Министерство транспорта Российской Федерации
ФГУП «ЗащитаИнфоТранс»

«УТВЕРЖДАЮ»
Генеральный директор
ФГУП «ЗащитаИнфоТранс»
Ю.В. Спасский
«06» июня 2019 г.

ТЕХНИЧЕСКИЕ УСЛОВИЯ

на подключение по защищенному каналу связи органов аттестации и аттестующих организаций к подсистеме аттестации сил обеспечения транспортной безопасности контура «К» ЕГИС ОТБ

(редакция 3.3)

1. Подсистема аттестации сил обеспечения транспортной безопасности (ПАТ) входит в состав контура информационного обеспечения транспортной безопасности (контур «К») Единой государственной информационной системы обеспечения транспортной безопасности (ЕГИС ОТБ).

Оператором ЕГИС ОТБ является Министерство транспорта Российской Федерации. Оператором эксплуатации ЕГИС ОТБ является ФГУП «ЗащитаИнфоТранс» Министерства транспорта Российской Федерации (ФГУП «ЗащитаИнфоТранс»).

Оператор эксплуатации ЕГИС ОТБ в соответствии с возложенными на него функциями в пределах своей компетенции осуществляет:

– обеспечение штатной работы программно-технических средств защищённого информационного взаимодействия удаленных рабочих мест органов аттестации (аттестующих организаций) с ЕГИС ОТБ в пределах своей зоны ответственности, а также оперативное устранение сбоев в их работе;

– обеспечение штатной работы программно-технических средств ПАТ, а также оперативное устранение сбоев в ее работе;

– обеспечение информационной безопасности ЕГИС ОТБ;

– подключение источников и/или потребителей данных и, при необходимости, управление техническими средствами обеспечения защищенного информационного взаимодействия при их подключении.

2. Технические условия используются для подключения органов аттестации (аттестующих организаций) к ПАТ ЕГИС ОТБ посредством информационно-вычислительной сети общего пользования Интернет.

3. Органы аттестации (аттестующие организации) используют собственную инфраструктуру программно-технических средств, включая рабочие места и средства защиты, а также организуют канал доступа к внешнему шлюзу ЕГИС ОТБ, обеспечивают штатную работу средств обеспечения информационного взаимодействия в пределах своей зоны ответственности и оперативное устранение сбоев в их работе.

Органы аттестации, имеющие установленные рабочие места контура «К», уже подключенные к инфраструктуре ЕГИС ОТБ по защищенным каналам связи, могут использовать данные рабочие места.

4. Зоной ответственности оператора ЕГИС ОТБ являются программно-технические средства информационного взаимодействия, входящие в состав ЕГИС ОТБ.

Зоной ответственности органа аттестации (аттестующей организации) являются собственные программно-технические средства информационного взаимодействия, а также каналы передачи данных от органа аттестации (аттестующей организации) до внешнего шлюза ЕГИС ОТБ.

5. Режим приема-передачи данных через шлюзы ПАТ ЕГИС ОТБ - круглосуточный.

6. Для передачи данных используется сеть Интернет. Эффективная пропускная способность канала передачи данных от рабочего места органа аттестации (аттестующей организации) подсистемы ПАТ до внешнего шлюза ЕГИС ОТБ должна обеспечить удовлетворительную работу пользователей и обеспечивать возможность передачи по сети файлов аудио- и видеофиксации результатов проверок больших объёмов (максимальный размер принимаемого файла 4Гб) и быть не менее 15 Мбит/с.

7. Прием и передача данных осуществляется через внешний шлюз ЕГИС ОТБ, к которому органы аттестации (аттестующие организации) обеспечивают подключение. Оператор эксплуатации ЕГИС ОТБ предоставляет

органу аттестации (аттестующий организации) параметры подключения к шлюзу.

8. Органы аттестации, в соответствии с функциональными задачами при проведении аттестации, обеспечивают обработку данных (ввод, просмотр, редактирование) через пользовательский интерфейс (толстый клиент) специального программного обеспечения (СПО) рабочего места органа аттестации ПАТ. Ввод результатов проверок и материалов аудио- и видеофиксации, органами аттестации, возможен так же и через СПО рабочего места аттестующей организации - портал аттестующей организации (тонкий клиент).

