



АДМИНИСТРАЦИЯ СМОЛЕНСКОЙ ОБЛАСТИ

ПОСТАНОВЛЕНИЕ

от 20.07.2015 № 424

О порядке использования распределенной мультисервисной сети связи и передачи данных органов исполнительной власти Смоленской области и органов местного самоуправления муниципальных образований Смоленской области

В соответствии с частью 2 статьи 15 Федерального закона «Об информации, информационных технологиях и о защите информации», в целях обеспечения информационной безопасности органов исполнительной власти Смоленской области и оптимизации доступа к информационным, программным и аппаратным ресурсам распределенной мультисервисной сети связи и передачи данных органов исполнительной власти Смоленской области и органов местного самоуправления муниципальных образований Смоленской области

Администрация Смоленской области п о с т а н о в л я е т:

1. Утвердить прилагаемое Положение о распределенной мультисервисной сети связи и передачи данных органов исполнительной власти Смоленской области и органов местного самоуправления муниципальных образований Смоленской области (далее также – Положение).

2. Определить Департамент Смоленской области по информационным технологиям оператором распределенной мультисервисной сети связи и передачи данных органов исполнительной власти Смоленской области и органов местного самоуправления муниципальных образований Смоленской области.

3. Руководителям органов исполнительной власти Смоленской области и подведомственных им организаций в срок до 1 июня 2016 года осуществить регистрацию в качестве абонента распределенной мультисервисной сети связи и передачи данных органов исполнительной власти Смоленской области и органов

местного самоуправления муниципальных образований Смоленской области в соответствии с Положением.

4. Рекомендовать руководителям органов местного самоуправления муниципальных образований Смоленской области и подведомственных им организаций в срок до 1 июня 2016 года осуществить регистрацию в качестве абонента распределенной мультисервисной сети связи и передачи данных органов исполнительной власти Смоленской области и органов местного самоуправления муниципальных образований Смоленской области в соответствии с Положением.

5. Признать утратившими силу:

- постановление Администрации Смоленской области от 14.04.2004 № 125 «Об упорядочивании доступа в сеть «Интернет» через Интернет-сервер Администрации Смоленской области»;

- постановление Администрации Смоленской области от 19.05.2008 № 304 «О внесении изменений в Положение о порядке предоставления и использования доступа в сеть «Интернет» через Интернет-сервер Администрации Смоленской области»;

- постановление Администрации Смоленской области от 22.04.2010 № 195 «О внесении изменений в Положение о порядке предоставления и использования доступа в сеть «Интернет» через Интернет-сервер Администрации Смоленской области».

Временно исполняющий обязанности
Губернатора Смоленской области

А.В. Островский

УТВЕРЖДЕНО
постановлением Администрации
Смоленской области
от 20.07.2015 № 424

ПОЛОЖЕНИЕ
о распределенной мультисервисной сети связи и передачи данных
органов исполнительной власти Смоленской области и органов местного
самоуправления муниципальных образований Смоленской области

1. Общие положения

1.1. Настоящее Положение определяет структуру и состав распределенной мультисервисной сети связи и передачи данных органов исполнительной власти Смоленской области и органов местного самоуправления муниципальных образований Смоленской области (далее – РМС СО), содержание и порядок использования РМС СО, условия и порядок подключения органов исполнительной власти Смоленской области, органов местного самоуправления муниципальных образований Смоленской области, иных органов государственной власти и организаций к РМС СО, размещения информационных систем в РМС СО и обеспечения их безопасности.

1.2. В целях настоящего Положения используются следующие понятия:

оператор РМС СО - уполномоченный орган исполнительной власти Смоленской области, определенный актом Администрации Смоленской области;

абонент РМС СО - орган исполнительной власти Смоленской области, орган местного самоуправления муниципального образования Смоленской области, государственные (муниципальные) организации и учреждения, иные органы государственной власти и организации, имеющие подключение к центральному телекоммуникационному узлу РМС СО;

администратор РМС СО - назначенное оператором РМС СО лицо, осуществляющее управление и (или) эксплуатацию РМС СО;

администратор локальной вычислительной сети абонента РМС СО - лицо, осуществляющее управление локальной вычислительной сетью абонента РМС СО и доступ пользователей к работе в РМС СО;

информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств, размещаемых в РМС СО;

оператор информационной системы - абонент РМС СО, осуществляющий деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных;

пользователь РМС СО - физическое лицо, пользующееся услугами РМС СО для получения информации или решения служебных задач;

