СОГЛАШЕНИЕ № ____/_____
о подключении к Единой защищенной сети передачи данных государственных органов Удмуртской Республики

г. Ижевск «_____» _____ 20___ г.

Министерство информатизации и связи Удмуртской Республики, именуемое в дальнейшем «Оператор сети», в лице заместителя Председателя Правительства Удмуртской Республики – министра информатизации и связи Удмуртской Республики В.Ю. Перешеина, действующего на основании Положения, утвержденного постановлением Правительства Удмуртской Республики от 30 августа 2010 года № 273, и _____
_____,
(наименование Участника защищенной сети)
именуем__ в дальнейшем «Участник защищенной сети», в лице_____
_____
(наименование должности, Ф.И.О.)
_____,
действующ_____ на основании _____
_____,
(наименование документа)
совместно именуемые в дальнейшем «Стороны», на основании Положения о Единой защищенной сети передачи данных государственных органов Удмуртской Республики, утвержденного Постановлением Правительства Удмуртской Республики от 16 апреля 2012 года № 169 заключили настоящее Соглашение о нижеследующем.

1. Для целей настоящего соглашения используются следующие понятия:

1) защищенная сеть – виртуальная, наложенная на физические каналы связи защищенная транспортная сеть, построенная с использованием технологий межсетевого экранирования и VPN и использующая для криптографической защиты алгоритм ГОСТ 28147-89, реализованные 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.

1. Предмет Соглашения

1. Настоящее Соглашение определяет регламент работы участников защищенной сети в Единой защищенной сети передачи данных государственных органов Удмуртской Республики (далее-защищенная сеть), цели, задачи и порядок её использования, права и обязанности Сторон, условия подключения к защищенной сети, вопросы администрирования, технического сопровождения и режим работы защищенной сети и заключается между Сторонами, руководствуясь Положением о Единой защищенной сети передачи данных государственных органов Удмуртской Республики, утвержденным Постановлением Правительства Удмуртской Республики от 16 апреля 2012 года № 169.

2. При работе в защищенной сети участники защищенной сети руководствуются:

1) Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

2) Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных»;

3) Указом Президента Российской Федерации от 17.03.2008 № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»;

4) Положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденным приказом ФСБ России от 09 февраля 2005 года № 66;

5) Инструкцией 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 ФАПСИ от 13 июня 2001 года № 152;

6) Приказом Министерства связи и массовых коммуникаций РФ от 27 декабря 2010 г. № 190 «Об утверждении Технических требований к взаимодействию информационных систем в единой системе межведомственного электронного взаимодействия»;

7) Приказом ФСТЭК РФ от 5 февраля 2010 г. № 58 «Положения о методах и способах защиты информации в информационных системах персональных данных».

8) Положением о Единой защищенной сети передачи данных государственных органов Удмуртской Республики, утвержденным Постановлением Правительства Удмуртской Республики от 16 апреля 2012 года № 169;

9) иными нормативными правовыми актами, регулирующими отношения в сфере информационных технологий и защиты информации.

2. Цели и задачи использования защищенной сети

3. Стороны обязуются использовать защищенную сеть для:

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

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

3) обеспечения безопасной передачи через открытые каналы связи информации ограниченного доступа между участниками защищенной сети;

4) обеспечения безопасного межсетевого взаимодействия между защищаемыми компонентами защищенной сети участников защищенной сети.

3. Требования, предъявляемые к работе защищенной сети

4. Применяемые в защищенной сети средства защиты информации должны соответствовать:

- требованиям ФСБ России к средствам криптографической защиты информации класса КС3 (на применяемое криптоядро и программно-аппаратный комплекс);
- требованиям ФСБ России к устройствам типа межсетевые экраны по 4 классу защищенности и иметь разрешение для использования для защиты информации от несанкционированного доступа в информационно-телекоммуникационных системах органов государственной власти Российской Федерации;
- требованиям ФСТЭК России к межсетевым экранам не ниже 3 класса, по контролю отсутствия недекларированных возможностей не ниже 4 уровня, иметь разрешение для использования в автоматизированных системах не ниже класса 1Г и при создании информационных систем персональных данных до 1 класса включительно.