9. Аттестующие организации передают результаты проверок и материалы аудио- и видеофиксации в ПАТ ЕГИС ОТБ через СПО рабочего места аттестующей организации - портал аттестующей организации (тонкий клиент) ПАТ, используя стандартный интернет-браузер.

Аттестующие организации, привлекаемые для обработки персональных данных, используют СПО рабочего места органа аттестации (ограниченного функционала) подсистемы ПАТ.

10. Установка СПО рабочего мест органа аттестации (аттестующей организации) подсистемы ПАТ выполняется в соответствии с инструкцией по подключению к ПАТ, предоставляемой оператором эксплуатации ЕГИС ОТБ.

11. СПО рабочего места органа аттестации (аттестующей организации) подсистемы ПАТ и параметры его настройки предоставляются органу аттестации (аттестующей организации) оператором эксплуатации ЕГИС ОТБ.

12. СПО рабочего места органа аттестации является клиентским приложением программной платформы TDMS [1]. Лицензионная политика данной платформы подразумевает использование лицензии для запуска каждого клиентского приложения, указанной платформы.

Для федеральных органов исполнительной власти, их территориальных органов и подведомственных им организаций лицензии для использования (запуска клиентского приложения) предоставляются оператором эксплуатации ЕГИС ОТБ бесплатно.

[1] Разработчик – компания CSoft Development, Москва; номер продукта в Реестре российского программного обеспечения – 962.

Для остальных организаций (юридических лиц) лицензии приобретаются у дистрибьюторов программной платформы TDMS самостоятельно. Как правило, для одного рабочего места приобретается:

- лицензия TDMS Client версии 5.0 или выше;
- лицензия TDMS Viewer версии 5.0 или выше

Количество и тип приобретаемых лицензий, в зависимости от количества используемых рабочих мест, рекомендуется согласовать с оператором эксплуатации ЕГИС ОТБ.

13. При использовании внешних информационных систем, обеспечивающих автоматизацию проведения проверок, прием данных о лицах, допущенных к проверкам, а также выгрузка данных о результатах проверок (в согласованном формате и в соответствии с регламентом информационного взаимодействия между ЕГИС ОТБ и информационной системой проведения проверок) - может производиться автоматизированным способом в электронном виде через шлюз ЕГИС ОТБ, к которому органы аттестации (аттестующие организации) обеспечивают подключение. Оператор эксплуатации ЕГИС ОТБ предоставляет органу аттестации (аттестующий организации) параметры подключения к шлюзу.

14. Безопасность персональных данных при их обработке, хранении и в ходе информационного обмена в пределах зон ответственности его участников обеспечивается с помощью системы защиты персональных данных, включающей в себя организационные меры и средства защиты информации (в том числе криптографические), а также соответствующие информационные технологии.

15. Меры по обеспечению информационной безопасности при обработке персональных данных программно-техническими средствами в пределах установленных зон ответственности должны соответствовать требованиям законодательства РФ в области персональных данных и защиты информации, в том числе приказа ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» и требованиям эксплуатационной документации на применяемые средства защиты информации (СЗИ), в том числе криптографические (СКЗИ).

16. Защита персональных данных при передаче через сеть Интернет должна обеспечиваться путем использования технологии виртуальной частной

сети (VPN-сети), которая представляет собой наложенную защищенную корпоративную сеть передачи данных (ЗКСПД), организатором которой является оператор эксплуатации ЕГИС ОТБ. ЗКСПД ЕГИС ОТБ реализована на базе продуктов семейства ViPNet.

Для подключения к VPN-сети орган аттестации (аттестующая организация) может использовать следующие продукты семейства ViPNet Custom[2]:

- криптошлюз ViPNet HW1000 или HW100A/B/C;
- сертифицированную версию ViPNet Client (к автоматизируемому рабочему месту (АРМ) пользователя предъявляются системные требования в соответствии с приложением 2 к настоящим техническим условиям (ТУ);

Продукты семейства ViPNet приобретаются органом аттестации (аттестующей организацией) самостоятельно.

