



**ДЕПАРТАМЕНТ
РАЗВИТИЯ ИНФОРМАЦИОННОГО
ОБЩЕСТВА
ИВАНОВСКОЙ ОБЛАСТИ**

153000, г. Иваново, пл. Революции, д. 2/1, офис 319, тел. 90-13-80, e-mail mail@it.ivanovoobl.ru

ПРИКАЗ

«01» 11 2022 г.

№ 49/22

г. Иваново

**О вводе в эксплуатацию защищенной сети передачи данных в органах
государственной власти, органах местного самоуправления и их
подведомственных организаций**

В рамках реализации полномочий Департамента развития информационного общества Ивановской области, в целях соблюдения требований законодательства Российской Федерации в части защиты передачи данных в электронном виде между органами государственной власти, органами местного самоуправления и их подведомственными организациями на территории Ивановской области, организации и регламентирования порядка подключения к защищенной сети передачи данных, по результатам опытной эксплуатации защищенной сети передачи данных Ивановской области **п р и к а з ы в а ю:**

1. Утвердить Положение о защищенной сети передачи данных Ивановской области (приложение 1).

2. Утвердить Регламент подключения участника электронного взаимодействия к защищенной сети передачи данных Ивановской области (приложение 2).

3. Возложить на Управление региональной информатизации Департамента развития информационного общества Ивановской области функции координатора защищенной сети передачи данных Ивановской области - уполномоченной структуры по назначению оператора, организации, эксплуатации и регламентированию присоединения к защищенной сети передачи данных Ивановской области, ее использованию.

4. Установить, что возможность использования государственных информационных систем Ивановской области органами государственной власти Ивановской области, иными государственными органами Ивановской области, органами местного самоуправления Ивановской области при оказании ими государственных и муниципальных услуг в электронном виде, осуществлении электронного документооборота, с прочими целями, обеспечивается посредством присоединения их к защищенной сети передачи данных Ивановской области.

5. Ввести в эксплуатацию защищенную сеть передачи данных Ивановской области (далее - ЗСПД Ивановской области).

6. Отделу информационных технологий Департамента развития информационного общества Ивановской области зарегистрировать ЗСПД Ивановской области как информационную систему.

7. Назначить ответственным лицом за защиту информации и обеспечение безопасности персональных данных в информационной системе ЗСПД Ивановской области – администратора информационной безопасности Департамента развития информационного общества Ивановской области.

8. Сектору технической защиты информации Департамента развития информационного общества Ивановской области разработать и организовать ведение учетной документации на ЗСПД Ивановской области.

9. Отделу информационных технологий Департамента развития информационного общества Ивановской области проинформировать заинтересованных лиц о вводе в эксплуатацию ЗСПД Ивановской области, обеспечить заключение соглашения о подключении к ЗСПД Ивановской области со всеми участниками электронного взаимодействия.

10. Отделу финансового обеспечения, государственных закупок и кадровой политики Департамента развития информационного общества Ивановской области принять на учет ЗСПД Ивановской области как информационную систему с балансовой стоимостью 480 000 (четыреста восемьдесят тысяч) рублей.

11. Контроль за выполнением настоящего приказа оставляю за собой.

Начальник Департамента



М.Е. Хохлов

Приложение 1
к приказу Департамента развития
информационного общества
Ивановской области
от 01.11.2022 № 49/22

ПОЛОЖЕНИЕ **о защищенной сети передачи данных Ивановской области**

1. Общие положения

1.1. Настоящее Положение определяет цели и задачи создания защищенной сети передачи данных Ивановской области (далее – ЗСПД Ивановской области), структуру и состав ЗСПД Ивановской области, полномочия участников электронного взаимодействия и условия подключения к ЗСПД Ивановской области.

1.2. ЗСПД Ивановской области является защищенной виртуальной сетью передачи данных, построенная на основе технологии виртуальных защищенных сетей ViPNet.

ЗСПД Ивановской области создана с целью обеспечения безопасности взаимодействия между органами государственной власти, органами местного самоуправления и их подведомственными организациями на территории Ивановской области, и иных органов, организаций, участвующих в предоставлении государственных и муниципальных услуг в электронном виде, выполнении государственных (муниципальных) функций, осуществлении электронного документооборота с прочими целями.

ЗСПД Ивановской области спроектирована и выполнена посредством применения программно-аппаратных решений продуктовой линейки ViPNet производителя АО «ИнфоТеКС» (порядковый регистрационный номер сети – №2421)

1.3. ЗСПД Ивановской области предназначена для решения следующих задач:

- обеспечение безопасного информационного межсетевое взаимодействия в электронном виде;
- организация взаимодействия информационных систем пользователей ЗСПД Ивановской области по защищенным каналам связи;
- обеспечение безопасности информации, передаваемой по каналам связи ЗСПД Ивановской области, в соответствии с действующим законодательством.

1.4. К ЗСПД Ивановской области подключаются информационно-телекоммуникационные сети и (или) автоматизированные рабочие места пользователей ЗСПД Ивановской области.

1.5. ЗСПД Ивановской области не предназначена для подключения информационно-телекоммуникационных сетей и автоматизированных рабочих мест, применяемых для хранения, обработки или передачи информации, содержащей сведения, составляющие государственную тайну, возмездного оказания услуг связи.

2. Структура и состав ЗСПД Ивановской области

2.1. В состав ЗСПД Ивановской области входят следующие компоненты:

- центр управления сетью (далее - ЦУС);

- аппаратно-программные сетевые узлы (далее - АПСУ);
- программные сетевые узлы (далее - ПСУ);
- средства обнаружения вторжений и угрозы безопасности информации (далее - СОВ);
- автоматизированные рабочие места пользователей защищенной сети передачи данных (далее - АРМ).

2.2. ЦУС - аппаратно-программные и программные комплексы, реализующие функции управления структурой ЗСПД Ивановской области.

2.3. АРМ - автоматизированные рабочие места пользователей на базе электронных вычислительных машин, взаимодействующие с АПСУ либо ПСУ с целью доступа к информационным ресурсам ЗСПД Ивановской области.

2.4. ПСУ - специальное программное обеспечение, выполняющее клиентские функции по шифрованию трафика или серверные функции по шифрованию и маршрутизации трафика для подключения АРМ к ЗСПД Ивановской области.

2.5. АПСУ - специальные программно-аппаратные комплексы, выполняющие серверные функции по шифрованию и маршрутизации трафика для подключения АРМ к ЗСПД Ивановской области.

2.6. СОВ - специальные программно-аппаратные, либо программные комплексы, выполняющие в автоматическом режиме поиск и обнаружение попыток неправомерного доступа к информации, попыток логического проникновения в информационно-телекоммуникационные сети, попыток внедрения вредоносных программных продуктов.

3. Участники ЗСПД и их полномочия

3.1. Участниками ЗСПД Ивановской области являются:

- координатор деятельности по созданию, развитию (модернизации) и эксплуатации ЗСПД Ивановской области (далее - Координатор);
- оператор ЗСПД Ивановской области;
- пользователи ЗСПД Ивановской области.

3.2. Координатор осуществляет общую координацию и методическое руководство процессами создания, развития (модернизации) и эксплуатации ЗСПД Ивановской области.

3.3. Оператор ЗСПД Ивановской области осуществляет эксплуатацию защищенной сети передачи данных и администрирование ЦУС.

3.4. Пользователями ЗСПД Ивановской области являются органы власти и прочие организации, заключившие соглашение о подключении к ЗСПД Ивановской области или соглашение о межсетевом взаимодействии участников ЗСПД Ивановской области:

- органы исполнительной власти Ивановской области;
- органы местного самоуправления в Ивановской области;
- иные органы и организации, участвующие в предоставлении государственных и муниципальных услуг и выполнении государственных и муниципальных функций.

3.5. Координатор и оператор ЗСПД Ивановской области определяются нормативным правовым актом Департамента развития информационного общества Ивановской области.

