ПРАВИТЕЛЬСТВО
УДМУРТСКОЙ РЕСПУБЛИКИ

УДМУРТ ЭЛЬКУН
КИВАЛТЭТ

ПОСТАНОВЛЕНИЕ

от 30 июля 2021 года № 388

г. Ижевск

О внесении изменений в постановление Правительства Удмуртской Республики от 16 апреля 2012 года № 169 «Об утверждении Положения о Единой защищенной сети передачи данных государственных органов Удмуртской Республики»

Правительство Удмуртской Республики **постановляет**:

1. Внести в постановление Правительства Удмуртской Республики от 16 апреля 2012 года № 169 «Об утверждении Положения о Единой защищенной сети передачи данных государственных органов Удмуртской Республики» следующие изменения:

1) в абзаце третьем пункта 2 слово «бюджетное» заменить словом «автономное»;

2) пункт 3 признать утратившим силу;

3) дополнить пунктами 3.1 и 3.2 следующего содержания:

«3.1. Министерству информатизации и связи Удмуртской Республики обеспечить технологическое сопровождение и координацию развития Единой защищенной сети передачи данных государственных органов Удмуртской Республики.

3.2. Администратору Единой защищенной сети передачи данных государственных органов Удмуртской Республики:

1) обеспечить техническую поддержку программных и программно-аппаратных комплексов, обеспечивающих работу Единой защищённой сети;

2) обеспечить эксплуатацию программных и программно-аппаратных комплексов, обеспечивающих работу Единой защищённой сети в соответствии с эксплуатационной документацией.»;

4) Положение о Единой защищенной сети передачи данных государственных органов Удмуртской Республики изложить в редакции согласно приложению.

2. Установить, что финансирование расходов, связанных с выполнением Положения о Единой защищенной сети передачи данных государственных

органов Удмуртской Республики, осуществляется в пределах бюджетных ассигнований, предусмотренных Министерству информатизации и связи Удмуртской Республики законом о бюджете Удмуртской Республики на соответствующий финансовый год и на плановый период на реализацию государственной программы Удмуртской Республики «Развитие информационного общества в Удмуртской Республике», утвержденной постановлением Правительства Удмуртской Республики от 1 июля 2013 года № 268 «Об утверждении государственной программы Удмуртской Республики «Развитие информационного общества в Удмуртской Республике».

Председатель Правительства
Удмуртской Республики **Я.В. Семенов**

Приложение
к постановлению Правительства
Удмуртской Республики
от 30 июля 2021 года № 388

«УТВЕРЖДЕНО
постановлением Правительства
Удмуртской Республики
от 16 апреля 2012 года № 169

ПОЛОЖЕНИЕ
о Единой защищенной сети передачи данных государственных органов Удмуртской Республики

I. 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, участника защищенной сети, функции администратора защищенной сети и порядок подключения к защищенной сети.

Обмен информацией между участниками защищенной сети осуществляется с помощью информационно-телекоммуникационной сети.

Защищенная сеть состоит из защищенных сетей передачи данных Министерства информатизации и связи Удмуртской Республики, Министерства социальной политики и труда Удмуртской Республики, Министерства природных ресурсов и охраны окружающей среды Удмуртской Республики, Министерства образования и науки Удмуртской Республики, Главного управления по государственному надзору Удмуртской Республики, Управления по обеспечению деятельности мировых судей Удмуртской Республики, государственного учреждения Удмуртской Республики «Служба гражданской защиты Удмуртской Республики».

II. Термины и определения

2. В настоящем Положении используются следующие термины и определения:

1) автоматизированное рабочее место администратора – компьютер с установленным специальным программным обеспечением для администрирования защищенной сети, установленный у администратора защищенной сети;

2) администратор защищенной сети – государственное учреждение Удмуртской Республики, осуществляющее администрирование защищенной сети с использованием автоматизированного рабочего места;

3) администрирование защищенной сети – действия администратора защищенной сети, непосредственно направленные на конфигурирование и управление компонентами защищенной сети в соответствии с законодательством Российской Федерации, настоящим Положением и эксплуатационной документацией на средства защиты информации;