При приобретении продукта семейства ViPNet необходимо указывать номер сети (2617), в рамках которой он будет функционировать.

17. При организации подключения к ПАТ органу аттестации (аттестующей организации) необходимо выбрать и согласовать с оператором эксплуатации ЕГИС ОТБ схему защищенного взаимодействия в соответствии с приложением 1 к настоящим ТУ, для этого необходимо:

- определить тип подключения;
- выбрать необходимые технические средства для подключения к ЗКСПД;
- в зависимости от выбранного типа подключения (таблица 1, приложение 1) согласовать с оператором эксплуатации ЕГИС ОТБ схему защищенного взаимодействия, включая версии продуктов VipNet и типы используемых криптошлюзов, а также предоставить всю необходимую информацию для выполнения процедуры подключения.

Для несогласованной, с оператором эксплуатации ЕГИС ОТБ, схемы подключения, - работоспособность канала связи не гарантируется.

Примечание: орган аттестации (аттестующая организация), при необходимости организации VipNet подключения между мобильным (мобильными) и стационарным рабочими местами, определяют (для конкретной конфигурации взаимодействующих рабочих мест) и согласовывают схему подключения с оператором эксплуатации ЕГИС ОТБ.

[2] Выбор продукта ViPNet обусловлен способом передачи данных и описан в Приложении №1.

18. В случае выбора перевозчиком схемы подключения, не согласованной с представителем оператора ЕГИС ОТБ, работоспособность канала передачи данных не гарантируется и технические консультации при неработоспособности канала связи не осуществляются вплоть до уточнения и согласования, а также, при необходимости, исправления схемы подключения.

19. Оператор эксплуатации ЕГИС ОТБ предоставляет уполномоченному лицу органа аттестации (аттестующей организации) параметры настройки СКЗИ ViPNet в виде дистрибутива ключевой информации (файл abnXXXX.dst) для подключения к VPN-сети ViPNet, который включает параметры:

- «номер узла сети ViPNet»;
- «IP-адрес шлюзового координатора сети ViPNet»;
- «IP-адреса туннелируемых ресурсов».

Передача дистрибутива ключевой информации осуществляется в офисе Оператора по адресу: г. Москва, Варшавское шоссе, дом 9, строение 1, корпус Мещерин, антресоль мансарды, помещение 664.

20. С целью подключения к ПАТ орган аттестации (аттестующая организация) направляет в адрес оператора ЕГИС ОТБ заявку на подключение установленной формы с указанием сведений об аккредитации и реестрового номера. На основании одобренной заявки заключается Соглашение об организации информационного взаимодействия между оператором эксплуатации ЕГИС ОТБ и органом аттестации (аттестующей организацией).

При изменении у органа аттестации (аттестующей организации) сведений: об аккредитации (аннулировании, продлении, получении новой); списка пользователей; схемы подключения - орган аттестации (аттестующая организация) направляет уведомление в адрес оператора ЕГИС ОТБ с указанием новых или изменяемых сведений.

В соответствии с Соглашением об организации информационного взаимодействия орган аттестации (аттестующая организация) обязан выполнить технические условия на подключение к ПАТ.

21. После заключения соглашения с органом аттестации (аттестующей организацией), при наличии официально предоставленных (или опубликованных компетентным органом) сведений об аккредитации (решения о назначении органом аттестации или решения о привлечении аттестующей организации к обработке персональных данных) оператор эксплуатации предоставляет параметры подключения и подключает орган аттестации (аттестующую организацию) к ПАТ на срок, не превышающий срока действия аккредитации в компетентном органе.

Приложение 1

Требования по организации защиты при подключении органов аттестации и аттестующих организаций по защищенному каналу связи к подсистеме аттестации сил обеспечения транспортной безопасности контура «К» ЕГИС ОТБ

Возможные варианты организации защиты передачи данных в ЕГИС ОТБ представлены в Таблице 1.