информационный ресурс - организованная совокупность документированной информации, включающая в себя базы и банки данных, другие массивы информации в информационных системах;

участники РМС СО - абоненты РМС СО, оператор РМС СО, администраторы РМС СО, администраторы локальных вычислительных сетей абонентов РМС СО, пользователи РМС СО;

участники межсетевого взаимодействия – органы исполнительной власти Смоленской области, подведомственные им учреждения, органы местного самоуправления муниципальных образований Смоленской области и иные органы государственной власти, имеющие собственную защищенную (VPN) сеть;

поставщики (подрядчики, исполнители) - участники контрактной системы в сфере закупок товаров, работ, услуг для обеспечения государственных или муниципальных нужд;

несанкционированный доступ к информации (далее - НСД) - доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

1.3. РМС СО предназначена для:

- осуществления информационного взаимодействия, в том числе юридически значимого, между абонентами РМС СО;
- формирования и использования информационных ресурсов;
- предоставления информационных ресурсов в совместное пользование определенным абонентам РМС СО для более эффективного выполнения служебных задач;
- проведения единой политики в сфере информационных технологий и безопасности информации всеми участниками РМС СО.

2. Структура и состав РМС СО

2.1. РМС СО представляет собой территориально распределенную информационно-телекоммуникационную сеть, включающую в себя совокупность каналов связи, маршрутизирующего и сервисного оборудования, узлов доступа к сети, серверного оборудования, рабочих станций, терминального и другого оборудования, предназначенного для обработки и передачи информации.

2.2. В состав РМС СО входят следующие компоненты:

2.2.1. Центральный телекоммуникационный узел связи, включающий в себя:

- серверы центрального телекоммуникационного узла связи;
- административно-технический сетевой сегмент;
- узел доступа к сети общего пользования «Интернет».

2.2.2. Вычислительный комплекс обработки данных Департамента Смоленской области по информационным технологиям.

2.2.3. Узлы доступа к РМС СО, обеспечивающие подключение абонентов РМС СО к центральному телекоммуникационному узлу связи.

2.2.4. Каналы связи, обеспечивающие соединение центрального телекоммуникационного узла связи и узлов доступа к РМС СО.

2.2.5. Серверное оборудование абонентов РМС СО и рабочие станции пользователей РМС СО, непосредственно подключенные к узлам доступа к РМС СО.

2.2.6. Информационные ресурсы РМС СО.

2.3. Для подключения абонентов РМС СО на технологических площадках абонентов РМС СО организованы узлы доступа к РМС СО. Подключение узлов доступа к РМС СО осуществляется через выделенные линии связи, мультисервисные сети операторов связи или с помощью коммутируемых линий связи.

2.4. Для подключения пользователей РМС СО и серверного оборудования абонентов РМС СО к узлам доступа используется инфраструктура локальных вычислительных сетей.

2.5. Информационные ресурсы РМС СО включают в себя:

- информационные системы общего назначения;
- информационные системы абонентов РМС СО, предоставленные для совместного использования в рамках РМС СО;
- информационные системы абонентов РМС СО, имеющие подключение к РМС СО, но не предназначенные для совместного использования;
- устройства и средства информационного взаимодействия и защиты информации.

2.6. К информационным системам общего назначения относятся информационные системы, обеспечивающие информационное взаимодействие и предоставляющие информационные сервисы пользователям, а также системы информационного обеспечения деятельности абонентов РМС СО. Ограничения по доступу к указанным ресурсам определяются оператором РМС СО.

2.7. Ответственность за обеспечение проведения мероприятий по защите и формированию информационных систем общего назначения возлагается на оператора РМС СО.

2.8. Ответственность за обеспечение проведения мероприятий по защите и формированию информационных систем абонентов РМС СО возлагается на руководителей абонентов РМС СО.

2.9. Общее руководство процессами развития и формирования РМС СО и информационных ресурсов РМС СО осуществляет оператор РМС СО.

3. Порядок подключения абонентов РМС СО

3.1. Для подключения абонентов РМС СО оператором РМС СО создаются точки доступа следующих типов:

3.1.1. Постоянное соединение по физической линии или предоставленному оператором связи выделенному каналу связи.

3.1.2. Удаленный доступ по открытым каналам связи с использованием средств криптографической защиты информации.