4) виртуальная частная сеть (далее также – VPN) – территориально распределенная корпоративная логическая сеть, создаваемая на базе уже существующих сетей (локальных корпоративных сетевых структур, сетей связи общего пользования, информационно-телекоммуникационной сети «Интернет», сетей связи операторов связи), имеющая сходный с основной сетью набор услуг и отличающаяся высоким уровнем защиты данных;

5) защищенная сеть – виртуальная сеть связи, наложенная на существующие сети связи, являющиеся частью инфраструктуры электронного правительства Удмуртской Республики, построенная с использованием технологий межсетевого экранирования и VPN, а также с использованием сертифицированных в установленном порядке средств защиты информации и применением средств криптографической защиты информации действующих по алгоритмам согласно ГОСТ 34.10-2018;

6) заявитель – 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, выполняющие процедуру заключения с оператором защищенной сети соглашения о подключении к защищенной сети и не подключенный к защищенной сети;

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

8) информационно-телекоммуникационная сеть – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;

9) информация ограниченного доступа – информация, доступ к которой ограничен в соответствии с федеральными законами;

10) инцидент информационной безопасности – появление одного или нескольких нежелательных, или неожиданных событий информационной безопасности, с которыми связана значительная вероятность компрометации операций и создания угрозы информационной безопасности;

11) контролируемая зона – пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска, и посторонних транспортных средств;

12) компоненты защищенной сети – подключаемые с применением оборудования к защищенной сети автоматизированные рабочие места

пользователей, серверы баз данных, иные защищенные сети и объекты, подключение которых необходимо для целей функционирования защищенной сети;

13) оборудование – аппаратно-программный комплекс, выполняющий функции межсетевого экрана и криптомаршрутизатора, имеющий сертификат соответствия Федеральной службы по техническому и экспортному контролю и Федеральной службы безопасности Российской Федерации, устанавливаемый у участника защищенной сети;

14) ответственный пользователь участника защищенной сети – должностное лицо участника защищённой сети, ответственное за взаимодействие с оператором защищенной сети и администратором защищенной сети;

15) оператор защищенной сети – исполнительный орган государственной власти Удмуртской Республики, осуществляющий от имени Правительства Удмуртской Республики управление защищенной сетью;

16) пользователь участника защищенной сети – должностное лицо участника защищённой сети, непосредственно использующее ресурсы защищенной сети при выполнении своих должностных обязанностей;

17) средства криптографической защиты информации – аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении;

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

19) 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, заключивший с оператором защищенной сети соглашение о подключении к защищенной сети и подключенный в установленном порядке к защищенной сети.

III. Цели и задачи создания защищенной сети

3. Основной целью создания защищенной сети является создание условий для обеспечения безопасного обмена между ее участниками информацией ограниченного доступа, не содержащей сведений, составляющих государственную тайну.

4. Основной задачей создания защищенной сети является обеспечение безопасного взаимодействия между участниками защищенной сети, соблюдение мер по защите информации и исключение неправомерных или случайных действий, создающих угрозу информационной безопасности.

IV. Требования, предъявляемые к защищенной сети

5. Защищенная сеть должна отвечать следующим требованиям:

1) обеспечение защиты информации при эксплуатации защищенной сети участниками защищенной сети;

2) обеспечение безопасного доступа к защищенной сети для каждого подключаемого компонента защищенной сети;

3) защищенная сеть должна быть организована с помощью аппаратно-программных комплексов шифрования и технологий, прошедших сертификацию Федеральной службы по техническому и экспортному контролю и Федеральной службы безопасности Российской Федерации;

4) защищенная сеть должна отвечать требованиям целостности, устойчивости и безопасности при подключении каждого подключаемого компонента защищенной сети.

