ПРАВИТЕЛЬСТВО УЛЬЯНОВСКОЙ ОБЛАСТИ

П О С Т А Н О В Л Е Н И Е

11 ноября 2016 г. № 534-П

Экз.№_____

г. Ульяновск

Об утверждении Порядка использования защищённой сети передачи данных Правительства Ульяновской области

В целях обеспечения информационно-технологического взаимодействия информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме, для осуществления государственных функций, а также совершенствования функционирования региональной системы межведомственного электронного взаимодействия в Ульяновской области Правительство Ульяновской области п о с т а н о в л я е т:

1. Утвердить прилагаемый Порядок использования защищённой сети передачи данных Правительства Ульяновской области.

2. Определить оператором защищённой сети передачи данных Правительства Ульяновской области областное государственное казённое учреждение «Корпорация развития интернет-технологий – многофункциональный центр предоставления государственных и муниципальных услуг в Ульяновской области».

Исполняющий обязанности
Губернатора области А.И.Якунин

Ульяновская область Правительство

УТВЕРЖДЁН

постановлением Правительства
Ульяновской области
от 11 ноября 2016 г. № 534-П

ПОРЯДОК
использования защищённой сети передачи данных Правительства Ульяновской области

1. Общие положения

1.1. Порядок использования защищённой сети передачи данных Правительства Ульяновской области (далее – Порядок) определяет регламент взаимодействия Правительства Ульяновской области, подразделений, образуемых в Правительстве Ульяновской области, исполнительных органов государственной власти Ульяновской области и подведомственных им государственных учреждений, органов местного самоуправления муниципальных образований Ульяновской области, а также юридических лиц (далее – Пользователи) при присоединении к защищённой сети передачи данных Правительства Ульяновской области с целью осуществления государственных и муниципальных функций, информационного обмена для предоставления государственных и муниципальных услуг и содержит технологические требования к присоединению, описание прав и обязанностей Пользователей при использовании сети передачи данных, а также показатели (критерии) качества сервисов сети передачи данных.

1.2. Защищённая сеть передачи данных Правительства Ульяновской области (далее – ЗСПД) – виртуальная, развёрнутая на существующих физических каналах связи защищённая телекоммуникационная сеть, построенная с использованием технологий VIPNet, являющаяся частью информационно-телекоммуникационной структуры исполнительных органов государственной власти Ульяновской области и органов местного самоуправления муниципальных образований Ульяновской области.

1.3. Целью использования ЗСПД является обеспечение безопасного информационного взаимодействия между Пользователями при осуществлении государственных и муниципальных функций и предоставлении государственных и муниципальных услуг.

1.4. ЗСПД предназначена для решения следующих задач:

обеспечение безопасного информационного взаимодействия в электронной форме при предоставлении государственных и муниципальных услуг и исполнении государственных и муниципальных функций;

взаимодействие информационных систем Пользователей по защищённым каналам связи;

обеспечение безопасной передачи информации через открытые каналы связи между Пользователями в соответствии с законодательством Российской Федерации;

обеспечение информационного взаимодействия с защищёнными сетями территориальных органов федеральных органов исполнительной власти.

1.5. ЗСПД не предназначена для подключения информационных систем, локальных вычислительных сетей и средств вычислительной техники, применяемых для хранения, обработки или передачи информации, содержащей сведения, составляющие государственную тайну.

1.6. Взаимодействие с защищёнными информационными сетями территориальных органов федеральных органов исполнительной власти осуществляется по защищённым каналам передачи данных.

2. Состав ЗСПД

ЗСПД состоит из линий связи, узлов ядра, центра управления сетью и узлов доступа.

Линии связи – линии передач, физические цепи и линейно-кабельные сооружения связи;

узлы ядра – высокопроизводительные программно-аппаратные комплексы, реализующие функции маршрутизации, криптографической защиты передаваемых данных, а также контроля и разграничения доступа пользователей к различным информационным ресурсам ЗСПД;

центр управления сетью – программно-аппаратный комплекс управления узлами и ключевой (криптографической) информацией ЗСПД, а также контроля состояния узлов доступа и узлов ядра ЗСПД с функцией оперативного оповещения участников;

узлы доступа – программные или программно-аппаратные комплексы объектового уровня, служащие для подключения Пользователей к узлам ядра ЗСПД.