3.2. Оператор РМС СО устанавливает организационные и (или) технические требования к:

- узлам доступа к РМС СО, обеспечивающим подключение абонентов РМС СО;
- локальным вычислительным сетям абонентов РМС СО;

- рабочим станциям пользователей РМС СО, непосредственно подключаемым к узлам доступа к РМС СО;
- порядку доступа и работы в РМС СО поставщиков (подрядчиков, исполнителей).

3.3. Для подключения к РМС СО руководитель абонента РМС СО распорядительным актом назначает лицо, ответственное за работу абонента РМС СО в РМС СО, с возложением на него обязанностей по:

- сбору и оформлению заявки на подключение к РМС СО;
- организации работы пользователей локальной вычислительной сети абонента РМС СО;
- организации взаимодействия с оператором РМС СО по вопросам эксплуатации подключенного к РМС СО сегмента локальной вычислительной сети абонента РМС СО.

3.4. В адрес оператора РМС СО от абонента РМС СО направляется заявка на подключение к РМС СО, в состав которой входят:

- данные о полном наименовании абонента РМС СО;
- данные о месте нахождения абонента РМС СО;
- данные об основных направлениях деятельности абонента РМС СО;
- обоснование необходимости подключения к РМС СО.

3.5. Заявка на подключение к РМС СО областных государственных учреждений и предприятий согласовывается с органом исполнительной власти Смоленской области, координирующем соответствующее направление деятельности.

3.6. К заявке на подключение к РМС СО прилагаются:

3.6.1. Копия распорядительного акта абонента РМС СО о назначении лица, ответственного за работу абонента РМС СО в РМС СО.

3.6.2. Информация о подключаемом сегменте локальной вычислительной сети абонента РМС СО, включающая в себя:

- адрес точки подключения к РМС СО;
- графическую схему подключаемого сегмента локальной вычислительной сети заявителя с отображением всех подключенных устройств, линий связи между ними и используемых средств защиты информации;
- перечень используемого активного оборудования и его краткие характеристики;
- общее количество подключенных серверов и рабочих станций;
- используемый диапазон IP-адресов;
- имеющиеся в сегменте сети информационные системы с разделением на общедоступные и ограниченного доступа.

3.6.3. Описание и схема подключения локальной вычислительной сети абонента РМС СО к внешним сетям, в том числе к сети общего пользования «Интернет».

3.6.4. Перечень программных и технических средств обеспечения безопасности информации с указанием типа и наименования используемых средств (средства антивирусной защиты, средства защиты от НСД, межсетевые экраны,

анализаторы атак и другие), а также сведений о наличии сертификата соответствия требованиям по защите информации.

3.6.5. Информация о наличии физической охраны средств вычислительной техники и носителей информации.

3.7. Поступившая заявка на подключение к РМС СО регистрируется оператором РМС СО в день поступления в интегрированной системе электронного документооборота и архива Администрации Смоленской области и органов исполнительной власти Смоленской области. Оператор РМС СО в течение 20 рабочих дней рассматривает поступившие заявки на подключение к РМС СО и выносит решение о возможности или невозможности подключения к РМС СО.

3.8. В случае принятия решения о возможности подключения к РМС СО оператор РМС СО в течение 5 рабочих дней направляет в адрес абонента РМС СО технические условия подключения к РМС СО и в случае необходимости оценку затрат на финансирование мероприятий по организации подключения.

3.9. Абонент РМС СО самостоятельно либо с привлечением администратора РМС СО осуществляет мероприятия по выполнению технических условий подключения к РМС СО.

3.10. В течение 5 рабочих дней после выполнения технических условий оператор РМС СО и абонент РМС СО заключают соглашение о подключении абонента РМС СО к РМС СО (далее также – соглашение).

3.11. Доступ к информационным ресурсам РМС СО предоставляется администратором РМС СО в течение 5 рабочих дней после подписания соглашения.

Выполнение данных работ подтверждается актом подключения, подписанным абонентом РМС СО и администратором РМС СО, который хранится у оператора РМС СО.

3.12. В случае принятия решения о невозможности подключения к РМС СО оператор РМС СО информирует заявителя о данном решении в течение 2 рабочих дней со дня его принятия с указанием мотивированной причины отказа.

3.13. Решение о невозможности подключения к РМС СО принимается по следующим основаниям:

- наличие в заявке на подключение к РМС СО недостоверных либо неполных сведений, предусмотренных пунктами 3.4 и 3.6 настоящего Положения;
- отсутствие у оператора РМС СО технической возможности предоставления доступа;
- отсутствие у абонента РМС СО технической возможности выполнения технических условий подключения к РМС СО;
- доступ абонента РМС СО к РМС СО был прекращен оператором РМС СО в соответствии с пунктом 4.1 настоящего Положения и абонент РМС СО не устранил нарушения, ставшие причиной прекращения доступа.