3.6. Оператор ЗСПД Ивановской области обеспечивает:

- размещение компонентов ЗСПД Ивановской области - АПСУ в соответствии с перечнем мест размещения компонентов ЗСПД Ивановской области, на основании заключенных соглашений о размещении компонентов ЗСПД;
- развитие (модернизацию) компонентов ЗСПД Ивановской области по согласованию с Координатором;
- подключение ЗСПД Ивановской области к другим защищенным сетям на основании заключенных соглашений о межсетевом взаимодействии участников электронного взаимодействия, за исключением случаев подключения ЗСПД Ивановской области к защищенным сетям федеральных органов исполнительной власти (их структурных подразделений), относительно подключения к которым правовыми актами федеральных органов исполнительной власти утверждены типовые соглашения;
- подключение к защищённой сети передачи данных АПСУ, ПСУ на основании заключенных соглашений о подключении к ЗСПД Ивановской области;
- решение организационных вопросов по взаимодействию с другими защищенными сетями;
- сбор и анализ предложений пользователей электронного взаимодействия по вопросам функционирования ЗСПД Ивановской области;
- консультирование пользователей электронного взаимодействия по вопросам эксплуатации ЗСПД Ивановской области;
- администрирование ЦУС;
- администрирование и обслуживание СОВ;
- информационную безопасность ЦУС, АПСУ и ПСУ оператора ЗСПД Ивановской области;
- проведение технического обслуживания компонентов ЗСПД Ивановской области оператора с возможностью прекращения функционирования защищенной сети передачи данных при обязательном уведомлении пользователей электронного взаимодействия;
- выполнение обязанностей оператора ЗСПД Ивановской области, требований и условий, предусмотренных заключаемыми соглашениями в целях использования ЗСПД Ивановской области.

3.7. Пользователи ЗСПД обеспечивают:

- выполнение обязанностей пользователя ЗСПД Ивановской области, требований и условий, предусмотренных заключаемыми соглашениями в целях использования ЗСПД Ивановской области;
- сохранность и информационную безопасность собственных используемых АПСУ или ПСУ (при наличии), в том числе защиту от несанкционированного доступа к ним третьих лиц;
- сохранность и информационную безопасность АРМ пользователей защищенной сети передачи данных.

4. Условия подключения к ЗСПД

4.1. Порядок подключения пользователей защищенной сети передачи данных, установления межсетевого электронного взаимодействия, отключения пользователей от защищенной сети передачи данных, обновления ключевой информации, действий

пользователей при компрометации ключевой информации определены в Регламенте подключения участника электронного взаимодействия к ЗСПД Ивановской области.

4.2. Подключение к ЗСПД Ивановской области возможно только при выполнении условий обеспечения информационной безопасности в соответствии с действующим законодательством Российской Федерации. В частности обязательным условием является наличие аттестата соответствия требованиям по защите информации на АРМ пользователя или информационно-телекоммуникационной сети, предполагаемых к подключению и работе в ЗСПД Ивановской области (в соответствии с Приказом ФСТЭК России №77 от 29.04.2021 г.).

Приложение 2
к приказу Департамента развития
информационного общества
Ивановской области
от 01.11.2022 № 49/22

РЕГЛАМЕНТ
подключения участника электронного взаимодействия к
защищенной сети передачи данных Ивановской области
(порядковый регистрационный номер сети - №2421)

1. Основные термины и определения

Интернет	Информационно-телекоммуникационная сеть «Интернет»
ПАК	Программно-аппаратный комплекс
ПК	Программный комплекс
ПО	Программное обеспечение
ЗСПД Ивановской области	Защищенная сеть передачи данных Ивановской области – защищенная виртуальная сеть передачи данных, построенная на основе технологии виртуальных защищенных сетей ViPNet (порядковый регистрационный номер сети - №2421)
Департамент	Департамент развития информационного общества Ивановской области
Оператор ЗСПД Ивановской области	Ответственная организация (осуществляющая функции в соответствии с Соглашением – Приложение №6) или структурное подразделение, назначаемое Координатором ЗСПД Ивановской области с целью развития, управления и обслуживания защищенной сети передачи данных
Участник электронного взаимодействия	Государственные органы, органы местного самоуправления и прочие организации, заключившие соглашение о подключении к ЗСПД Ивановской области или соглашение о межсетевом взаимодействии участников ЗСПД Ивановской области
ViPNet Coordinator	ПАК, выполняющий функции универсального сервера виртуальной защищённой сети ViPNet
ViPNet Client	Программное обеспечение, реализующее на рабочем месте пользователя или сервере функцию VPN-клиента и межсетевого экрана
Компрометация ключа	Утрата доверия к используемому ключу по обеспечению безопасности информации
РНПК	Резервный набор персональных ключей

2. Назначение документа

2.1. Настоящий Регламент определяет порядок подключения участника электронного взаимодействия к ЗСПД Ивановской области.

2.2. Регламент разработан во исполнение требований следующих нормативно-правовых и локальных актов:

- ✓ Федеральный закон от 27 июля 2006 года №149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- ✓ Федеральный закон от 27 июля 2006 года №152-ФЗ «О персональных данных»;
- ✓ Постановление Правительства РФ от 01 ноября 2012 года №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- ✓ Приказ ФСБ России от 10 июля 2014 года №378 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;
- ✓ Приказ ФАПСИ Российской Федерации от 13 июня 2001 №152 «Об утверждении инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»;
- ✓ Модель угроз безопасности к информационной системе «Защищенная сеть передачи данных Ивановской области» от 27 октября 2022 года;

3. Общие положения

3.1. Порядок подключения участников электронного взаимодействия к ЗСПД Ивановской области включает в себя следующие этапы:

- приобретение участником электронного взаимодействия за свой счет ПК (или ПАК) ViPNet;
- формирование ответственными лицами Оператора ЗСПД Ивановской области ключевого дистрибутива и передача его уполномоченному представителю подключаемой организации;
- передача ключевого дистрибутива участнику электронного взаимодействия;
- настройка и подключение ПК (или ПАК) ViPNet участника электронного взаимодействия к ЗСПД Ивановской области.

4. Приобретение ПК (или ПАК) ViPNet

4.1. Для подключения к ЗСПД Ивановской области участнику электронного взаимодействия необходимо за свой счет приобрести сертифицированный (ФСБ России и ФСТЭК России) ПК (или ПАК) ViPNet класса защищенности не ниже КСЗ, с лицензией сети ViPNet №2421.

4.2. Для приобретения ПК (или ПАК) ViPNet, а также услуг по их сопровождению участнику электронного взаимодействия необходимо обратиться к официальным представителям АО «ИнфоТекС», перечисленным на сайте организации в сети Интернет.

5. Формирование и передача ключевого дистрибутива

5.1. Для формирования ключевого дистрибутива участнику электронного взаимодействия необходимо направить Оператору ЗСПД Ивановской области заявку в письменной форме на подключение к ЗСПД Ивановской области (Приложение 1).

Заявка рассматривается Оператором ЗСПД Ивановской области в течение трех рабочих дней с момента получения.

5.2. При получении сведений, указанных в п. 5.1, ответственные лица Оператора ЗСПД Ивановской области принимают решение о возможности формирования ключевого дистрибутива.

В случае если сведения, указанные в п. 5.1, предоставлены не в полном объеме, ответственные лица Оператора ЗСПД Ивановской области имеют право:

- запросить у участника электронного взаимодействия сведения, необходимые для формирования ключевого дистрибутива;
- отказать в формировании ключевого дистрибутива, до момента предоставления участником электронного взаимодействия сведений, указанных в п. 5.1.

5.3. В случае принятия решения о возможности формирования ключевого дистрибутива ответственные лица Оператора ЗСПД Ивановской области:

- формируют ключевой дистрибутив;
- размещают ключевой дистрибутив на оптическом носителе информации (оптический носитель предоставляется организацией-заказчиком ключевого дистрибутива);
- помещают оптический носитель с ключевым дистрибутивом в бумажный конверт и запечатывают;
- передают запечатанный конверт уполномоченному представителю организации, направившей заявку на подключение.

