



ПОСТАНОВЛЕНИЕ



от 16 апреля 2012 года

№ 169

г. Ижевск

Об утверждении Положения о Единой защищенной сети передачи данных государственных органов Удмуртской Республики

Пурхонен А. А.
Ермаков С. П.

В целях реализации Федерального закона от 27 июля 2010 года № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», обеспечения функционирования региональной системы межведомственного электронного взаимодействия в Удмуртской Республике **Правительство Удмуртской Республики ПОСТАНОВЛЯЕТ:**

1. Утвердить прилагаемое Положение о Единой защищенной сети передачи данных государственных органов Удмуртской Республики (далее - Положение).

2. Определить:

Министерство информатизации и связи Удмуртской Республики оператором Единой защищенной сети передачи данных государственных органов Удмуртской Республики;

бюджетное учреждение Удмуртской Республики «Ресурсный информационный центр Удмуртской Республики» администратором Единой защищенной сети передачи данных государственных органов Удмуртской Республики.

3. Министерству информатизации и связи Удмуртской Республики разработать документы и проекты соглашений, регламентирующие условия подключения к Единой защищенной сети передачи данных государственных органов Удмуртской Республики, в течение одного месяца с момента вступления в силу настоящего постановления.

4. Администрации Президента и Правительства Удмуртской Республики, исполнительным органам государственной власти Удмуртской Республики, государственным учреждениям Удмуртской Республики совместно с Министерством информатизации и связи Удмуртской Республики обеспечить подключение информационных систем к Единой защищенной сети

передачи данных государственных органов Удмуртской Республики в соответствии с Положением.

5. Рекомендовать территориальным органам федеральных органов исполнительной власти в Удмуртской Республике, органам местного самоуправления и муниципальным учреждениям в Удмуртской Республике обеспечить подключение к Единой защищенной сети передачи данных государственных органов Удмуртской Республики в соответствии с Положением.

**Председатель Правительства
Удмуртской Республики Ю.С.Наумович**



Положение о Единой защищенной сети передачи данных государственных органов Удмуртской Республики

1. Общие положения

1. Настоящее Положение определяет цели и задачи создания Единой защищенной сети передачи данных государственных органов Удмуртской Республики (далее – защищенная сеть), требования, предъявляемые к работе защищенной сети, полномочия оператора защищенной сети и администратора защищенной сети, права участника защищенной сети и условия подключения к защищенной сети.

2. Для целей настоящего Положения используются следующие понятия:

1) защищенная сеть – виртуальная, наложенная на физические каналы связи защищенная транспортная сеть, построенная с использованием технологий межсетевое экранирования и VPN и использующая для криптографической защиты алгоритм ГОСТ 28147-89, реализованная сертифицированными в установленном порядке средствами защиты информации, являющаяся частью информационно – коммуникационной инфраструктуры электронного правительства Удмуртской Республики;

2) оператор защищенной сети – государственный орган Удмуртской Республики, осуществляющий от имени Правительства Удмуртской Республики управление защищенной сетью;

3) участник защищенной сети – государственный орган Удмуртской Республики, государственное учреждение Удмуртской Республики, территориальный орган федерального органа исполнительной власти в Удмуртской Республике, орган местного самоуправления, муниципальное учреждение в Удмуртской Республике, подписавший с оператором защищенной сети двустороннее соглашение о подключении к защищенной сети и подключенный в установленном порядке к защищенной сети;

4) компоненты защищенной сети – подключаемые с применением оборудования к защищенной сети автоматизированные рабочие места пользователей, серверы баз данных, защищенные сети участников, иные объекты, подключение которых необходимо для целей функционирования защищенной сети;

5) автоматизированное рабочее место администратора (далее – АРМ администратора) – компьютер с установленным специальным программным обеспечением для администрирования защищенной сети, установленный в организации, осуществляющей администрирование защищенной сети;

6) оборудование – аппаратно-программный комплекс, выполняющий функции межсетевого экрана и криптомаршрутизатора,

имеющий сертификат соответствия Федеральной службы по техническому и экспортному контролю Российской Федерации и Федеральной службы безопасности Российской Федерации, устанавливаемый у участника защищенной сети;

7) информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

8) администратор защищенной сети – организация, осуществляющая администрирование защищенной сети с использованием АРМ администратора;

9) администрирование защищенной сети – действия администратора защищенной сети, непосредственно направленные на конфигурирование и управление компонентами защищенной сети, в соответствии с законодательством Российской Федерации, в том числе нормативно-правовыми актами иных органов, настоящим Положением и эксплуатационной документацией на средства защиты информации;

10) техническое сопровождение защищенной сети – консультирование участников защищенной сети по вопросам работы оборудования;

11) информация ограниченного доступа – информация, доступ к которой ограничен федеральными законами.

2. Цель и задачи создания защищенной сети

3. Основной целью создания защищенной сети является обеспечение безопасной передачи информации между участниками защищенной сети, в том числе информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, с использованием публичных и выделенных каналов связи путем организации виртуальной сети.

4. Основными задачами создания защищенной сети являются:

1) обеспечение безопасного взаимодействия участников защищенной сети при работе в региональной системе межведомственного электронного взаимодействия в Удмуртской Республике (далее – СМЭВ);

2) обеспечение безопасного взаимодействия участников защищенной сети при работе с Региональным порталом государственных и муниципальных услуг и с Единым порталом государственных и муниципальных услуг;

3) обеспечение безопасной передачи через открытые каналы связи информации ограниченного доступа между участниками защищенной сети:
для взаимодействия между участниками защищенной сети при работе в системе межведомственного электронного документооборота,
при работе с системой исполнения регламентов в СМЭВ;

4) обеспечение безопасного межсетевое взаимодействие между защищаемыми компонентами защищенной сети участников защищенной сети и сетью Интернет.