4. Прекращение доступа абонента РМС СО к РМС СО

4.1. Прекращение доступа абонента РМС СО к РМС СО осуществляется оператором РМС СО по собственной инициативе в одностороннем порядке в случае неоднократного (два и более) в течение одного квартала нарушения абонентом

РМС СО требований настоящего Положения (при наличии письменного уведомления оператора РМС СО о выявлении нарушения), если такие нарушения не были устранены абонентом РМС СО в указанные в уведомлении сроки.

4.2. Прекращение доступа абонента РМС СО к РМС СО осуществляется оператором РМС СО по заявке абонента РМС СО в случае прекращения необходимости доступа к РМС СО.

4.3. О прекращении доступа оператор РМС СО письменно уведомляет абонента РМС СО не позднее рабочего дня, следующего за днем прекращения доступа к сети.

4.4. Возобновление доступа абонента РМС СО к РМС СО производится в порядке, определенном разделом 3 настоящего Положения.

5. Регистрация пользователей РМС СО. Доступ к информационным системам. Назначение доступа к ресурсам РМС СО

5.1. Состав пользователей РМС СО, их права и возможность доступа к информационным системам общего назначения и сети общего пользования «Интернет» устанавливаются администратором РМС СО на основании заявки абонента РМС СО.

5.2. При подключении нового пользователя к РМС СО лицом, ответственным за работу абонента РМС СО в РМС СО, производится подготовка компьютера пользователя путем:

- отключения от телекоммуникационных сетей общего пользования;
- настройки BIOS компьютера, исключающей возможность загрузки с внешних носителей, несанкционированного доступа к настройкам BIOS, использования встроенных адаптеров Wi-Fi и модемов;
- установки и актуализации сертифицированного антивирусного программного обеспечения;
- выполнения полной проверки компьютера средствами антивирусной защиты;
- установки критических обновлений операционной системы (согласно рекомендациям разработчика операционной системы);
- настройки операционной системы, исключающей возможность изменения состава и конфигурации программных и технических средств компьютера без санкции администратора локальной вычислительной сети абонента РМС СО;
- настройки сетевых параметров (присвоения компьютеру IP-адреса с указанием шлюза, DNS-серверов, прокси-сервера либо установки автоматических параметров);
- исключения пользователя из состава локальных администраторов подключаемого в РМС СО компьютера, за исключением случаев, согласованных с оператором РМС СО.

5.3. Пользователь РМС СО должен иметь доступ только к тем информационным ресурсам, которые разрешены для него.

5.4. Пользователь РМС СО должен иметь уникальный идентификатор и пароль, а в случае использования криптографических средств защиты информации - ключи шифрования для криптографических средств, используемых для защиты

информации при передаче ее по каналам связи и хранения, а также для систем электронной подписи. При этом пользователи РМС СО должны нести ответственность за сохранность своих идентификаторов и паролей.

5.5. По решению оператора РМС СО для идентификации пользователей РМС СО может использоваться Единая система идентификации и аутентификации.

5.6. Пользователи РМС СО несут персональную ответственность за нарушения порядка автоматизированной обработки информации, правил хранения, использования и передачи находящихся в их распоряжении защищаемых ресурсов системы.

6. Порядок размещения информационных ресурсов в РМС СО

6.1. Информационные системы абонентов РМС СО размещаются в РМС СО на основании поданной оператору РМС СО в произвольной форме заявки на размещение информационного ресурса.

6.2. К заявке на размещение информационного ресурса прилагаются:

- сведения о необходимых вычислительных мощностях, типе операционной системы и предустановленном общесистемном программном обеспечении;
- согласованный с оператором РМС СО порядок подключения пользователей РМС СО к информационной системе, в котором определяются оператор информационной системы, основные пользователи, цели функционирования, режимы функционирования, порядок предоставления доступа к информационной системе, вопросы защиты от несанкционированного доступа, вопросы защиты программно-аппаратного комплекса информационной системы от потери либо несанкционированного изменения содержащихся в ней данных и вопросы антивирусной защиты;
- сведения об оцениваемом среднем объеме переданной и принятой информации одним пользователем информационной системы в течение рабочего дня для оценки нагрузки;
- сведения о категории доступа к информации, обрабатываемой в информационной системе;
- в случаях, предусмотренных федеральным законодательством, сведения о классификации информационной системы по требованиям защиты информации.