5.4. Передача ключевого дистрибутива осуществляется на руки руководителю или доверенному лицу участника электронного взаимодействия при предъявлении им доверенности на получение ключевой информации, в соответствии с действующим законодательством Российской Федерации.

5.5. Порядок организации межсетевого взаимодействия ЗСПД Ивановской области и ViPNet-сетей сторонних организаций регламентирован типовым Соглашением об организации межсетевого взаимодействия ЗСПД Ивановской области и ViPNet-сети сторонней организации, представленным в Приложении 4 к настоящему Регламенту.

5.6. Порядок организации межсетевого взаимодействия ЗСПД Ивановской области со сторонними организациями регламентирован типовым Соглашением об организации межсетевого взаимодействия ЗСПД Ивановской области со сторонней организации, представленным в Приложении 5 к настоящему Регламенту.

6. Настройка и подключение ПК (или ПАК) ViPNet.

6.1. Для подключения к ЗСПД Ивановской области участник электронного взаимодействия самостоятельно осуществляет первичную настройку ПК (или ПАК) ViPNet согласно инструкциям, размещенным в сети Интернет по адресу: <https://infotecs.ru/>.

7. Техническое сопровождение

7.1. При подключении ПК (или ПАК) ViPNet участника электронного взаимодействия к ЗСПД Ивановской области, Оператор ЗСПД Ивановской области оказывает техническое сопровождение защищённого канала на безвозмездной основе.

В рамках технического сопровождения Оператор ЗСПД Ивановской области не оказывает следующие услуги:

- монтаж и коммутацию оборудования;
- техническую поддержку оборудования VipNet;
- иные мероприятия по сопровождению, требующие непосредственного доступа к оборудованию.

7.2. По вопросам технического сопровождения защищенного канала связи необходимо обращаться в Департамент по адресу: support2421@ivreg.ru.

8. Порядок обновления ключевой информации

8.1. Участник электронного взаимодействия обращается к Оператору ЗСПД Ивановской области посредством электронной почты (по адресу: support2421@ivreg.ru) и в письменной форме, сообщая о своём желании произвести замену ключевой информации. К письму необходимо приложить заполненную форму заявки на обновление ключевой информации участника электронного взаимодействия ЗСПД Ивановской области (Приложение 2).

8.2. Срок рассмотрения заявки составляет три рабочих дня с момента подачи. При положительном решении ответственный сотрудник Оператора ЗСПД Ивановской области связывается с контактным лицом участника электронного взаимодействия и согласовывает технологическое окно для проведения работ по замене ключевой информации.

8.3. Участникам электронного взаимодействия, эксплуатирующим для подключения программный комплекс, необходимо помимо заявки сформировать на рабочем месте запрос на обновление ключевой информации согласно инструкциям, размещенным в сети Интернет по адресу: <https://infotecs.ru/>.

8.4. Для участников электронного взаимодействия, эксплуатирующих для подключения программно-аппаратный комплекс замена ключевой информации инициируется ответственными сотрудниками Оператора ЗСПД Ивановской области.

9. Порядок отключения от ЗСПД Ивановской области

9.1. Участники электронного взаимодействия, которые не производили ни одного подключения к ЗСПД Ивановской области (бездействовали) на протяжении более 6 (шести) месяцев будут отключены. Для возобновления доступа необходимо

предоставить заполненную анкету, содержащую актуальную информацию, и получить вновь сформированный дистрибутив ключевых носителей.

9.2. В соответствии с требованиями законодательства в части использования в составе защищенной сети передачи данных только сертифицированных программных, аппаратных и программно-аппаратных продуктов, в ЗСПД Ивановской области, соответственно, возможно использование только таких средств.

По мере вывода из эксплуатации в связи с окончанием срока действия сертификации, Оператором ЗСПД Ивановской области заблаговременно будут рассылаться уведомления о прекращении использования того или иного программного обеспечения или аппаратных продуктов.

Участники электронного взаимодействия самостоятельно отслеживают актуальность версий используемого ими программного, аппаратного и программно-аппаратного обеспечения.

10. Порядок действий при компрометации ключей

10.1. Ключи пользователя ЗСПД Ивановской области могут считаться скомпрометированными в следующих случаях:

- посторонним лицам мог стать доступным файл ключевого дистрибутива;
- посторонним лицам мог стать доступным съемный носитель с паролем доступа к ключевой информации;
- посторонние лица могли получить неконтролируемый физический доступ к ключевой информации, хранящийся на компьютере;
- уволился пользователь, имевший доступ к паролям и ключам.

10.2. В случае компрометации ключей участник электронного взаимодействия обязан прекратить работу на своём узле и незамедлительно сообщить об этом в порядке, установленном в Приложении 3 настоящего Регламента.

Приложение 1
к Регламенту подключения участника
электронного взаимодействия к ЗСПД
Ивановской области

«Заявка на подключение к ЗСПД Ивановской области»

Анкета участника электронного взаимодействия

Информация о пользователе ЗСПД Ивановской области	
1. Полное наименование (в соответствии с учредительными документами)	
2. Местонахождение (в соответствии с учредительными документами):	
3. Фактический адрес:	
4. ОГРН:	
5. Телефон:	
6. ФИО и контакты лица, уполномоченного на получение СКЗИ:	
7. ФИО и контакты технического специалиста, осуществляющего установку СКЗИ:	
8. Выбранный продукт ViPNet (ПК/ПАК):	
9. Количество (шт.):	

«__» _____ 20__ г.
(дата)

(подпись)

(ФИО, должность)

Приложение 2
к Регламенту подключения участника
электронного взаимодействия к ЗСПД
Ивановской области

*«Заявка на обновление ключевой информации участника электронного
взаимодействия ЗСПД Ивановской области»*

Анкета участника электронного взаимодействия

Информация о пользователе ЗСПД Ивановской области	
1. Полное наименование (в соответствии с учредительными документами)	
2. Телефон:	
3. ФИО и контакты лица, уполномоченного на получение СКЗИ:	
4. ФИО и контакты технического специалиста, осуществляющего установку СКЗИ:	
5. Продукт ViPNet (ПК/ПАК):	

«__» _____ 20__ г.
(дата)

(подпись)

(ФИО, должность)

Приложение 3
к Регламенту подключения участника
электронного взаимодействия к ЗСПД
Ивановской области

Порядок действий в случае компрометации ключей пользователя

В случае компрометации ключей пользователя участнику электронного взаимодействия необходимо:

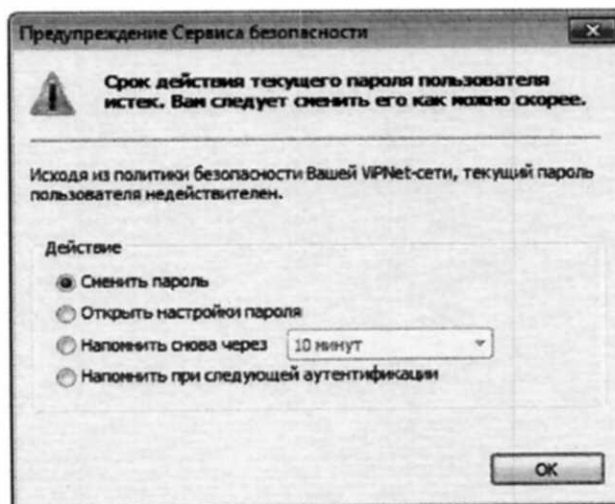
1. Незамедлительно прекратить работу на своём узле и обратиться к Оператору ЗСПД Ивановской области, посредством электронной почты по адресу: support2421@ivreg.ru и телефонной связи, сообщить об инциденте. В письме необходимо указать:

- ✓ Тема – Компрометация ключей;
- ✓ Идентификатор узла;
- ✓ Контактные данные для связи (номер стационарного или мобильного телефона).