3. Требования, предъявляемые к работе защищенной сети

5. Защищенная сеть состоит из АРМ администратора и оборудования, установленного в помещениях участников защищенной сети, принадлежащих им на правах владения, аренды, безвозмездного пользования или на иных условиях, обеспечивающих защиту от несанкционированного доступа к оборудованию третьих лиц, а также каналов передачи данных.

6. Участник защищенной сети должен обеспечить информационную безопасность каждого подключаемого компонента защищенной сети в соответствии с законодательством Российской Федерации.

7. Оборудование, устанавливаемое у участников защищенной сети, должно находиться в пределах их контролируемой зоны.

8. Защищенная сеть должна находиться в работоспособном режиме постоянно.

9. Оборудование, установленное у участника защищенной сети, должно находиться в работоспособном состоянии, быть доступным для других участников защищенной сети при межсетевом, защищенном взаимодействии с использованием сети Интернет, за исключением времени проведения ремонтно-профилактических работ.

10. Администрирование и техническое сопровождение защищенной сети осуществляется администратором защищенной сети самостоятельно, либо с привлечением сторонних организаций. Привлекаемые для администрирования и технического сопровождения защищенной сети организации осуществляют данную деятельность в соответствии с законодательством Российской Федерации, настоящим Положением и эксплуатационной документацией на используемое (применяемое) оборудование и программное обеспечение.

4. Полномочия оператора защищенной сети и администратора защищенной сети

11. Оператор защищенной сети выполняет следующие функции:

- 1) подписывает соглашения о подключении участника защищенной сети;
- 2) предоставляет при необходимости оборудование участнику защищенной сети;
- 3) определяет полномочия и порядок работы администратора защищенной сети при работе с защищенной сетью;
- 4) ведет реестр участников защищенной сети;
- 5) определяет технологию, предназначенную для построения защищенной сети путем использования системы межсетевых экранов на защищаемых элементах распределенной сети (рабочие станции, сервера, локальные сети) и объединения защищаемых элементов через виртуальные соединения (туннели), обеспечивающую шифрование сетевого трафика между этими элементами, применяет и использует её при функционировании защищенной сети;

6) с учетом требований законодательства определяет наименование применяемого в защищенной сети оборудования, а также его количество, характеристики и требования к нему, в том числе в области защиты информации;

7) разрабатывает и предоставляет участникам защищенной сети документы, регламентирующие порядок и условия подключения к защищенной сети, порядок работы участников защищенной сети в защищенной сети, проекты соглашений о подключении к защищенной сети.

12. Оператор защищенной сети имеет право:

1) разрабатывать документацию по вопросам, касающимся эксплуатации и управления защищенной сети;

2) запрашивать и получать от участников защищенной сети необходимые материалы и сведения об использовании ими защищенной сети;

3) отключать, с уведомлением администратора, от защищенной сети участников защищенной сети, нарушающих требования настоящего Положения.

13. Администратор защищенной сети выполняет следующие функции:

1) обеспечивает бесперебойный и безопасный доступ подключенных участников защищенной сети к расположенным в ней компонентам защищенной сети;

2) обеспечивает администрирование защищенной сети, наблюдение за работоспособностью защищенной сети и, по необходимости, принимает меры по восстановлению её работоспособности;

3) управляет доступом участников защищенной сети к компонентам защищенной сети и сетевым сервисам защищенной сети;

4) обеспечивает защиту оборудования защищенной сети от несанкционированных действий внутренних и внешних пользователей, в рамках своих полномочий;

5) управляет техническими средствами защищенной сети;

6) предпринимает необходимые меры для развития и поддержания работоспособности защищенной сети;

7) определяет по согласованию с оператором защищенной сети необходимые меры и технологии (в том числе криптографические) для обеспечения безопасной передачи данных по защищенной сети;

8) подключает по согласованию с оператором защищенной сети защищенную сеть к другим сетям для осуществления государственных (муниципальных) услуг (функций);

9) приостанавливает по согласованию с оператором защищенной сети функционирование защищенной сети не более чем на 10 часов в месяц для проведения обслуживания оборудования, при обязательном уведомлении всех участников защищенной сети о планируемых работах, не позднее, чем за 1 день до их начала, а так же уведомляет об окончании таких работ;

10) подключает к защищенной сети новых участников защищенной сети в соответствии с настоящим Положением;

- 11) осуществляет техническое сопровождение защищенной сети;
- 12) осуществляет ремонтно-профилактические работы на оборудовании защищенной сети;
- 13) определяет по согласованию с оператором защищенной сети необходимый перечень программного и аппаратного обеспечения (в том числе специального) для обеспечения функционирования АРМ администратора.

5. Права участника защищенной сети

14. Участник защищенной сети имеет право:
 - 1) получать доступ к защищенной сети в соответствии с условиями, утвержденными оператором защищенной сети;
 - 2) получать справочную и иную информацию о работе и использовании защищенной сети;
 - 3) получать от оператора защищенной сети документацию, регламентирующую порядок и условия подключения к защищенной сети, проекты соглашений о подключении к защищенной сети;
 - 4) на техническое сопровождение защищенной сети.
15. Полномочия участника защищенной сети при работе с защищенной сетью определяются соглашением о подключении к защищенной сети.

6. Условия подключения к защищенной сети

16. Подключение осуществляется после подписании соглашения о подключении к защищенной сети.
17. Подключение и взаимодействие с участниками защищенной сети, имеющими собственные защищенные сети, может быть осуществлено при условии заключения с оператором защищенной сети соглашения о подключении к защищенной сети.