Таблица 1

№ схемы	Тип подключения	Описание технических средств
1.1	Аттестующая организация	Защита посредством установки СКЗИ ViPNet Client на специализированном АРМ.
2.1	Орган аттестации и его территориальные подразделения	По количеству рабочих мест: 1-2 – Защита посредством установки СКЗИ ViPNet Client на специализированном АРМ.
2.2		2-10 – Взаимодействие посредством ПАК ViPNet HW100; Более 10 – Взаимодействие посредством ПАК ViPNet HW1000.
3.1	Информационная система	Подключение внешней ИС с помощью криптошлюза в режиме горячего резервирования.
3.2		Подключение внешней ИС с помощью криптошлюза в режиме холодного резервирования.

Схема 1. Требования к реализации защищенного взаимодействия для органа аттестации (аттестующей организации) при работе с тонким клиентом

Схема 1 - использование выделенного АРМ с установленным СКЗИ ViPNet Client.

Выделенный АРМ должен быть оснащен необходимыми средствами защиты информации, сертифицированными по требованиям безопасности информации ФСТЭК России и ФСБ России, такими как аппаратно-программный модуль доверенной загрузки и антивирусное средство.

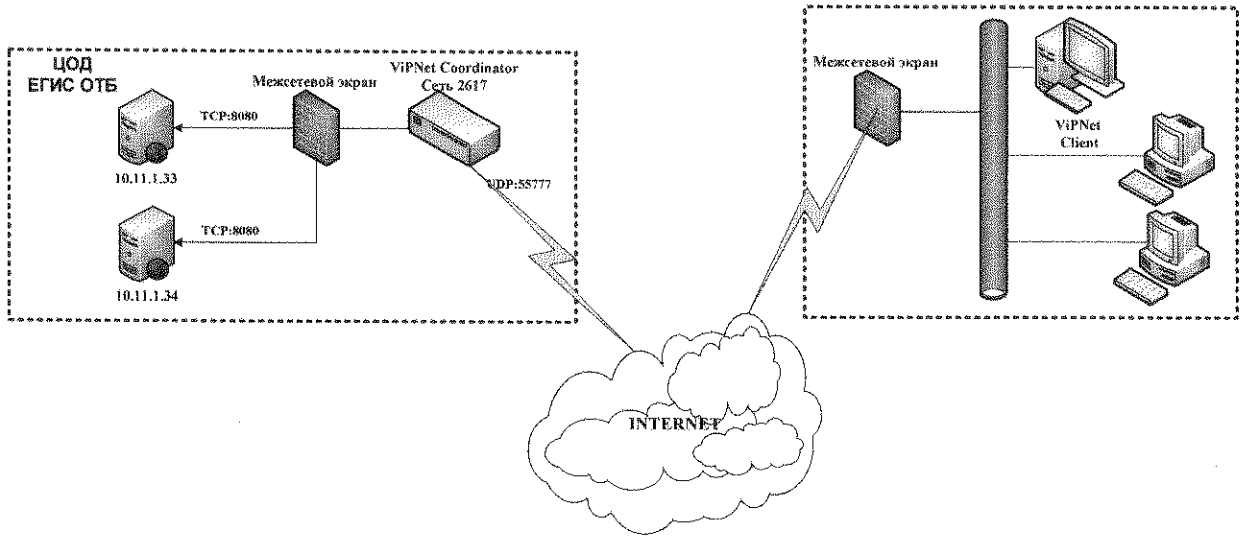

Схема 1.

Схема 2. Требования к реализации защищенного взаимодействия для органа аттестации (аттестующей организации) при работе с толстым и тонким клиентом

Для реализации защищенного взаимодействия в зависимости от количества рабочих мест используются следующие варианты:

Схема 2.1 - при количестве рабочих мест не более 2 – защита посредством установки СКЗИ на специализированном АРМ;

Схема 2.2 - при количестве рабочих мест от 2 до 10 – взаимодействие посредством ПАК ViPNet HW100. При количестве рабочих мест более 10 – взаимодействие посредством ПАК ViPNet HW1000.

Для организации защищенного канала связи с ЗКСПД должно быть использовано СКЗИ, сертифицированное или имеющее положительное заключение ФСБ России, с классом криптографической защиты не ниже КС2.