2. Сотрудники Оператора ЗСПД Ивановской области, ответственные за подключение к ЗСПД Ивановской области производят необходимые работы по замене ключей, после которых на компьютере пользователя будет произведен перезапуск ПО ViPNet Client.

3. На ПК пользователя в ПО ViPNet Client появится диалоговое окно, в котором участнику электронного взаимодействия необходимо будет указать путь до РНПК (Путь по умолчанию: C:\ProgramFiles(x86)\InfoTeCS\ViPNetClient\user_"Идентификатор_пользователя"\key_disk\dom) и ввести пароль пользователя.

4. После успешного обновления на узле, появится диалоговое окно с информацией о том, что текущий пароль истёк и его следует сменить. Для смены пароля необходимо выбрать пункт «Открыть настройки пароля и установить новый пароль» (рис. 1).



(рис.1)

В случае, если файл РНПК отсутствует на компьютере, необходимо запросить новый дистрибутив с ключевой информацией у Оператора ЗСПД Ивановской области.

Приложение 4
к Регламенту подключения участника
электронного взаимодействия к ЗСПД
Ивановской области

СОГЛАШЕНИЕ

**об организации межсетевого взаимодействия Защищенной сети передачи данных
Ивановской области и ViPNet-сети сторонней организации**

«__» _____ 20__ г.

г. Иваново

Департамент развития информационного общества Ивановской области в лице начальника Хохлова Михаила Евгеньевича, действующего на основании Положения, именуемый далее – Департамент, с одной стороны, и _____ в лице _____, действующего на основании _____, с другой стороны, совместно именуемые – Стороны, заключили настоящее Соглашение о нижеследующем.

I. ПРЕДМЕТ СОГЛАШЕНИЯ

1.1. Настоящее Соглашение определяет условия и порядок организации межсетевого взаимодействия между развернутыми у каждой из Сторон защищенными виртуальными частными сетями, построенным с использованием программного комплекса ViPNet (далее – ПК ViPNet).

1.2. Настоящее Соглашение разработано для обеспечения реализации защищенного и юридически значимого обмена информацией в электронной форме между Сторонами в рамках заключаемых соглашений и регламентов, определяющих порядок информационного взаимодействия, в соответствии с Федеральными законами от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 27.07.2006 № 152-ФЗ «О персональных данных», от 06.04.2011 № 63-ФЗ «Об электронной подписи» в целях организации единого информационного пространства.

1.3. Настоящее Соглашение является безвозмездным.

1.4. Термины и понятия, используемые в настоящем Соглашении, применяются в значениях, установленных действующим законодательством Российской Федерации, эксплуатационной документацией на ПК ViPNet.

II. ОПРЕДЕЛЕНИЕ УСЛОВИЙ МЕЖСЕТЕВОГО ВЗАИМОДЕЙСТВИЯ

2.1. Межсетевое взаимодействие между ViPNet-сетью ЗСПД Ивановской области (ViPNet -сеть №2421) и ViPNet-сетью _____ (ViPNet-сеть № _____) (далее – межсетевое взаимодействие) осуществляется через координаторы ViPNet-сетей Сторон.

2.2. Межсетевое взаимодействие организуется с помощью межсетевого мастер-ключа (ИСММК). ИСММК формирует администратор одной из ViPNet-сетей Сторон для ViPNet-сети другой Стороны.

2.3. Межсетевое взаимодействие организуется в соответствии со схемой межсетевого взаимодействия подписанной уполномоченными представителями Сторон (Приложение №1). Разделение ответственности в рамках межсетевого взаимодействия назначается по границе сетей.

2.4. Стороны выбирают устройства (координаторы ViPNet-сетей), которые будут выполнять функции серверов-шлюзов при межсетевом взаимодействии, а также выделяют узлы своих ViPNet-сетей – абонентские пункты (автоматизированные рабочие места с установленным программным обеспечением ViPNet Client, далее – АП), – которые будут участвовать в межсетевом взаимодействии. Выделенные узлы сетей будут связаны в Центрах управления сетью (далее – ЦУС) взаимодействующих ViPNet-сетей.

2.5. В случае если Стороны включают в состав узлов, участвующих в межсетевом взаимодействии, автоматизированные рабочие места, на которых не установлено программное обеспечение ViPNet, при обмене информацией между Сторонами применяется технология туннелирования.

III. ОРГАНИЗАЦИЯ МЕЖСЕТЕВОГО ВЗАИМОДЕЙСТВИЯ

3.1. Администратор одной из ViPNet-сетей Сторон готовит официальное информационное письмо, в котором информирует другую Сторону о необходимости организации межсетевого взаимодействия.

3.2. В ЦУС и Удостоверяющем и ключевом центре (далее – УКЦ) ViPNet-сети №2421 в соответствии с «Руководство администратора. ViPNet [Центр управления сетью]» и «Руководство администратора. ViPNet [Удостоверяющий и ключевой центр]» производится формирование необходимой адресной и ключевой информации – формирование начального экспорта (ИСММК, справочная информация), включая корневые сертификаты ViPNet-сети №2421 для ViPNet-сети № ____ (далее – начальный экспорт). Начальный экспорт доверенным способом передается в ЦУС ViPNet-сети № ____.

3.3. В ЦУС и УКЦ ViPNet-сети № ____ в соответствии с «Руководство администратора. ViPNet [Центр управления сетью]» и «Руководство администратора. ViPNet [Удостоверяющий и ключевой центр]» производится ввод и обработка (импорт) полученных из ЦУС ViPNet-сети №2421 данных (начального экспорта), установление связей своих узлов с узлами ЦУС ViPNet-сети, предоставившего информацию. Далее в ЦУС и УКЦ ViPNet-сети № ____ создается ответная информация (ответный экспорт) для ЦУС ViPNet-сети №2421, приславшего первичную информацию, включая корневые сертификаты ViPNet-сети № ____.

3.4. Ответная информация (ответный экспорт) доверенным способом передается в ЦУС ViPNet-сети №2421, где она обрабатывается и вводится в действие. На этом этапе завершается процесс организации взаимодействия между ЦУС ViPNet-сети №2421 и ЦУС ViPNet-сети № ____, и дальнейший обмен данными между указанными ЦУС производится в автоматическом режиме посредством программного модуля ViPNet MFTR, входящего в состав ПК ViPNet.

3.5. После рассылки каждым ЦУС ViPNet-сетей Сторон сформированных обновлений ключевой и справочной информации на свои узлы, участвующие в межсетевом взаимодействии, обеспечивается техническая возможность осуществления защищенного обмена между данными узлами информацией в электронной форме, и процедура установления межсетевого взаимодействия считается завершенной.

3.6. После завершения процедуры установления межсетевого взаимодействия уполномоченными представителями Сторон подписывается протокол установления межсетевого взаимодействия (далее – Протокол) (Приложение 3).

3.7. Модификация межсетевого взаимодействия осуществляется в соответствии с «Руководство администратора. ViPNet [Центр управления сетью]» и «Руководство администратора. ViPNet [Удостоверяющий и ключевой центр]» с фиксацией изменений, установленным порядком использования СКЗИ (в Журнале изменений по организации межсетевого взаимодействия сетей ViPNet, Форма журнала в Приложении 4 к настоящему Соглашению) в следующих случаях:

- изменение состава узлов, участвующих в межсетевом взаимодействии;
- плановая смена межсетевого мастер-ключа;
- внеплановая смена межсетевого мастер-ключа;
- компрометация ключевой информации.

IV. ПОРЯДОК ДЕЙСТВИЙ ПРИ ИЗМЕНЕНИИ СОСТАВА УЗЛОВ

4.1. О необходимости изменения состава узлов, участвующих в межсетевом взаимодействии (добавлении или удалении сетевого узла), Стороны уведомляют друг друга в письменной форме с обоснованием необходимости таких изменений.

4.2. При изменении состава узлов ViPNet-сети администратор данной ViPNet-сети в своем ЦУС производит соответствующие изменения в структуре связей своей сети, формирует экспортные данные и передает их в соответствующий ЦУС другой Стороны в автоматическом режиме в соответствии с «Руководство администратора. ViPNet [Центр управления сетью]».