V. Требования, предъявляемые к оборудованию защищенной сети

6. Оборудование, используемое для организации защищенной сети, должно отвечать следующим требованиям:

1) централизованное управление защищенной сетью, сетевыми настройками и узлами безопасности с возможностью просмотра журналов событий;

2) шифрование трафика по алгоритмам ГОСТа;

3) наличие полного контроля и фильтрации проходящего трафика по каналам защищенной сети;

4) безопасный доступ участников защищенной сети к ресурсам защищенной сети;

5) обеспечение безопасного удаленного доступа пользователей участников защищенной сети к ресурсам защищенной сети;

6) идентификация и аутентификация пользователей участников защищенной сети;

7) наличие механизма трансляции IP-адресов NAT;

8) наличие функций статической и динамической маршрутизации IP- пакетов;

9) наличие технологии VPN-тунеллирования;

10) наличие параметров отказоустойчивости для быстрого восстановления работы защищенной сети;

11) оборудование, обеспечивающее защиту информации должно иметь кластеры горячего резервирования;

12) наличие сертификатов соответствия по требованиям защиты информации Федеральной службы по техническому и экспортному контролю и Федеральной службы безопасности Российской Федерации.

VI. Порядок подключения к защищенной сети

7. Подключение к защищенной сети осуществляется в следующем порядке:

1) подключение к защищенной сети осуществляется на основании заявок, направленных в адрес оператора защищенной сети.

К заявке на подключение к защищенной сети прилагаются заверенные в установленном порядке копии приказа или иного документа о назначении должностного лица, ответственного за организацию подключения к защищенной сети, а также утвержденный список пользователей участника защищенной сети;

2) оператор защищенной сети совместно с администратором защищенной сети в течении трех рабочих дней со дня получения документов, предусмотренных подпунктом 1 настоящего пункта, на основании полученных документов проводят оценку технической возможности подключения к защищенной сети;

3) по результатам оценки технической возможности подключения к защищенной сети оператор защищенной сети принимает решение о подключении заявителя к защищенной сети либо об отказе в подключении к защищенной сети в случае отсутствия технической возможности подключения;

4) в случае принятия решения о подключении к защищенной сети оператор защищенной сети уведомляет официальным письмом администратора защищенной сети, направляет заявителю проект соглашения о подключении к Единой защищенной сети передачи данных государственных органов Удмуртской Республики (далее – соглашение);

5) соглашение заключается заявителем в течение 30 рабочих дней со дня получения его проекта. В случае незаключения соглашения в указанный срок или отказа заявителя от заключения соглашения оператор защищенной сети принимает решение об отказе в подключении заявителя к защищенной сети;

6) в случае принятия решения об отказе в подключении заявителя к защищенной сети по основаниям, предусмотренным подпунктом 3 настоящего пункта, оператор защищенной сети:

совместно с администратором защищенной сети принимают меры по устранению невозможности подключения заявителя к защищенной сети;

уведомляет официальным письмом заявителя о причинах отказа в течении 30 рабочих дней со дня принятия решения об отказе.

После устранения причин, явившихся основанием для принятия решения об отказе в подключении заявителя к защищенной сети, оператор защищенной сети совместно с администратором защищенной сети уведомляют об этом заявителя официальным письмом в течение 30 рабочих дней со дня устранения причин отказа и осуществляют подключение заявителя к защищенной сети в течение 30 рабочих дней со дня направления заявителю уведомления, предусмотренного настоящим абзацем;

7) администратор защищенной сети на основании соглашения выполняет работы по организации безопасного доступа заявителя к защищенной сети и в

течение 30 рабочих дней со дня завершения работ уведомляет оператора защищенной сети и участника защищенной сети.

8. Подключение и взаимодействие с участниками защищенной сети, имеющими собственные защищенные сети, осуществляется при условии заключения с оператором защищенной сети соглашения.

VII. Полномочия оператора защищенной сети

9. Оператор защищенной сети выполняет следующие функции:

1) определяет состав и количество технических и аппаратно-программных средств для организации защищенной сети;

2) осуществляет закупку оборудования, необходимого для функционирования защищенной сети;

3) ведет реестр участников защищенной сети;

4) определяет перечень используемых средств защиты информации и средств криптографической защиты информации;

5) определяет перечень используемых средств антивирусной защиты;

6) предоставляет (при необходимости) оборудование, необходимое для функционирования защищённой сети, участнику защищенной сети;