5. Участники защищенной сети Удмуртской Республики признают, что использование в системе сертифицированных средств защиты информации, обеспечивающих межсетевое экранирование и криптографическое преобразование передаваемых данных, достаточно для безопасного подключения к сети Интернет и обеспечения конфиденциальности информационного взаимодействия.

6. Подсистема информационной безопасности каждого компонента защищенной сети, подключаемой к защищенной сети, должна обеспечивать установленные законодательством Российской Федерации уровни защищенности информации, обрабатываемой в этой системе.

7. Каналы связи защищенной сети, выходящие за пределы контролируемых зон участников защищенной сети, должны быть защищены с помощью оборудования, удовлетворяющих установленным требованиям и находящихся в пределах контролируемых зон участников сети.

8. Защищенная сеть состоит из АРМ администратора и оборудования, установленного в помещениях участников защищенной сети, принадлежащих принадлежащего 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.

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.

4. Полномочия оператора защищенной сети

10. 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 защищенные соединения (криптографические 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.

11. 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 Соглашения.

12. Оператор защищенной сети не несет ответственность за состав и содержание информации, передаваемой по защищенной сети между участниками защищенной сети.

5. Администратор защищенной сети, его полномочия, администрирование и техническое сопровождение защищенной сети

13. Администратор защищенной сети не несет ответственность за состав и содержание информации, передаваемой по защищенной сети между участниками защищенной сети.

14. 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 и эксплуатационной документацией на используемое (применяемое) оборудование и программное обеспечение.

15. Доступ администратора защищенной сети к ресурсам защищенной сети обуславливается технической и технологической необходимостью. Администратору защищенной сети запрещается неправомерное использование информации, к которой он получает доступ в связи с выполнением своих функций.

16. Зоной ответственности администратора защищенной сети к ресурсам и техническим средствам защищенной сети является оконечное оборудование, установленное у участников защищенной сети.

17. Администратор защищенной сети не несет ответственности за обеспечение информационной безопасности подключаемых компонентов защищенной сети участников защищенной сети.

18. 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 Условиями подключения к защищенной сети;

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.

6. Полномочия участника защищенной сети

19. 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 использованию 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;

5) отключать оборудование, с предварительным уведомлением администратора защищенной сети за 24 часа до планируемого отключения, но не более чем на 24 часа в месяц.

20. Участник защищенной сети обязан:

1) соблюдать правила техники безопасности при работе с оборудованием;

2) обеспечивать неразглашение конфиденциальных данных, используемых для доступа к ресурсам защищенной сети;

3) препятствовать несанкционированному доступу к ресурсам защищенной сети;

4) препятствовать несанкционированному использованию ресурсов защищенной сети;

5) содействовать сохранности ресурсов защищенной сети;

6) обеспечивать защиту информации на подключаемых компонентах защищенной сети к защищенной сети на необходимом уровне, в соответствие с законодательством

7) обеспечить круглосуточную работу установленного оборудования, за исключением случаев проведения профилактических работ;

8) сообщить об обнаружении недоступности защищенной сети, либо других нештатных ситуациях, препятствующих её нормальному функционированию.

21. Участнику защищенной сети запрещается:

1) отключение электропитания оборудования;

2) предоставлять доступ к ресурсам защищенной сети посторонним лицам и пользователям других сетей в любой форме;

3) распространять в сети общего пользования Интернет информацию, являющуюся интеллектуальной собственностью Удмуртской Республики, информацию ограниченного доступа и защищенную законодательством об авторском праве и смежных правах;

4) создавать и поддерживать средствами защищенной сети любые ресурсы, содержание, цели и задачи которых не связаны с основными задачами защищенной сети;

5) изменять сетевые настройки информационных ресурсов, оборудования без согласования с администратором защищенной сети;