4.3. В ЦУС ViPNet-сети, которого касается данная модификация, в соответствии с «Руководство администратора. ViPNet [Центр управления сетью]» производится обработка (импорт) полученных данных. Далее в ЦУС создается ответная информация (ответный экспорт) для ЦУС, приславшего первичную информацию.

4.4. Ответная информация передается в ЦУС ViPNet-сети, от которого поступила первичная информация, в автоматическом режиме по защищенному каналу связи, где она

обрабатывается и вводится в действие. На этом завершается процесс модификации межсетевого взаимодействия

4.5. После рассылки каждым ЦУС Сторон сформированных обновлений ключевой и справочной информации на свои узлы, которых касается модификация, данные узлы продолжают или прекращают производить защищенный обмен информацией в электронной форме.

V. ПОРЯДОК ДЕЙСТВИЙ ПРИ ПЛАНОВОЙ СМЕНЕ МЕЖСЕТЕВОГО МАСТЕР-КЛЮЧА

5.1. Перед тем как осуществлять плановую смену межсетевого мастер-ключа, администраторы ViPNet-сетей Сторон, для связи ViPNet-сетей которых будет использоваться новый межсетевой мастер-ключ, должны согласовать следующие вопросы:

- выбрать тип межсетевого мастер-ключа, который будет использоваться для связи между сетями; если предполагается использовать симметричный мастер-ключ, то выбрать администратора, который будет создавать новый межсетевой мастер-ключ;
- выбрать и согласовать время проведения смены межсетевого мастер-ключа и последующего обновления ключей шифрования для узлов своих сетей.

5.2. Формирование нового межсетевого мастер-ключа производится в соответствии с «Руководство администратора. ViPNet [Удостоверяющий и ключевой центр]».

5.3. После смены межсетевого мастер-ключа производится процедура создания экспортных данных и приема импортных данных в соответствии с «Руководство администратора. ViPNet [Центр управления сетью]» и «Руководство администратора. ViPNet [Удостоверяющий и ключевой центр]».

5.4. После смены межсетевого мастер-ключа связь между сетевыми узлами взаимодействующих ViPNet-сетей Сторон возможна только после прохождения обновлений ключевой информации на всех соответствующих сетевых узлах данных сетей.

VI. ПОРЯДОК ДЕЙСТВИЙ ПРИ КОМПРОМЕТАЦИИ КЛЮЧЕЙ

Под компрометацией ключей подразумевается утрата доверия к тому, что используемые ключи обеспечивают безопасность информации (целостность, конфиденциальность, подтверждение авторства, невозможность отказа от авторства).

Основные события, квалифицируемые как компрометация ключей, перечислены в «Руководство администратора. ViPNet [Удостоверяющий и ключевой центр]».

При наступлении любого из событий, квалифицируемых как компрометация ключей и перечисленных в «Руководство администратора. ViPNet [Удостоверяющий и ключевой центр]», пользователь (участник межсетевого взаимодействия) должен немедленно прекратить работу на своем АП и сообщить о факте компрометации (или предполагаемом факте компрометации) администратору своей ViPNet-сети.

По факту компрометации ключей должно быть проведено служебное расследование.

Администратор ViPNet-сети в случае компрометации ключей пользователя своей сети в ЦУС и УКЦ своей сети проводит процедуру внеплановой компрометации ключей данного пользователя в соответствии с «Руководство администратора. ViPNet [Центр управления сетью]» и «Руководство администратора. ViPNet [Удостоверяющий и ключевой центр]», которая предполагает выполнение следующих технологических и организационных мероприятий:

- администратор сети оповещает о факте компрометации ключей всех пользователей, связанных со скомпрометированным пользователем; после получения данного сообщения пользователи не должны использовать скомпрометированные ключи;
- администратор сети объявляет ключи данного пользователя скомпрометированными, создает и отправляет экспорт адресно-ключевой информации в сети, с пользователями которых был связан скомпрометированный пользователь;
- администратор сети создает и отправляет (либо передает доверенным способом) новую ключевую информацию как для скомпрометированного пользователя, так и для всех пользователей своей сети, с которыми он был связан;

- после приема и обработки импорта переданных данных администратор сети, пользователи которой взаимодействовали с пользователем, ключи которого скомпрометированы, создает новую ключевую информацию своим пользователям;
- после прохождения обновления новой ключевой информации на всех взаимодействующих узлах ViPNet-сетей Сторон пользователи данных узлов могут продолжать производить защищенный обмен информацией в электронной форме.

Внеплановая смена межсетевого мастер-ключа.

Внеплановая смена ключей выполняется в случае компрометации или угрозы компрометации межсетевого мастер-ключа, на котором происходит организация межсетевого взаимодействия.

В случае компрометации межсетевого мастер-ключа считается скомпрометированной вся ключевая информация, которая используется при межсетевом взаимодействии, и межсетевое взаимодействие должно быть немедленно остановлено.

Для восстановления межсетевого взаимодействия необходимо провести технологические и организационные мероприятия, описанные в разделе «Порядок действий при плановой смене межсетевого мастер-ключа».

VII. ОБЯЗАННОСТИ СТОРОН

Стороны обязуются:

- ✓ обеспечить у пользователей на своей стороне поддержание в работоспособном состоянии аппаратных и программных средств, необходимых для организации и обеспечения межсетевого взаимодействия, в том числе средств криптографической защиты информации (далее – СКЗИ);
- ✓ обеспечить выполнение требований, установленных действующим законодательством Российской Федерации о защите информации, о персональных данных, в том числе требования к информационным системам персональных данных и обеспечению безопасности эксплуатации СКЗИ;
- ✓ предоставлять техническую и другую информацию, необходимую для осуществления взаимодействия в рамках реализации настоящего Соглашения;
- ✓ своевременно информировать другую Сторону об изменении обстоятельств, связанных с реализацией настоящего Соглашения, изменении информации, сообщенной другой Стороне в рамках реализации настоящего Соглашения;
- ✓ без предварительного согласования не производить в настройках и структуре своих ViPNet-сетей изменений, которые могут привести к нарушению межсетевого взаимодействия;
- ✓ выполнять правила работы и требования эксплуатационной документации на используемые для обеспечения межсетевого взаимодействия программные и технические средства, в том числе СКЗИ;
- ✓ немедленно приостанавливать обмен информацией в электронной форме с другой Стороной при получении от нее сообщения о компрометации ключевой информации;
- ✓ не разглашать и предпринимать все необходимые меры с целью предотвращения разглашения любой информации конфиденциального характера, передаваемой между ними либо ставшей им известной в связи с исполнением настоящего Соглашения;
- ✓ определить (назначить) должностных лиц, ответственных за организацию и обеспечение эксплуатации средств защиты информации, средств криптографической защиты информации (далее - СЗИ/СКЗИ), а также системы защиты персональных данных субъектов персональных данных (далее – СЗПДн);
- ✓ определить работников (сотрудников), ответственных за взаимодействие в рамках настоящего Соглашения (далее - уполномоченные лица), и сообщить об определении таких уполномоченных лиц с указанием их контактных данных, в соответствии с Приложением 2 настоящего Соглашения. Об изменении указанных сведений своевременно информировать другую Сторону;
- ✓ в случае невозможности исполнения обязательств по настоящему Соглашению, Стороны немедленно извещают друг друга в письменной форме о факте приостановления выполнения обязательств;
- ✓ все возникающие споры, связанные с обеспечением межсетевого взаимодействия, решаются путем переговоров Сторон.

VIII. ОТВЕТСТВЕННОСТЬ СТОРОН

8.1. Стороны несут ответственность за неисполнение или ненадлежащее исполнение своих обязательств по настоящему Соглашению в соответствии с законодательством Российской Федерации.

8.2. Стороны не несут ответственность за неисполнение или ненадлежащее исполнение обязательств, принятых на себя в соответствии с настоящим Соглашением, если надлежащее исполнение оказалось невозможным вследствие наступления обстоятельств непреодолимой силы.