6.3. Оператор РМС СО изучает поступившие заявки на размещение информационного ресурса и регистрирует их в день поступления в интегрированной системе электронного документооборота и архива Администрации Смоленской области и органов исполнительной власти Смоленской области. Оператор РМС СО рассматривает указанные заявки в течение 20 рабочих дней со дня их поступления и принимает решение о размещении информационной системы в РМС СО либо об отказе в размещении информационной системы в РМС СО.

6.4. Решение об отказе в размещении информационной системы в РМС СО принимаются по следующим основаниям:

- наличие в заявке недостоверных либо неполных сведений, предусмотренных пунктом 6.2 настоящего Положения;

- отсутствие у оператора РМС СО технической возможности для размещения информационной системы в РМС СО;

- доступ абонента РМС СО к РМС СО был прекращен оператором РМС СО в соответствии с пунктом 4.1 настоящего Положения и абонент РМС СО не устранил нарушения, ставшие причиной прекращения доступа;

- работа информационной системы в РМС СО была прекращена оператором РМС СО по собственной инициативе и абонент РМС СО не устранил нарушения, ставшие причиной прекращения работы информационной системы.

6.5. Оператор РМС СО в течение 5 рабочих дней со дня принятия решения о размещении информационной системы в РМС СО информирует заявителя письменно о принятом решении. Одновременно с этим администратор РМС СО размещает информационную систему в РМС СО.

6.6. В случае принятия решения об отказе в размещении информационной системы в РМС СО оператор РМС СО информирует абонента РМС СО, подавшего заявку, о данном решении в течение 2 рабочих дней со дня его принятия с указанием мотивированной причины отказа.

6.7. Прекращение работы информационной системы в РМС СО осуществляется оператором РМС СО в следующих случаях:

- по собственной инициативе в одностороннем порядке в случае неоднократного (два и более) в течение одного квартала нарушения абонентом РМС СО требований настоящего Положения (при наличии письменного уведомления оператора РМС СО о выявлении нарушения), если такие нарушения не были устранены абонентом РМС СО в указанные в уведомлении сроки;

- по заявке оператора информационной системы в случае прекращения необходимости в размещении информационной системы в РМС СО.

6.8. О прекращении работы информационной системы оператор РМС СО письменно сообщает абоненту РМС СО не позднее рабочего дня, следующего за днем прекращения работы.

7. Обязанности участников РМС СО

7.1. Оператор РМС СО обязан:

7.1.1. Разрабатывать правила формирования, развития и работы РМС СО.

7.1.2. Осуществлять контроль соблюдения настоящего Положения.

7.1.3. Разрабатывать предложения по внесению изменений в настоящее Положение.

7.1.4. Разрабатывать предложения по формированию и внедрению компонентов РМС СО.

7.1.5. Обеспечивать техническое управление комплексом РМС СО.

7.1.6. Обеспечивать управление узлом доступа к информационно-телекоммуникационной сети «Интернет».

7.1.7. Обеспечивать разработку и внедрение прикладных программных приложений, функционирующих в интересах всех участников РМС СО.

7.1.8. Организовывать закупку услуг передачи данных в целях функционирования РМС СО, за исключением абонентов РМС СО, которые закупают такие услуги самостоятельно.

7.1.9. Информировать руководителей абонентов РМС СО о невыполнении их сотрудниками настоящего Положения.

7.1.10. Отключать участников РМС СО от телекоммуникационного узла в случае выявления деятельности, нарушающей настоящее Положение.

7.1.11. Вносить предложения по модернизации и развитию РМС СО.

7.1.12. Обеспечивать процесс подключения абонентов к РМС СО.

7.1.13. Обеспечивать пользователям РМС СО предоставление и аннулирование доступа к РМС СО и информационным системам общего назначения.

7.1.14. Обеспечивать размещение информационных систем в РМС СО.

7.1.15. Обеспечивать осуществление межсетевого взаимодействия.

7.1.16. Обеспечивать мониторинг состояния уровня защищенности ресурсов РМС СО в соответствии с законодательством Российской Федерации, руководящими документами Федеральной службы безопасности Российской Федерации и Федеральной службы по техническому и экспортному контролю.

7.1.17. Обеспечивать процесс внедрения и эксплуатации РМС СО.