6) публиковать и рассылать информацию, нарушающую действующее законодательство Российской Федерации, включая порнографические и оскорбительные материалы, пропаганду насилия, расизма, религиозной ненависти, распространения, изготовления и применения наркотических и опасных веществ, а также политическую и религиозную пропаганду;

7) фальсифицировать обратный адрес электронной почты, IP-адреса рабочего места, адресов, используемых в других сетевых протоколах, при передаче данных, а также использовать идентификационные данные (в том числе имена, адреса, телефоны) третьих лиц, кроме случаев, когда такие действия санкционированы и согласованы с администратором защищенной сети;

8) осуществлять попытки несанкционированного или неправомерного доступа к ресурсам защищенной сети, проводить или участвовать в сетевых атаках и сетевом взломе, а также осуществлять сканирование ресурсов защищенной сети и осуществлять другие действия, направленные на выявление параметров и характеристик ресурсов защищенной сети, их структуры и структуры взаимодействия;

9) производить действия, направленные на нарушение нормального функционирования защищенной сети;

10) производить действия по созданию, использованию и распространению вредоносных программ и компьютерных вирусов, в том числе направленных на получение несанкционированного доступа к любым системам и службам либо на нарушение целостности и работоспособности этих систем;

11) осуществлять любые другие действия с ресурсами защищенной сети, запрещенные законодательством в области связи, информационных технологий, массовых коммуникаций и защиты информации;

22. Участник защищенной сети исключает доступ посторонних лиц ко всем техническим средствам защищенной сети, каналам связи и поддерживающим системам (электропитания, вентиляции, кондиционирования и т.п.) в контролируемой зоне.

23. Участник защищенной сети несет ответственность за состав и содержание информации, передаваемой по защищенной сети.

24. Участник защищенной сети, в целях обеспечения защиты информации, содержащейся в информационных системах, подключенных к защищенной сети:

- обеспечивает при обслуживании информационных систем, подключенных к защищенной сети, исполнение установленных требований по информационной, производственной, технологической и противопожарной безопасности;

- осуществляет контроль доступа посторонних лиц к техническим средствам и каналам связи в контролируемой зоне участника защищенной сети, включая время проведения ремонтных работ и уборки помещений;

- обеспечивает обслуживание информационных систем, подключенных к защищенной сети, 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 защищенной сети, расположенному в контролируемой зоне участника защищенной сети, а также лиц, имеющих возможность изменения конфигурации информационных систем участника защищенной сети, подключенных к защищенной сети.

7. Ответственность сторон

25. При нарушении условий настоящего Соглашения Оператор сети в одностороннем порядке имеет право расторгнуть настоящее Соглашение.

26. Участник защищенной сети несет материальную ответственность за ущерб, причиненный защищенной сети при ненадлежащем исполнении им условий настоящего Соглашения.

8. Заключительные положения

27. Настоящее Соглашение вступает в силу с момента подписания его Сторонами и действует бессрочно.

28. Все изменения и дополнения к настоящему Соглашению оформляются Дополнительными двусторонними соглашениями и действуют с момента их подписания Сторонами.

29. Настоящее Соглашение составлено в двух экземплярах, имеющих одинаковую юридическую силу, по одному для каждой из Сторон.

9. Реквизиты и подписи Сторон

Участник сети

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Оператор сети:

Министерство информатизации и связи Удмуртской Республики

426007, г. Ижевск, ул. Пушкинская, 214
Тел.: (3412) 497-018, факс: 497-498
ИНН 1831142969 КПП 183101001
ОГРН 1101831004582
УФК по Удмуртской Республике
(Минфин Удмуртии
(Министерство информатизации и связи Удмуртской Республики))
Р/с 40201810400000010002
в ГРКЦ НБ Удмуртской Республики
Банка России г. Ижевск БИК 049401001
e-mail: mininf@udmurt.ru

Заместитель Председателя Правительства Удмуртской Республики – министр информатизации и связи Удмуртской Республики

_____ / В.Ю. Перешеин /
М.П.