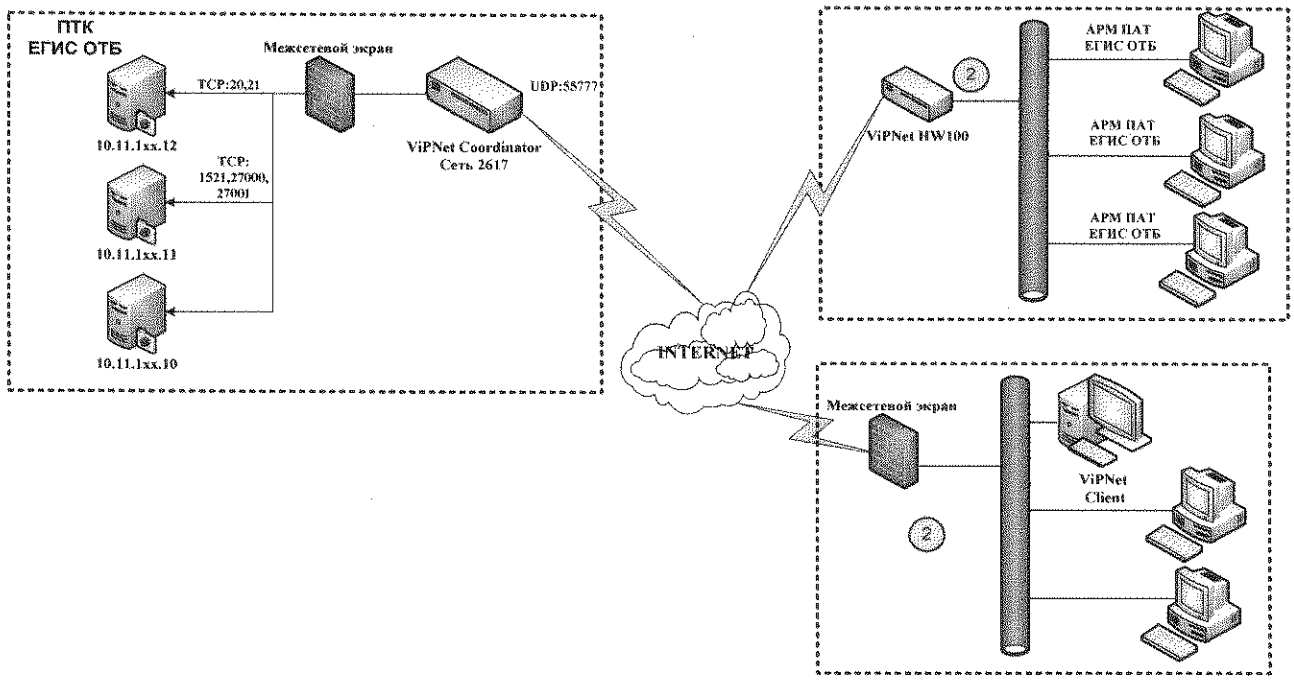

Схема 2.

Схема 3. Требования к реализации защищенного взаимодействия для информационной системы проведения проверок

Для реализации защищенного информационного взаимодействия с ЕГИС ОТБ, внешним информационным системам проведения проверок, необходимо использовать следующие схемы подключения:

Схема 3.1 - подключение внешней ИС посредством криптошлюза в режиме горячего резерва;

Схема 3.2 - подключение внешней ИС посредством криптошлюза в режиме холодного резерва.

Для организации защищенного канала связи с ЗКСПД должно быть использовано СКЗИ, сертифицированное или имеющее положительное заключение ФСБ России, с классом криптографической защиты не ниже КС2.

С целью обеспечения оперативного восстановления канала связи в случае выхода из строя СКЗИ рекомендуется использовать средства организации защищенного взаимодействия, установленные в режиме резервирования, например:

криптошлюз реализованный в виде ПАК ViPNet Coordinator HW1000 в режиме горячего резервирования;

криптошлюз ПАК ViPNet Coordinator HW100A/B/C в режиме холодного резервирования.