7.1.18. Обеспечивать контроль состояния технических средств магистрали сети, телекоммуникационных узлов и их соединения с другими сетями.

7.1.19. Обеспечивать услуги системы межведомственного электронного документооборота и делопроизводства, электронной почты, видеоконференций, других телематических служб.

7.1.20. Обеспечивать возможность администрирования информационных систем, размещенных в РМС СО, операторам информационных систем.

7.1.21. Обеспечивать целостность файловой системы серверов центрального телекоммуникационного узла.

7.1.22. Обеспечивать защиту информации в РМС СО.

7.2. Администраторы РМС СО обязаны:

7.2.1. Выполнять требования настоящего Положения, а также правила работы в РМС СО, принятые в рамках исполнения своих обязанностей оператором РМС СО.

7.2.2. Осуществлять непосредственное управление режимами работы РМС СО.

7.2.3. Осуществлять техническую поддержку работоспособности компонентов РМС СО.

7.2.4. Осуществлять мероприятия по обеспечению информационной безопасности компонентов РМС СО.

7.2.5. Обеспечивать работоспособность компьютерного и коммутационного оборудования центрального узла РМС СО.

7.2.6. Осуществлять мероприятия по модернизации и развитию РМС СО.

7.2.7. Предоставлять абонентам РМС СО по мотивированным заявкам необходимые сервисные функции РМС СО.

7.2.8. Информировать администраторов локальной вычислительной сети абонентов РМС СО о правилах формирования, развития и работы РМС СО и

последствиях их нарушения, о проводимых работах по обслуживанию РМС СО, возможных перебоях в ее работе.

7.3. В обязанности администраторов РМС СО не входит:

7.3.1. Контролировать содержание проходящих по сети данных.

7.3.2. Контролировать данные, находящиеся на рабочих станциях в локальных вычислительных сетях абонентов РМС СО.

7.3.3. Обеспечивать работоспособность вычислительных сетей абонентов РМС СО.

7.4. Администраторы локальных вычислительных сетей абонентов РМС СО обязаны:

7.4.1. Выполнять требования настоящего Положения, а также правила работы в РМС СО, принятые в рамках исполнения своих обязанностей оператором РМС СО.

7.4.2. Обеспечивать подключение сегмента локальной вычислительной сети абонента РМС СО к РМС СО.

7.4.3. Осуществлять мероприятия по обеспечению информационной безопасности компонентов РМС СО абонента РМС СО.

7.4.4. Устанавливать ограничения по паролям, рабочим станциям, с которых разрешена регистрация, по времени работы, объемам доступного дискового пространства, правам доступа к каталогам и файлам с учетом правил формирования, развития и работы РМС СО.

7.4.5. Принимать меры по пресечению несанкционированного доступа к компонентам РМС СО со стороны пользователей, уведомлять руководителя абонента РМС СО о случаях нарушений и принятых мерах.

7.4.6. Сообщать непосредственному руководителю, администратору РМС СО и оператору РМС СО о действиях пользователей, осуществивших несанкционированный доступ к защищаемым ресурсам РМС СО или нарушивших другие требования настоящего Положения.

7.4.7. Представлять администратору РМС СО предложения, касающиеся разработки правил формирования, при наличии таких предложений или по запросу администратора РМС СО, развития и работы РМС СО, после соответствующего согласования с руководителем абонента РМС СО.

7.4.8. Направлять в адрес администраторов РМС СО информацию об изменениях имеющихся в их распоряжении компонентов сегмента локальной вычислительной сети абонента РМС СО, подключенного к РМС СО.

7.5. Пользователи РМС СО обязаны:

7.5.1. Выполнять требования настоящего Положения, а также правила работы в РМС СО, принятые в рамках исполнения своих обязанностей оператором РМС СО.

7.5.2. При сообщениях тестовых программ о появлении вредоносных или потенциально опасных объектов или при обнаружении подозрительных действий немедленно доложить об этом администратору локальной вычислительной сети абонента РМС СО и прекратить работу в РМС СО.

7.5.3. Сохранять свою учетную запись и пароль для работы в РМС СО в тайне и не допускать к подключенной в РМС СО рабочей станции посторонних лиц.

7.5.4. Исключить возможность бесконтрольного использования рабочей станции, подключенной к РМС СО.

7.5.5. Пользоваться информационными системами РМС СО в соответствии с настоящим Положением и федеральным законодательством.