8.3. Сторона, для которой создалась невозможность исполнения своих обязательств по настоящему Соглашению по причине наступления обстоятельств непреодолимой силы, должна предпринять все возможные действия для извещения другой Стороны о наступлении, ожидаемом сроке действия и прекращении таких обстоятельств.

8.4. Исполнение обязательств возобновляется немедленно после прекращения действия обстоятельств непреодолимой силы.

IX. СРОК ДЕЙСТВИЯ СОГЛАШЕНИЯ

9.1. Настоящее Соглашение вступает в силу с даты его подписания и действует в течение одного года.

9.2. В случае если ни одна из Сторон не известила другую о прекращении действия Соглашения за один месяц до истечения срока его действия, Соглашение считается пролонгированным на следующий год.

9.3. Все изменения и дополнения к настоящему Соглашению действительны только в том случае, если они имеют ссылку на Соглашение, оформлены в письменном виде и подписаны уполномоченными на то представителями Сторон.

9.4. В случае нарушения одной из Сторон обязательств, предусмотренных данным Соглашением, другая Сторона вправе в одностороннем порядке расторгнуть настоящее Соглашение, письменно уведомив об этом за один месяц другую Сторону.

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

X. ЮРИДИЧЕСКИЕ АДРЕСА, КОНТАКТНАЯ ИНФОРМАЦИЯ И ПОДПИСИ СТОРОН

Департамент развития информационного общества Ивановской области:

153000, Ивановская область, г. Иваново, пл. Революции, д. 2/1, к. 319

тел. (4932) 93-13-80, e-mail: mail@it.ivanovoobl.ru

Абонент:

Начальник

Департамента развития информационного общества Ивановской области

_____ М. Е. Хохлов

_____ 20__ года

М.П.

Должность руководителя организации

Название организации

(подпись, инициалы, фамилия)

_____ 20__ года

М.П.

Приложение 1
к Соглашению об организации
межсетевое взаимодействие ЗСПД
Ивановской области и ViPNet-сети
сторонней организации
от «__» _____ 20__ г.

Начальник

Департамента развития информационного
общества Ивановской области

_____ М. Е. Хохлов

от «__» _____ 20__ года

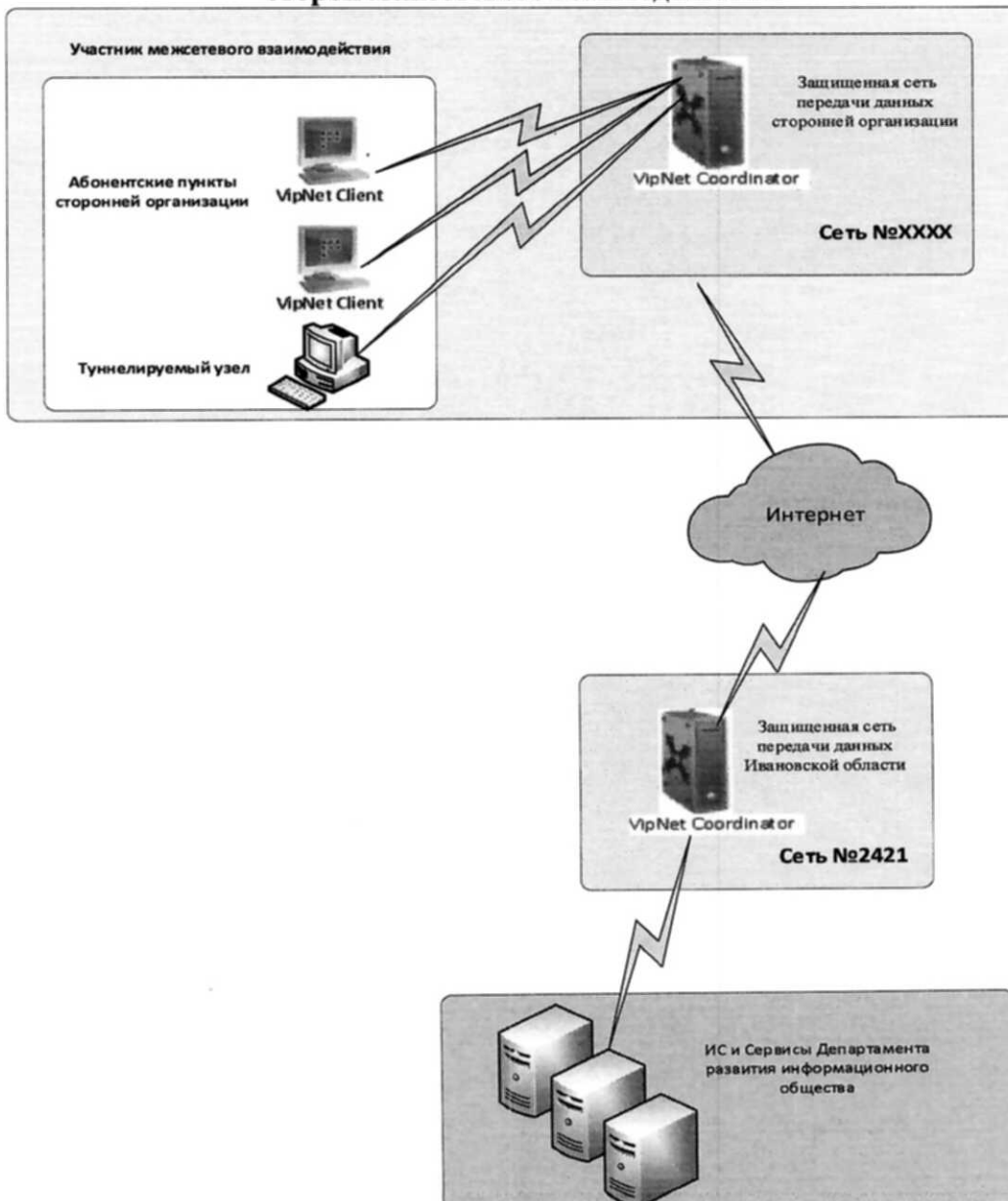
Должность руководителя организации

Название организации

(подпись, инициалы, фамилия)

от «__» _____ 20__ года

**Схема взаимодействия, при подключении через координаторы ViPNet –сетей
сторон межсетевое взаимодействие**



Приложение 2
к Соглашению об организации
межсетевое взаимодействия ЗСПД
Ивановской области и VipNet-сети
сторонней организации
от «__» _____ 20__ г.

Список уполномоченных лиц Организации _____
(от организации участника информационного взаимодействия)

№	Ф. И. О.	Роль	Название АП
1			
2			
3			

Приложение 3
к Соглашению об организации
межсетевого взаимодействия ЗСПД
Ивановской области и ViPNet-сети
сторонней организации
от «_» _____ 20__ г.

Форма протокола установления межсетевого взаимодействия

1. Межсетевое взаимодействие устанавливается между следующими сетями:

№	Номер сети ViPNet	Наименование владельца сети ViPNet
1	№2421	<i>Департамент развития информационного общества Ивановской области</i>
2	№_____	

2. Процедуру установления межсетевого взаимодействия осуществляли:

№	Номер сети ViPNet	Должность	Ф.И.О.
1	№2421		
2	№_____		

3. Передача начального и ответного экспорта между сетями № 2421 и № _____ осуществлялась через администратора СЗИ/СКЗИ, ответственного за организацию и обеспечение безопасности информации (обработки персональных данных), уполномоченного Сторонами на данные действия.
4. Для установления межсетевого взаимодействия использовался индивидуальный симметричный межсетевой мастер-ключ, созданный в ViPNet-сети №2421.
5. Для установления межсетевого взаимодействия были назначены серверы-маршрутизаторы для организации шлюза:

№	Наименование координатора в защищенной сети	№ сети	ViPNet ID сетевого узла (координатора)
1			
2			

6. Перечень сетевых узлов администраторов защищенных сетей:

№	Наименование сетевого узла	№ сети	Ф.И.О. администратора и контактный телефон
1			
2			

7. Перечень сетевых узлов пользователей Организации № _____:

№	Наименование	Версия
1		
2		
3		

8. Перечень туннелируемых узлов Организации ViPNet-сети № _____:

№	Наименование туннелируемого ресурса	IP адрес	DNS-имя	Предназначение

9. Смена межсетевых ключей, изменение состава абонентских пунктов и туннелируемых ресурсов, участвующих в межсетевом взаимодействии, производится после предварительного согласования между администраторами защищенных сетей с помощью ПО ViPNet [Клиент] [Деловая почта] с указанием производимых изменений.
10. Стороны обязуются без предварительного согласия не производить изменений в настройках и структуре защищенных сетей, могущих привести к нарушению межсетевого взаимодействия.

