_____
наименование подразделения

по адресу _____
в помещении №_____.
в соответствии с эксплуатационно-технической документацией и введен в эксплуатацию.

Состав ПАК «ViPNet Coordinator HW»:

Системный блок № _____, опечатан _____.
ПАК «ViPNet Coordinator HW», вариант комплектации _____ , учетный номер _____, регистрационный номер _____ .

Дополнительное оборудование (наименование, назначение, серийный номер и т. д.) указать:

_____
_____
_____

Председатель комиссии	_____	_____	_____
	должность	Ф.И.О.	Подпись
Члены комиссии:	_____	_____	_____
	должность	Ф.И.О.	Подпись
	_____	_____	_____
	должность	Ф.И.О.	Подпись
	_____	_____	_____
	должность	Ф.И.О.	Подпись

Приложение №16. Справка о проведенном контроле (форма)

СПРАВКА (Форма)

_____

(наименование участника информационного взаимодействия)

о проведенном контроле соответствия требованиям информационной безопасности

защищенной сети передаче данных РСМЭВ Кировской области

Информируем Вас о том, что в целях реализации контроля соответствия требованиям информационной безопасности защищенной сети передачи данных РСМЭВ Кировской области нами были проведены следующие мероприятия:

1. Актуализированы сведения о назначении ответственных лиц по вопросам обеспечения защищенного взаимодействия с РСМЭВ;

2. Проверено соблюдение условий эксплуатации и работоспособность средств криптографической защиты информации, средств защиты информации, технических средств Универсальных АРМ.

3. Проверено соответствие реализуемого подключения Универсальных АРМ требованиям информационной безопасности.

_____

(наименование участника информационного взаимодействия)

соблюдает обязательства по обеспечению защищенного взаимодействия с РСМЭВ и несет ответственность за качество их выполнения.

Состояние актуальности сведений:

Наименование документа	Дата последнего предоставления	Наличие изменений
Анкета Участника информационного взаимодействия	__.__.20__	
Копия приказа о назначении лица, ответственного за осуществление защищенного взаимодействия в РСМЭВ	__.__.20__	
Перечень сведений для подключения к сети передачи данных для схемы № ____	__.__.20__	

В целях обеспечения актуальности сведений прилагаем документы, содержащие изменения, относительно последнего предоставления, а также документы, подтверждающие результаты контроля:

1. Протокол оценки соответствия _____
(наименование участника информационного взаимодействия)
требованиям информационной безопасности для схемы № ___ – на __ листах в __ экз.

2. Анкета _____
(наименование участника информационного взаимодействия)
– на __ листах в __ экз.;

3. Копия приказа о назначении лица, ответственного за осуществление защищенного взаимодействия _____
_____
(наименование участника информационного взаимодействия)
в РСМЭВ – на __ листах в __ экз;

4. Перечень сведений для подключения к сети передачи данных для схемы № схемы – на __ листах в __ экз.

Ответственность за достоверность предоставляемых сведений оставляю за собой.

Руководитель _____/_____

М.П.

Приложение №17. Типовая форма акта уничтожения ключевой информации

Акт № ____

уничтожения ключевой информации

г._____ «____» _____ 20 __ года

В связи с ___

_____

(истечение срока действия, плановая смена ключей, смена должностных обязанностей пользователя и т.д.)

Комиссия в составе:

Председателя:

_____

(должность, ФИО)

И членов комиссии: _____

(должность, ФИО)

_____

(должность, ФИО)

_____

(должность, ФИО)

составила настоящий акт уничтожения ключевой информации, указанной в таблице, путем

_____

(стирания ключевой информации без повреждения носителя или физического уничтожения ключевого носителя)

Тип ключевого носителя	Учетный №	Экз. №	Имя файла

Настоящий акт составлен в 2 экземплярах на 1 листе каждый.

_____	_____	_____
(должность)	(подпись)	(ФИО)
_____	_____	_____
(должность)	(подпись)	(ФИО)
_____	_____	_____
(должность)	(подпись)	(ФИО)
_____	_____	_____
(должность)	(подпись)	(ФИО)