7.5.6. Обращаться к своему руководителю для решения вопросов об использовании информационных систем другого абонента РМС СО, доступ к которым предоставляется посредством РМС СО.

7.5.7. Обращаться к администратору локальной вычислительной сети абонента РМС СО в случае возникновения проблем с доступностью и работоспособностью информационных ресурсов.

7.6. При работе участников РМС СО в РМС СО не допускается:

7.6.1. Распространение и представление информации, не связанной с исполнением полномочий участников РМС СО, за исключением случаев, предусмотренных федеральным законодательством.

7.6.2. Обработка и распространение с использованием РМС СО информации, содержащей сведения, составляющие государственную тайну.

7.6.3. Распространение и представление информации, которая направлена на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды, а также иной информации, за распространение которой предусмотрена уголовная или административная ответственность.

7.6.4. Осуществление действий, направленных на получение несанкционированного доступа, в том числе привилегированного, к информационным системам, компьютерам пользователей и другому оборудованию, последующее использование такого доступа, а также уничтожение или модификация программного обеспечения или данных, не принадлежащих пользователю, без согласования с их владельцами либо участие в сетевых атаках и сетевом взломе.

7.6.5. Осуществление действий, направленных на нарушение нормального функционирования компонентов РМС СО (компьютеров, другого оборудования или программного обеспечения).

7.6.6. Передача в РМС СО бессмысленной или бесполезной информации, создающей «паразитную» нагрузку на компьютеры или оборудование, а также на саму сеть в объемах, превышающих минимально необходимые для проверки связности и доступности отдельных ее элементов.

7.6.7. Фальсификация адресов, используемых в сетевых протоколах, при передаче данных в РМС СО, использование несуществующих обратных адресов при отправке электронных писем.

7.6.8. Подключение к РМС СО и использование беспроводных точек доступа, за исключением случаев, согласованных с оператором РМС СО при заключении соглашения.

7.6.9. Подключение компонентов РМС СО к сторонним сетям, в том числе с использованием мобильных устройств, за исключением случаев, согласованных с оператором РМС СО при заключении соглашения.

8. Требования при предоставлении доступа к РМС СО поставщикам (подрядчикам, исполнителям).

8.1. Предоставление доступа к РМС СО поставщикам (подрядчикам, исполнителям) осуществляется в случаях:

8.1.1. Наличия действующего государственного контракта на выполнение работ и оказание услуг, для исполнения которого требуется доступ к РМС СО.

8.1.2. Наличие обоснованной заявки на подключение поставщика (подрядчика, исполнителя) к РМС СО от органа исполнительной власти Смоленской области, выступающего заказчиком выполнения работ или оказания услуг.

8.2. Предоставление доступа к РМС СО поставщикам (подрядчикам, исполнителям) осуществляется при выполнении следующих условий:

8.2.1. Для передачи информации по каналам связи должны использоваться защищенные каналы связи, в том числе защищенные волоконно-оптические линии связи, или предназначенные для этого криптографические средства защиты информации класса не ниже КС2. Применяемые при этом средства защиты информации должны быть сертифицированы Федеральной службой безопасности Российской Федерации.

8.2.2. Подключение информационных систем сторонних организаций к РМС СО должно осуществляться с использованием межсетевого экрана, требования к которому определяются руководящим документом Федеральной службы по техническому и экспортному контролю «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации».

8.2.3. Наличие у поставщика (подрядчика, исполнителя) должностного лица, ответственного за обеспечение безопасности информации.

8.3. Поставщик (подрядчик, исполнитель), подключаемый к РМС СО, должен заключить соглашение с оператором РМС СО, в котором указаны условия подключения, требования по защите информации, перечень ресурсов РМС СО, к которым разрешен доступ работникам поставщика (подрядчика, исполнителя), и срок предоставления доступа к РМС СО.

8.4. На этапе эксплуатации работниками поставщика (подрядчика, исполнителя) должны строго соблюдаться все требования и инструкции по работе в РМС СО и требования по обеспечению защиты информации.

8.5. Срок предоставления доступа к РМС СО поставщику (подрядчику, исполнителю) ограничивается сроком обеспечения государственных или муниципальных нужд Смоленской области и не должен превышать срок, установленный государственным контрактом и гарантийными обязательствами, требующимися для его исполнения, или 1 год.