3. Права и обязанности Пользователя

3.1. Пользователь обязан:

обеспечивать информационную безопасность каждого подключаемого компонента ЗСПД в соответствии с законодательством Российской Федерации;

обеспечивать беспрепятственный доступ технических специалистов к оборудованию;

обеспечить надлежащие условия для работы оборудования в рамках ЗСПД, установленного на объекте Пользователя. Пользователь не вправе осуществлять воздействие на оборудование, включая отключение его от сети связи или сети электропитания, без согласования с оператором;

обеспечить самостоятельное обслуживание собственного оборудования (далее – Пользовательский терминал) в надлежащие сроки и надлежащего качества;

обеспечить подключение оператором ЗСПД;

обеспечить приёмку по акту приёма-передачи оборудования, если для организации ЗСПД необходима его установка на объекте Пользователя;

использовать оборудование, сертифицированное в соответствии с Федеральным законом от 07.07.2003 № 126-ФЗ «О связи»;

соблюдать требования к узлам доступа для подключения информационных систем Пользователя (приложение № 1 к Порядку);

при использовании ЗСПД не допускать препятствий в работоспособности данной сети и осуществления иных несанкционированных действий, в том числе распространения спама и вредоносного программного обеспечения с Пользовательских терминалов;

заключить соглашение о подключении к ЗСПД;

получить ключевой дистрибутив на основании доверенности (приложение № 2 к Порядку);

обеспечить размещение средств криптографической защиты информации;

назначить ответственного за обеспечение безопасного функционирования ЗСПД;

обеспечить учёт всех средств защиты информации в специальных журналах;

обеспечить содержание оборудования Пользователя в специально предназначенном для этого помещении (месте), отвечающем требованиям производителя данного оборудования.

3.2. Пользователь имеет право:

запрашивать и получать от оператора консультации, информацию и документы по вопросам эксплуатации и управления ЗСПД, проект соглашения о подключении к ЗСПД;

получать доступ к ЗСПД в соответствии с настоящим Порядком и соглашением о подключении к ЗСПД.

4. Права и обязанности оператора

4.1. Оператор обязан:

выполнять функции по организации ЗСПД в интересах Пользователей в соответствии с законодательством Российской Федерации, нормативными правовыми актами Российской Федерации в области связи, за исключением перерывов для проведения плановых работ;

уведомлять о проведении плановых работ Пользователя не менее чем за сутки до начала работ с указанием их продолжительности;

извещать Пользователя о необходимости проведения внепланового перерыва в функционировании ЗСПД по электронной почте или по факсу;

устранять неисправности, препятствующие функционированию ЗСПД;

урегулировать разногласия при подключении и эксплуатации ЗСПД.

4.2. Оператор имеет право:

в случае нарушения Пользователем требований, установленных законодательством Российской Федерации, настоящим Порядком и (или)

соглашением о подключении к ЗСПД, приостановить оказание услуг связи до устранения нарушения;

разрабатывать проекты документов по вопросам эксплуатации и управления ЗСПД;

запрашивать и получать от Пользователей информацию об использовании ими ЗСПД.

5. Функции оператора

Оператор осуществляет следующие функции:

принимает и рассматривает заявки Пользователей на подключение к ЗСПД;

заключает соглашения о подключении Пользователей к ЗСПД;

предоставляет ключевой дистрибутив Пользователям;

ведёт реестр Пользователей;

определяет требования к применяемому в ЗСПД оборудованию, а также к его количественным и качественным характеристикам;

обеспечивает надлежащее техническое обслуживание ЗСПД;

осуществляет техническое сопровождение и профилактические работы узлов ядра ЗСПД;

обеспечивает доступ Пользователей к компонентам ЗСПД и сетевым ресурсам ЗСПД.

6. Условия подключения к ЗСПД

6.1. Для подключения к ЗСПД Пользователь предоставляет оператору заявку на подключение к ЗСПД (приложение № 3 к Порядку).

6.2. Оператор регистрирует заявки на подключение к ЗСПД в день их поступления в журнале регистрации заявок на подключение к ЗСПД.

6.3. Оператор в течение трёх рабочих дней с даты поступления рассматривает заявки на подключение к ЗСПД и принимает решение о подключении Пользователя к ЗСПД либо об отказе в подключении.

6.4. О принятом решении Пользователь уведомляется оператором в течение двух рабочих дней посредством направления почтового отправления, с использованием информационно-телекоммуникационной сети «Интернет» либо передачи лично Пользователю уведомления о подключении к ЗСПД с приложением проекта соглашения о подключении либо уведомления об отказе в подключении к ЗСПД с указанием причины отказа.

6.5. Соглашение о подключении к ЗСПД должно содержать:

перечень информации, передача которой осуществляется с использованием ЗСПД и которая необходима для оказания государственных или муниципальных услуг либо для осуществления государственных и муниципальных функций;

права и обязанности сторон;

ответственность сторон;

основания и порядок расторжения соглашения.

6.6. Пользователь после получения проекта соглашения о подключении к ЗСПД в течение пяти рабочих дней уведомляет оператора о согласии на подписание соглашения либо об отказе в подписании соглашения.