Администратор ViPNet-сети №2421

Администратор ViPNet-сети № _____

(ФИО)

(ФИО)

(подпись)

(подпись)

«__» _____ 20__ г.

«__» _____ 20__ г.

Приложение 4
к Соглашению об организации
межсетевого взаимодействия ЗСПД
Ивановской области и ViPNet-сети
сторонней организации
от «__» _____ 20__ г.

**Журнал
изменений по организации межсетевого взаимодействия сетей ViPNet**

№	Наименование произведенного изменения в межсетевом взаимодействии	Дата изменения	Подпись специалиста, проводившего изменения

.....
Пояснение по ведению Журнала изменений:

1. В журнал заносятся все события, которые относятся к организации защищенного информационного взаимодействия:

- установление межсетевого взаимодействия;*
- выбор Координатора, выполняющего функции сервера-шлюза;*
- формирование межсетевого мастер-ключа;*
- плановая смена межсетевого мастер-ключа;*
- смена ключей при их компрометации;*
- модификация межсетевого взаимодействия (добавление или удаление сетевого узла, изменение состава туннелируемых ресурсов).*

2. Каждая запись Журнала в обязательном порядке заверяется подписью специалиста (администратора СЗИ/СКЗИ), производившего изменения.

Приложение 5
к Регламенту подключения участника
электронного взаимодействия к ЗСПД
Ивановской области

СОГЛАШЕНИЕ
об организации защищенного соединения средствами Защищенной сети передачи
данных Ивановской области со сторонней организацией

«__»____20__ г.

г. Иваново

Департамент развития информационного общества Ивановской области в лице начальника Хохлова Михаила Евгеньевича, действующего на основании Положения, именуемый далее – Департамент, с одной стороны, и _____ в лице _____, действующего на основании _____, именуемый далее – Абонент, с другой стороны, совместно именуемые – Стороны, заключили настоящее Соглашение о нижеследующем.

I. ПРЕДМЕТ СОГЛАШЕНИЯ

1.1. Настоящее Соглашение определяет условия и порядок защищенного соединения средствами Защищенной сети передачи данных Ивановской области (регистрационный порядковый номер - №2421) (далее - ЗСПД) между техническими средствами Сторон с использованием программно-аппаратных средств ViPNet (далее – средства ViPNet).

1.2. Настоящее Соглашение разработано для обеспечения реализации защищенного и юридически значимого обмена информацией в электронной форме между Сторонами в рамках заключаемых соглашений и регламентов, определяющих порядок информационного взаимодействия, в соответствии с Федеральными законами от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 27.07.2006 № 152-ФЗ «О персональных данных», от 06.04.2011 № 63-ФЗ «Об электронной подписи» в целях организации единого информационного пространства.

1.3. Настоящее Соглашение является безвозмездным.

1.4. Термины и понятия, используемые в настоящем Соглашении, применяются в значениях, установленных действующим законодательством Российской Федерации, эксплуатационной документацией на средства ViPNet.

II. ОПРЕДЕЛЕНИЕ УСЛОВИЙ УСТАНОВЛЕНИЯ СОЕДИНЕНИЯ

2.1. Использование защищенного соединения по ЗСПД осуществляется через средства ViPNet Сторон.

2.2. Соединение организуется с помощью файлов с ключевой информацией (DST-файлы). DST-файлы формируются оператором ЗСПД для средств ViPNet другой Стороны.

2.3. Подключение к ЗСПД организуется на основании волеизъявления сторонней организации или в соответствии с необходимостью организации защищенного канала связи. Заявка на подключение оформляется в соответствии с Регламентом.

2.4. Стороны выбирают средства ViPNet, посредством которых будет установлено защищенное соединение. Сторона, которой необходимо подключение к ЗСПД предоставляет оператору ЗСПД информацию об абонентских пунктах (автоматизированных рабочих местах с установленным программным обеспечением ViPNet Client, далее – АП), – которые будут участвовать в сетевом взаимодействии.

III. ОРГАНИЗАЦИЯ СОЕДИНЕНИЯ

Порядок организации соединения приведен в п. 5 Регламента подключения участника электронного взаимодействия к ЗСПД Ивановской области, утверждаемом Департаментом и может быть изменен в соответствии с требованиями законодательства Российской Федерации.

IV. ПОРЯДОК ДЕЙСТВИЙ ПРИ КОМПРОМЕТАЦИИ КЛЮЧЕЙ

Порядок действий при компрометации ключевой информации приведен в п. 10 Регламента подключения участника электронного взаимодействия к защищенной сети передачи данных Ивановской области №2421, утверждаемом Департаментом и может быть изменен в соответствии с требованиями законодательства Российской Федерации.

V. ОБЯЗАННОСТИ СТОРОН

Стороны обязуются:

- ✓ обеспечить у пользователей на своей стороне поддержание в работоспособном состоянии аппаратных и программных средств, необходимых для организации соединения, в том числе средств криптографической защиты информации (далее – СКЗИ);
- ✓ обеспечить выполнение требований, установленных действующим законодательством Российской Федерации о защите информации, о персональных данных, в том числе требования к информационным системам персональных данных и обеспечению безопасности эксплуатации СКЗИ;
- ✓ предоставлять техническую и другую информацию, необходимую для осуществления взаимодействия в рамках реализации настоящего Соглашения;
- ✓ своевременно информировать другую Сторону об изменении обстоятельств, связанных с реализацией настоящего Соглашения, изменении информации, сообщенной другой Стороне в рамках реализации настоящего Соглашения;
- ✓ соблюдать правила работы и требования эксплуатационной документации на используемые для обеспечения межсетевое взаимодействие программные и технические средства, в том числе СКЗИ;
- ✓ немедленно приостанавливать обмен информацией в электронной форме с другой Стороной при получении от нее сообщения о компрометации ключевой информации;
- ✓ не разглашать и предпринимать все необходимые меры с целью предотвращения разглашения любой информации конфиденциального характера, передаваемой между ними либо ставшей им известной в связи с исполнением настоящего Соглашения;
- ✓ в случае невозможности исполнения обязательств по настоящему Соглашению, Стороны немедленно извещают друг друга в письменной форме о факте приостановления выполнения обязательств;
- ✓ все возникающие споры, связанные с обеспечением соединения, решаются путем переговоров Сторон.

VI. ОТВЕТСТВЕННОСТЬ СТОРОН

6.1. Стороны несут ответственность за неисполнение или ненадлежащее исполнение своих обязательств по настоящему Соглашению в соответствии с законодательством Российской Федерации.

6.2. Стороны не несут ответственность за неисполнение или ненадлежащее исполнение обязательств, принятых на себя в соответствии с настоящим Соглашением, если надлежащее исполнение оказалось невозможным вследствие наступления обстоятельств непреодолимой силы.

6.3. Сторона, для которой создавалась невозможность исполнения своих обязательств по настоящему Соглашению по причине наступления обстоятельств непреодолимой силы, должна предпринять все возможные действия для извещения другой Стороны о наступлении, ожидаемом сроке действия и прекращении таких обстоятельств.

6.4. Исполнение обязательств возобновляется немедленно после прекращения действия

обстоятельств непреодолимой силы.