7) представляет участникам защищенной сети документы, регламентирующие порядок работы участников защищенной сети в защищенной сети, а также проект соглашения;

8) определяет порядок работы администратора защищенной сети с защищенной сетью;

9) осуществляет мероприятия по развитию и модернизации защищенной сети;

10) взаимодействует с администратором защищенной сети и участником защищенной сети по вопросам защиты информации;

11) осуществляет контроль и участвует в выявлении неправомерных или случайных действий, создающих угрозу информационной безопасности, которые могут привести к сбою, возникновению угроз безопасности информации или нарушению функционирования защищенной сети;

12) соблюдение требований защиты информации;

10. Оператор защищенной сети имеет право:

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

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

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

VIII. Функции администратора защищенной сети

11. Администратор защищенной сети выполняет следующие функции:

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

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

3) управляет доступом участников защищенной сети к компонентам защищенной сети;

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

5) управляет оборудованием 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 предоставления государственных (муниципальных) услуг (осуществления государственных и муниципальных функций);

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

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

11) осуществляет администрирование и техническое сопровождение защищенной сети. 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;

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 автоматизированного рабочего места администратора защищенной сети;

14) соблюдение требований защиты информации.

IX. Полномочия участника защищенной сети

12. Участник защищенной сети выполняет следующие функции:

1) назначение ответственного пользователя участника защищенной сети, а также лица, его замещающего;

2) соблюдение требований защиты информации;

3) обеспечение размещения и охраны компонентов защищенной сети;

4) уведомление оператора и администратора защищенной сети о действиях пользователей, осуществляющих несанкционированный доступ к ресурсам защищенной сети или нарушивших требования защиты информации;

5) определение состава и количества пользователей для организации доступа к ресурсам защищенной сети.

13. Участник защищенной сети имеет право:

1) получать доступ к защищенной сети при соблюдении порядка подключения к защищенной сети;

2) получать от оператора защищенной сети, администратора защищенной сети информацию о работе и об использовании защищенной сети;

3) получать от оператора защищенной сети документацию, регламентирующую порядок подключения к защищенной сети, проект соглашения;

4) на техническое сопровождение защищенной сети.

X. Полномочия ответственного пользователя участника защищенной сети

14. Ответственный пользователь участника защищенной сети выполняет следующие функции:

1) осуществление технического контроля эксплуатации пользователями участника защищенной сети компонентов защищенной сети;

2) ознакомление пользователей с действующим законодательством Российской Федерации в сфере защиты информации;

3) осуществление мер по поддержанию работоспособности и состоянию защищенности компонентов защищенной сети;

4) уведомление руководителя участника защищенной сети и администратора защищенной сети об инцидентах информационной безопасности, выявленных в процессе эксплуатации компонентов защищенной сети;

5) составление перечня пользователей участника защищенной сети для организации доступа к ресурсам защищенной сети;

6) осуществление контроля доступа к компонентам и ресурсам защищенной сети;

7) осуществление установки, настройки и контроля эксплуатации средств защиты информации, средств криптографической защиты информации, средств антивирусной защиты и оборудования защищенной сети;

8) осуществление установки компонентов защищенной сети в пределах контролируемой зоны;

9) соблюдение требований защиты информации;

10) контроль эксплуатации пользователями оборудования и компонентов защищенной сети.

15. Ответственный пользователь участника защищенной сети имеет право:

1) ограничивать доступ пользователям участника защищенной сети при выявлении или предотвращении нарушений требований защиты информации;

2) осуществлять контроль за пользователями участника защищенной сети во время использования ресурсов защищенной сети в целях соблюдения требований законодательства Российской Федерации в сфере безопасности информации.

XI. Полномочия пользователей участника защищенной сети

16. Пользователь участника защищенной сети выполняет следующие обязанности:

1) соблюдает требования законодательства Российской Федерации в сфере защиты информации при использовании ресурсов защищенной сети;

2) уведомляет ответственного пользователя участника защищенной сети о нарушениях работы средств защиты информации, средств криптографической защиты информации, средств антивирусной защиты.

17. Пользователь имеет право использовать ресурсы и компоненты защищенной сети для выполнения своих должностных обязанностей.».