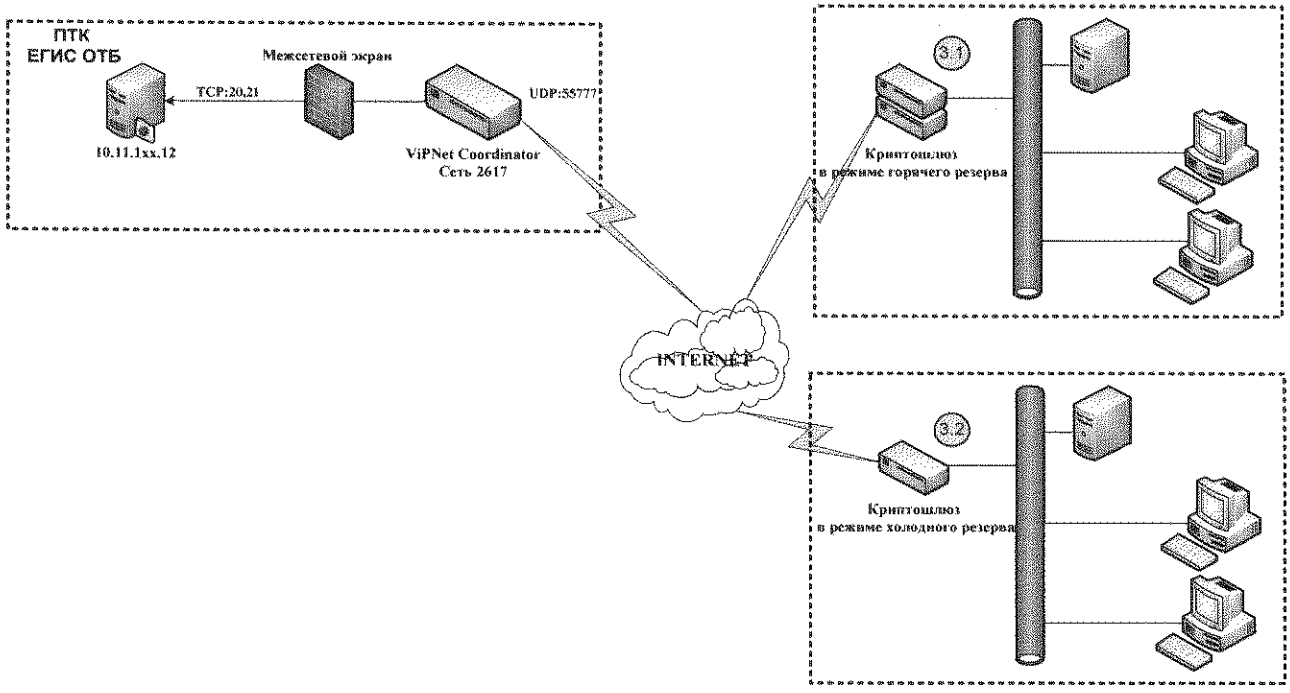
ПТК
ЕГИС ОТБ
Межсетевой экран
TCP:20,21
UDP:55777
10.11.1xx.12
ViPNet Coordinator
Сеть 2617
INTERNET
3.1
Криптошлюз
в режиме горячего резерва
3.2
Криптошлюз
в режиме холодного резерва

Схема 3.

Приложение 2

Требования к компьютеру для установки программы ViPNet Client

1. Процессор — Intel Core 2 Duo или другой схожий по производительности x86-совместимый процессор с количеством ядер 2 и более.
2. Объем оперативной памяти — не менее 1 Гбайт.
3. Свободное место на жестком диске — не менее 150 Мбайт (рекомендуется 250 Мбайт).
4. Сетевой интерфейс или модем.
5. Операционная система — Vista (32/64-разрядная), Server 2008 (32/64-разрядная), Server 2008 R2 (64-разрядная), Small Business Server 2008 (64 разрядная), Small Business Server 2008 SP2 (64-разрядная), Windows 7 (32/64-разрядная), Windows 8 (32/64-разрядная), Windows 8.1 (32/64-разрядная), Small Business Server 2011 (64 разрядная), Server 2012 (64-разрядная), Server 2012 R2 (64-разрядная), Windows 10 (32/64 разрядная).
6. Для операционной системы должен быть установлен самый последний пакет обновлений.
7. При использовании более ранних версий Windows, чем Windows 8, на компьютере должен быть установлен накопительный пакет обновления часовых поясов KB2570791.
8. При использовании Internet Explorer — версия 10.0 или выше.