VII. СРОК ДЕЙСТВИЯ СОГЛАШЕНИЯ

7.1. Настоящее Соглашение вступает в силу с даты его подписания и действует бессрочно.

7.2. Все изменения и дополнения к настоящему Соглашению действительны только в том случае, если они имеют ссылку на Соглашение, оформлены в письменном виде и подписаны уполномоченными на то представителями Сторон.

7.3. В случае нарушения одной из Сторон обязательств, предусмотренных данным Соглашением, другая Сторона вправе в одностороннем порядке расторгнуть настоящее Соглашение, письменно уведомив об этом за один месяц другую Сторону.

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

VIII. ЮРИДИЧЕСКИЕ АДРЕСА, КОНТАКТНАЯ ИНФОРМАЦИЯ И ПОДПИСИ СТОРОН

Департамент развития информационного общества Ивановской области:

153000, Ивановская область, г. Иваново, пл. Революции, д. 2/1, к. 319

тел. (4932) 93-13-80, e-mail: mail@it.ivanovoobl.ru

Абонент:

Начальник

Департамента развития информационного общества Ивановской области

_____ М. Е. Хохлов

_____ 20__ года

М.П.

Должность руководителя организации

Название организации

(подпись, инициалы, фамилия)

_____ 20__ года

М.П.

Приложение 6
к Регламенту подключения участника
электронного взаимодействия
к ЗСПД Ивановской области

СОГЛАШЕНИЕ

о выполнении функций Оператора Защищенной сети передачи данных Ивановской области силами привлекаемой организации

«__» _____ 20__ г.

г. Иваново

Департамент развития информационного общества Ивановской области в лице начальника Хохлова Михаила Евгеньевича, действующего на основании Положения, именуемый далее – Департамент, с одной стороны, и _____ в лице _____, действующего на основании _____, именуемый далее – Оператор, с другой стороны, совместно именуемые – Стороны, заключили настоящее Соглашение о нижеследующем.

I. ПРЕДМЕТ СОГЛАШЕНИЯ

1.1. Настоящее Соглашение определяет условия и порядок исполнения обязательств Оператора Защищенной сети передачи данных Ивановской области (регистрационный порядковый номер - №2421) (далее - ЗСПД).

1.2. Настоящее Соглашение разработано для обеспечения работоспособности, отказоустойчивости ЗСПД сотрудниками Оператора, а также для оперативного получения информации о возможностях развития и масштабирования ЗСПД.

1.3. Настоящее Соглашение является безвозмездным.

1.4. Термины и понятия, используемые в настоящем Соглашении, применяются в значениях, установленных действующим законодательством Российской Федерации, эксплуатационной документацией на средства VipNet.

II. ПРАВА И ОБЯЗАННОСТИ СТОРОН

2.1. Департамент обязан:

- предоставлять Оператору необходимую информацию, требуемую для обеспечения его деятельности в рамках настоящего Соглашения;
- обеспечивать доступ к оборудованию, узлам сети, программным и прочим продуктам, посредством которых функционирует ЗСПД;
- своевременно реагировать на рекомендации и требования Оператора в части соблюдения мероприятий, касающихся работоспособности ЗСПД;

2.2. Оператор обязан:

- в рамках настоящего Соглашения обеспечить работоспособность и отказоустойчивость ЗСПД при условии выполнения Департаментом обязательств согласно п. 6;
- при выявлении инцидентов немедленно сообщать о них в Департамент;
- выдавать в адрес Департамента рекомендации по развитию, масштабированию, обеспечению отказоустойчивости ЗСПД при их наличии; осуществлять технические работы на ЗСПД только по согласованию с Департаментом.
- при исполнении своих обязательств руководствоваться официальной документацией на обслуживаемые программные и аппаратные средства, сети передачи данных, а также Регламент ЗСПД, утверждаемые Департаментом.

2.3. Департамент вправе:

- получать необходимую информацию о деятельности Оператора в рамках настоящего соглашения по первому требованию;
- лично присутствовать при проведении работ Оператором в рамках настоящего соглашения.

2.4. Оператор вправе:

- требовать от Департамента информацию, необходимую для исполнения им обязательств в соответствии с настоящим Соглашением;

- в случаях, когда Департамент не может, в силу обстоятельств, принять однозначного решения на выполнение тех или иных работ, необходимых для устранения критических неисправностей, принимать самостоятельные решения с предварительным уведомлением Департамента.

III. СРОКИ И УСЛОВИЯ ОКАЗАНИЯ УСЛУГ

3.1. Настоящее Соглашение вступает в силу с момента подписания его Сторонами и действует до «__» _____ 20__ года.

3.2. Соглашение, может быть, расторгнуто досрочно по взаимному согласию сторон с письменным уведомлением не менее чем за 1 (один) месяц.

IV. ОТВЕТСТВЕННОСТЬ СТОРОН

4.1. За неисполнение или ненадлежащее исполнение обязательств по настоящему Соглашению Стороны несут ответственность в соответствии с действующим законодательством Российской Федерации.

4.2. Сторона, не исполнившая или ненадлежащим образом исполнившая обязательство, не несет ответственности, если докажет, что надлежащее исполнение оказалось невозможным вследствие непреодолимой силы, то есть чрезвычайных и непредотвратимых при данных условиях обстоятельств, возникших после заключения настоящего Соглашения.

4.3. Сторона, для которой создавалась невозможность исполнения обязательств по Соглашению по указанным выше обстоятельствам, должна уведомить об этом другую Сторону в течение трех календарных дней с момента наступления этих обстоятельств. Если Сторона не уведомила о наступлении вышеуказанных обстоятельств, то она не вправе ссылаться на них, как на причину неисполнения или ненадлежащего исполнения своих обязательств.

4.4. Вышеуказанные обстоятельства п. 4.2 и п. 4.3, освобождающие Стороны от ответственности и возмещения убытков, должны быть соответствующим образом удостоверены в компетентных органах.

V. ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ РЕЖИМА КОНФИДЕНЦИАЛЬНОСТИ

5.1. Департамент и Оператор обязуются строго хранить конфиденциальность информации, полученной в результате осуществления деятельности в рамках настоящего Соглашения, и будут принимать все возможные меры для защиты этой информации от раскрытия.

5.2. Передача конфиденциальной информации третьим лицам или иное ее разглашение может осуществляться только в порядке, предусмотренном законодательными актами Российской Федерации.

VI. ПОРЯДОК РАЗРЕШЕНИЯ СПОРОВ

6.1. Все споры, возникающие между Сторонами в связи с исполнением обязательств по настоящему Соглашению, решаются путем двухсторонних переговоров.

6.2. В случае невозможности нахождения приемлемого для обеих Сторон решения спорного вопроса путем переговоров, споры разрешаются арбитражным судом по месту нахождения Оператора.

VII. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

7.1. Настоящее Соглашение вступает в силу с момента его подписания сторонами и действует до исполнения сторонами своих обязательств.

7.2. Все изменения и дополнения к настоящему Соглашению могут вноситься по инициативе каждой из Сторон, составляются в письменной форме в виде дополнительных соглашений, вступают в силу после подписания Сторонами и являются неотъемлемой частью настоящего Соглашения.

7.3. Настоящее Соглашение составлено в двух подлинных экземплярах, имеющих равную юридическую силу, по одному экземпляру для каждой Стороны.

VIII. ЮРИДИЧЕСКИЕ АДРЕСА, КОНТАКТНАЯ ИНФОРМАЦИЯ И ПОДПИСИ
СТОРОН

Департамент развития информационного общества Ивановской области:

153000, Ивановская область, г. Иваново, пл. Революции, д. 2/1, к. 319

тел. (4932) 93-13-80, e-mail: mail@it.ivanovoobl.ru

Оператор:

Начальник

Департамента развития информационного
общества Ивановской области

_____ М. Е. Хохлов

_____ 20__ года

М.П.

Должность руководителя организации

Название организации

(подпись, инициалы, фамилия)

_____ 20__ года

М.П.