

УТВЕРЖДАЮ

Директор

ГКУ ТО «ЦИТТО»

 Усманов А. Р.

« 02 » июля 2024 г.

**РЕГЛАМЕНТ ПОДКЛЮЧЕНИЯ
К ЗАЩИЩЕННОЙ СЕТИ ПЕРЕДАЧИ ДАННЫХ
УЧАСТНИКОВ ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ**

Перечень сокращений

АРМ	Автоматизированное рабочее место
ГКУ ТО "ЦИТТО"	Государственное казенное учреждение "Центр информационных технологий Тюменской области"
ЗСПД ViPNet	Защищенная сеть передачи данных Правительства Тюменской области
ИБ	Информационная безопасность
ИС	Информационная система (в т.ч. государственная информационная система и информационная система персональных данных)
ЛВС	Локальная вычислительная сеть
УИВ	Участник информационного взаимодействия
ПАК	Программно-аппаратный комплекс
СКЗИ	Средства криптографической защиты информации
ФСБ	Федеральная служба безопасности Российской Федерации
ФСТЭК	Федеральная служба по техническому и экспортному контролю
ЦОД ПТО	Центр обработки данных Правительства Тюменской области
Оператор	Оператор ЗСПД ViPNet — ГКУ ТО "ЦИТТО"
Заявитель	Участник информационного взаимодействия, направивший заявку на подключение к ЗСПД
Администратор безопасности УИВ	Лицо, отвечающее за организационные вопросы при подключении к ЗСПД со стороны УИВ
Администратор ИБ	Администратор информационной безопасности ЗСПД

ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Предмет регулирования

Настоящий Регламент определяет порядок подключения участников информационного взаимодействия к защищенной сети передачи данных ViPNet ГКУ ТО «ЦИТТО».

Актуальная версия Регламента размещена на официальном сайте ГКУ ТО ЦИТТО в разделе «Главная» - «Направление деятельности» - «Служащим» - «Удаленный доступ».

1.2 Общие сведения о ЗСПД ViPNet

Виртуальная защищенная сеть передачи данных Правительства Тюменской области построена на основе технологии виртуальных защищенных сетей ViPNet.

Оператором ЗСПД ViPNet является ГКУ ТО "ЦИТТО" (далее — Оператор).

Почтовый адрес Оператора: 625000, г.Тюмень, ул.Советская, д.61

Адрес электронной почты Администратор ИБ ЗСПД: oib@72to.ru

1.3 Участники информационного взаимодействия

Участниками информационного взаимодействия являются организации, подключающиеся к ЗСПД ViPNet, при наличии действующего контракта на сопровождение ИС.

1.4 Нормативные акты

Настоящий регламент разработан во исполнение требований следующих нормативно-правовых и локальных нормативных актов:

- 1) Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- 2) Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- 3) Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»;
- 4) Состав и содержание 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, утверждены приказом Федеральной службы безопасности Российской Федерации от 10.07.2014 №

378;

- 5) Инструкция 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, утверждена приказом Федерального агентства правительственной связи и информации от 13.06.2001 № 152;
- 6) Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)», утверждено приказом Федеральной службы безопасности Российской Федерации от 09.02.2005 г. № 66).

1.5 Условия подключения к ЗСПД

Требования Регламента распространяются на организации, подключаемые к ЗСПД. Описанные в настоящем разделе условия являются обязательными для начала работ по подключению участников информационного взаимодействия к ЗСПД.

Автоматизированные рабочие места УИВ, подключаемые к ЗСПД, должны соответствовать требованиям информационной безопасности. УИВ обязаны обеспечить наличие на АРМ следующих средств защиты информации:

1. Средство антивирусной защиты (например: Kaspersky Endpoint Security, Dr.Web Desktop Security Suite);
2. Средства защиты от несанкционированного доступа (например: Secret Net Studio, Dallas Lock);
3. Криптопровайдер, сертифицированный ФСБ России как средство криптографической защиты информации (например: ViPNet CSP, КриптоПро CSP).

2. Варианты подключения к ЗСПД

В целях подключения к ЗСПД УИВ выбирает один из следующих вариантов подключения в зависимости от количества пользователей, используемых операционных систем.

Вариант 1 — Программно-аппаратный доступ

Подключение к защищенной сети ViPNet обеспечивается через программно-аппаратный комплекс ViPNet Coordinator HW 4, сертифицированный ФСБ по классу не

ниже КС2. Для подключения должны быть выполнены требования, указанные в п.1.5 Регламента. В данном случае УИВ принимает на себя обязательство по обеспечению технической поддержки купленного устройства.

Вариант 2 — Клиентский доступ

Данный Вариант применим в случае необходимости клиентского доступа к ЗСПД VipNet. Подключение АРМ УИВ к ЗСПД обеспечивается через программное обеспечение VipNet Client 4.x, сертифицированное ФСБ по классу не ниже КС2. Для подключения должны быть выполнены требования, указанные в п.1.5 Регламента. В таком случае УИВ принимает на себя обязательство по обеспечению технической поддержки эксплуатируемого УИВ программного обеспечения VipNet Client 4.x.