Разногласия, возникшие у сторон при подписании соглашения о подключении к ЗСПД, разрешаются в рабочем порядке.

6.7. После подписания соглашения о подключении к ЗСПД оператор осуществляет подключение Пользователя к ЗСПД в течение десяти рабочих дней.

ПРИЛОЖЕНИЕ № 1

к Порядку

ТРЕБОВАНИЯ
к узлам доступа для подключения информационных систем Пользователей

1. Общие положения

Требования к узлам доступа для подключения информационных систем Пользователей (далее – Требования) определяют рекомендации, соответствие которым необходимо обеспечить Пользователю для подключения к ЗСПД.

Для функционирования различных информационных систем, требующих в рамках ЗСПД обеспечения криптографической защиты информации при взаимодействии по открытым общедоступным сетям, Пользователям необходимо организовать подключение автоматизированных систем с различной архитектурой построения, расположения и назначения.

Для подключения к ЗСПД Пользователем может быть использован один из вариантов использования продукции открытого акционерного общества «ИнфоТеКС» (далее – Инфотекс):

кластер программно-аппаратного комплекса (далее – ПАК) HW1000;

одиночный ПАК HW1000;

одиночный ПАК HW100 модификаций A/B/C;

ViPNetClient.

2. Рекомендации по номенклатуре используемых решений

В таблице 1 представлены рекомендации по выбору типа ПАК ViPNet в зависимости от количества используемых Пользователем сетевых узлов (автоматизированных рабочих мест (далее – АРМ), серверов, терминалов), обрабатывающих подлежащую защите информацию.

Таблица 1

№ п/п	Количество серверов, АРМ и терминалов в защищаемом сегменте	Рекомендуемая номенклатура решений Инфотекс
1.	Более 500	HW2000
2.	От 10 до 500	HW1000
3.	От 6 до 10	HW100C
4.	От 3 до 5	HW100B
5.	От 1 до 3	HW100A
6.	1	ViPNet Client

3. Рекомендации по номенклатуре решений, обеспечивающих необходимую пропускную способность каналов связи

В таблице 2 представлены рекомендации по выбору типа ПАК ViPNet в зависимости от необходимой пропускной способности при подключении Пользователя к ЗСПД.

Таблица 2

№ п/п	Необходимая производительность шифрования	Рекомендуемая номенклатура решений Инфотекс
1.	До 2,7 Гбит/с	HW2000
2.	До 250 Мбит/с	HW1000
3.	До 20 Мбит/с	HW100A/B/C

ПРИЛОЖЕНИЕ № 2

к Порядку

ДОВЕРЕННОСТЬ
на получение дистрибутива ключей

_____ №_____
(дата)

_____
(наименование организации)

в лице _____,
(Ф.И.О. руководителя)

действующего на основании_____, уполномочивает

_____
(Ф.И.О., должность)

_____
(серия и номер паспорта, кем и когда выдан, код подразделения)

получить в областном государственном казённом учреждении «Корпорация развития интернет-технологий – многофункциональный центр предоставления государственных и муниципальных услуг в Ульяновской области» ключевой дистрибутив (файл с расширением *dst) к VipNet Клиент в сеть № 2500.

Настоящая доверенность выдана сроком до _____20__г.

Подпись лица, получившего доверенность _____

_____	_____	_____
(наименование должности руководителя организации)	(подпись)	(расшифровка подписи)

_____

0111кк1

ПРИЛОЖЕНИЕ № 3

к Порядку

ЗАЯВКА
на подключение к защищённой сети передачи данных
Правительства Ульяновской области

1. Полное наименование организации (на основании учредительных документов) _____

_____

2. Сокращённое наименование организации _____

3. ИНН/КПП организации _____

_____

4. Юридический адрес организации с индексом _____

_____

5. Фактический (почтовый) адрес организации с индексом _____

_____

6. Должность, фамилия, имя, отчество руководителя _____

_____

7. Цель подключения к защищённой сети (ССТУ/ГИС ГМП/АРМ платежи/ ТВИС/ другое)_____

_____

8. Тип подключения к защищённой сети (VipNet Client/ПАК VipNet Coordinator) _____

_____

9. Количество приобретаемых лицензий/ПАКов _____

_____

10. Работы по установке и настройке VipNet Client/ПАК VipNet Coordinator _____

_____

11. Фамилия, имя, отчество, должность, тел./e-mail пользователя VipNet Client/ПАК VipNet Coordinator _____

_____

12. Должность, фамилия, имя, отчество системного администратора/ технического специалиста в организации _____

_____

13. Контактные телефоны, e-mail системного администратора/ технического специалиста в организации _____

_____

_____

0111кк1