9. Осуществление межсетевого взаимодействия

При необходимости организации взаимодействия с VPN-сетями органов исполнительной власти Смоленской области, подведомственных им учреждений и предприятий, органов местного самоуправления муниципальных образований

Смоленской области и иных органов государственной власти абоненты РМС СО, являющиеся участниками межсетевого взаимодействия, по согласованию с оператором РМС СО заключают соглашение о межсетевом взаимодействии.

10. Организация доступа к сети общего пользования «Интернет»

10.1. Абоненты РМС СО обязаны организовывать подключение к сети общего пользования «Интернет» только через централизованный и защищенный канал оператора РМС СО, если другое не определено соглашением о подключении абонента РМС СО к РМС СО.

10.2. Подключение РМС СО к сети общего пользования «Интернет» должно осуществляться через средства разграничения доступа в виде межсетевых экранов. Не допускается подключение к сети общего пользования «Интернет» в обход межсетевого экрана. Межсетевые экраны должны быть сертифицированы по требованиям безопасности информации.

10.3. Для выполнения задач, связанных с исполнением служебных обязанностей, пользователям РМС СО предоставляется доступ к ресурсам сети общего пользования «Интернет». Доступ к ресурсам сети общего пользования «Интернет» в других целях запрещен.

10.4. Доступ пользователей РМС СО к сети общего пользования «Интернет» осуществляется с соблюдением требований настоящего Положения и федерального законодательства в области защиты информации посредством прокси-сервера. Прокси-сервер должен быть сертифицирован по требованиям безопасности информации.

10.5. Оператор РМС СО имеет право ограничивать доступ к ресурсам сети общего пользования «Интернет», содержание которых не имеет отношения к исполнению пользователями РМС СО служебных обязанностей, а также к ресурсам, содержание и направленность которых запрещены международным и российским законодательством.

10.6. При работе с ресурсами сети общего пользования «Интернет» недопустимы:

- разглашение сведений конфиденциального характера, ставших известными пользователю РМС СО по служебной необходимости либо иным путем;
- распространение защищенных авторскими правами материалов, затрагивающих патент, торговую марку, коммерческую тайну, копирайт или иные права собственности и/или авторские и смежные права третьей стороны;
- публикация, загрузка и распространение материалов, содержащих вирусы или другие компьютерные коды, файлы или программы, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или телекоммуникационного оборудования или программ, для осуществления несанкционированного доступа, а также серийные номера к коммерческим программным продуктам и программы для их генерации, логины, пароли и прочие средства для получения несанкционированного доступа к платным ресурсам сети «Интернет», а также размещения ссылок на вышеуказанную информацию;

- ведение служебной переписки с использованием бесплатных почтовых сервисов.

10.7. При работе с ресурсами сети общего пользования «Интернет» запрещено:

- загружать и запускать файлы без предварительной проверки средством антивирусной защиты на наличие вредоносного кода (компьютерного вируса);
- использовать анонимные прокси-серверы;
- использовать программные и аппаратные средства, позволяющие получить доступ к ресурсу сети общего пользования «Интернет», запрещенному к использованию оператором РМС СО.

11. Контроль за обеспечением информационной безопасности РМС СО

11.1. Контроль за обеспечением информационной безопасности РМС СО осуществляется с целью своевременного выявления и предотвращения утечки информации по техническим каналам, несанкционированного доступа к ней, преднамеренных программно-технических воздействий на информацию и оценки эффективности ее защиты.

11.2. Контроль заключается в проверке выполнения участниками РМС СО законодательства Российской Федерации по вопросам защиты информации, решений Федеральной службы по техническому и экспортному контролю, требований настоящего Положения, а также в оценке обоснованности и эффективности принятых мер защиты информации.

11.2.1. Контроль за обеспечением информационной безопасности РМС СО осуществляют:

- оператор РМС СО;
- абонент РМС СО в части обеспечения информационной безопасности подключенного к РМС СО сегмента локальной вычислительной сети абонента РМС СО;
- федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации, в пределах своей компетенции.

11.2.2. Контроль за обеспечением информационной безопасности в РМС СО проводится:

- оператором РМС СО не реже одного раза в год;
- абонентом РМС СО не реже одного раза в полгода.

11.3. По решению оператора РМС СО для проведения работ по контролю за обеспечением информационной безопасности РМС СО могут привлекаться специализированные организации, имеющие лицензии на право проведения работ в области защиты информации.

11.4. Обеспечение информационной безопасности в РМС СО считается эффективным, если принимаемые меры соответствуют установленным требованиям или нормам по защите информации. Несоответствие мер установленным требованиям или нормам по защите информации является нарушением.