Вариант 3 — Межсетевое взаимодействие

Данный вариант применим в случае необходимости организации межсетевого взаимодействия существующих сетей VipNet УИВ с ЗСПД VipNet ГКУ ТО «ЦИТТО». Подключаемые сети VipNet должны быть по классу не ниже КС2. Для подключения должны быть выполнены требования, указанные в п.1.5 Регламента.

3. Порядок подключения к защищенной сети передачи данных

Подключение участников информационного взаимодействия к ЗСПД осуществляется в следующем порядке:

- 1) Заявитель выбирает вариант подключения к ЗСПД (см. раздел 2 настоящего Регламента);
- 2) Заявитель направляет на электронную почту или по адресу местонахождения Оператора заполненную заявку на подключение к ЗСПД;

Заявка на подключение включает в себя:

- официальное письмо на имя руководителя Оператора;
 - заполненная анкета на подключение (Приложение № 1);
 - заполненная анкета на Соглашение (Приложение № 2) при выборе варианта 3 раздела 2 настоящего Регламента.
- 4) Оператор проводит рассмотрение заявки, по результатам которого в течении 10 рабочих дней направляет в адрес Заявителя принятое решение.

В случае положительного решения о подключении заявителя к ЗСПД:

- а) для варианта 1 и 2 подключения:

- Заявитель осуществляет закупку необходимого программного обеспечения или программно-аппаратного комплекса для подключения к ЗСПД;
- Информация о лицензии на приобретенное ПО (ПАК) направляется на электронную почту Администратора ИБ ЗСПД;
- Администратор ИБ ЗСПД проводит формирование файла ключевого дистрибутива (DST) и направляет ключевую информацию Заявителю доверенным способом передачи;
- Заявитель проводит работы по инициализации ViPNet узла с использованием файла ключевого дистрибутива (DST);
- Администратор ИБ проверяет доступность узла сети.

б) для варианта 3 подключения:

- Заявитель, при необходимости, осуществляет заключение Соглашения об установлении защищенного межсетевого взаимодействия. Реквизиты заключенного Соглашения направляются на электронную почту Администратора ИБ ЗСПД;
- Администратор ИБ и Администратор сторонней сети ViPNet УИБ согласовывают время проведения работ;
- Администратор ИБ осуществляет формирование файла с межсетевой информацией и индивидуального симметричного межсетевого мастер-ключа (далее – мастер-ключ);
- Администратор ИБ доверенным способом передает экспортные файлы Администратору сторонней сети ViPNet УИБ;
- Администратор сторонней сети ViPNet УИБ принимает межсетевую информацию, импортирует мастер-ключ, создает файл с ответной межсетевой информацией и передает Администратору ИБ;
- Администратор ИБ проверяет доступность узла сети.

Анкета на подключение к ЗСПД Правительства Тюменской области

1. Сведения об Участнике информационного взаимодействия (УИВ)

1.	Сокращенное наименование организации	
2.	Полное наименование организации	
3.	ИНН / ОГРН	
4.	Юридический адрес организации	
5.	Фактический (почтовый) адрес организации	
6.	Телефон организации (с кодом города)	

2. Информация для подключения к ЗСПД

7.	Выбранный вариант подключения к ЗСПД в соответствии с разделом 2 Регламента	
8.	Наименование ИС	
9.	Реквизиты контракта на сопровождение ИС	
10.	Реквизиты Соглашения (при наличии) <i>(только для варианта межсетевого взаимодействия)</i>	
11.	Номер сторонней сети ViPNet <i>(только для варианта межсетевого взаимодействия)</i>	
12.	Класс защищенности сети ViPNet УИВ <i>(только для варианта межсетевого взаимодействия)</i>	

3. Сведения об ответственных лицах со стороны УИВ

№	ФИО	Должность	Электронная почта	Контактный телефон

Подтверждаем ознакомление и согласие со всеми положениями Регламента подключения к защищенной сети передачи данных, размещенного на официальном сайте ГКУ ТО ЦИТТО в разделе «Главная» - «Направление деятельности» - «Служащим» - «Удаленный доступ».

Подтверждаем выполнение предъявленных требований о защите информации в соответствии с действующим законодательством Российской Федерации. Достоверность предоставленных данных гарантируем. Обо всех изменениях параметров подключения к защищенной сети передачи данных обязуемся уведомлять Оператора ЗСПД — ГКУ ТО «ЦИТТО».

(наименование должности руководителя
юридического лица-заявителя)

(подпись) (инициалы, фамилия)

Анкета для Соглашения

1. Наименование организации	
2. Номер сети ViPNet организации	
3. Юридический адрес организации	
4. Электронная почта организации	
5. Телефон организации	
6. ОГРН	
7. ИНН	
8. КПП	
9. ФИО Генерального директора	
10. Наименование координатора в сети ViPNet организации	
11. Идентификатор координатора в сети ViPNet организации (например: 05C90010)	
12. ФИО Администратора ViPNet сети организации	
13. Наименование сетевого узла ViPNet с ролью администратора сети организации	
14. Идентификатор сетевого узла ViPNet с ролью администратора сети организации (например: 05C90010)	

(наименование должности руководителя
юридического лица-заявителя)

(подпись) (инициалы, фамилия)