Регламент

подключения к защищенной сети государственной информационной системы «Типовое облачное решение по автоматизации контрольной (надзорной) деятельности»

версия 2.0

2021

Содержание

Перечень сокращений

Сокращение	**Наименование**
АРМ	Автоматизированное рабочее место
ВИС КНО	Ведомственная информационная система автоматизации контрольно-надзорной деятельности контрольно-надзорного органа
ГИС ТОР КНД	Государственная информационная система «Типовое облачное решение по автоматизации контрольной (надзорной) деятельности»
ЕФТТ	Единые функционально-технические требования по автоматизации приоритетных видов регионального государственного контроля (надзора) в целях внедрения риск-ориентированного подхода, утвержденные Приказом Министерства цифрового развития, связи и массовый коммуникаций Российской Федерации от 26.01.2021 № 29
КНО	Контрольно-надзорный орган или организация
ЛВС	Локально-вычислительная сеть
ОИ	Объект информатизации
ПО	Программное обеспечение
ПК	Персональный компьютер
ПЭВМ	Персональная электронно-вычислительная машина
СВТ	Средство вычислительной техники
СКЗИ	Средство криптографической защиты информации
СТП	Служба технической поддержки
СЭП	Средство электронной подписи
УКЭП	Усиленная квалифицированная электронная подпись
ФСБ России	Федеральная служба безопасности Российской Федерации
ФСТЭК России	Федеральная служба по техническому и экспортному контролю
ЦОД	Центр обработки данных
ЭП	Электронная подпись

1. Общие положения

1.1. Предмет регулирования

Настоящий Регламент устанавливает требования и определят порядок подключения внешних объектов информатизации (далее – ОИ КНО) к защищенной сети государственной информационной системы «Типовое облачное решение по автоматизации контрольной (надзорной) деятельности» (далее – ГИС ТОР КНД) в целях организации защищенного информационного взаимодействия внешних информационных систем (далее – ВИС КНО) с ГИС ТОР КНД и обеспечения защищенной работы пользователей с информационными ресурсами ГИС ТОР КНД.

Настоящий регламент вступает в силу после его утверждения и опубликования на сайте информационного портала ГИС ТОР КНД по адресу https://knd.gov.ru.

Требования настоящего Регламента не распространяются на ОИ КНО, подключенные к ГИС ТОР КНД до даты его опубликования на портале ГИС ТОР КНД.

1.2. Сведения о государственной информационной системе

ГИС ТОР КНД является государственной информационной системой, соответствующей требованиям законодательства Российской Федерации и подзаконных нормативных правовых актов в области защиты информации:

1) «Требования о защите информации, не составляющей государственной тайны, содержащейся в государственных информационных системах», утвержденные приказом ФСТЭК России от 11 февраля 2013 г. № 17 – по второму классу защищенности;
2) «Требования к защите персональных данных при их обработке в информационных системах персональных данных», утвержденные Постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 – по третьему уровню защищенности персональных данных.

Оператором ГИС ТОР КНД является Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации (далее – Оператор).

Эксплуатирующей организацией ГИСТОР КНД является Федеральное государственное автономное учреждение «Научно-исследовательский институт «Восход» (далее – эксплуатирующая организация).

1.3. Сведения о технической поддержке

Служба технической поддержки (далее – СТП) эксплуатирующей организации осуществляет прием запросов по электронной почте (круглосуточно: 24 часа в сутки, 7 дней в неделю) и по телефону (с 09:00 до 18:00 часов по московскому времени ежедневно по рабочим дням, установленным Правительством Российской Федерации).

Запросы обрабатываются с 09:00 до 18:00 часов по московскому времени ежедневно по рабочим дням, установленным Правительством Российской Федерации.

Контактные данные СТП эксплуатирующей организации:

1) электронная почта: kndsupport@voskhod.ru;
2) телефон: +7 (495) 788-85-71.

1.4. Перечень нормативно-правовых актов

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

1) Постановление Правительства Российской Федерации от 21.04.2018 № 482 «О государственной информационной системе «Типовое облачное решение по автоматизации контрольной (надзорной) деятельности»;
2) Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
3) Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
4) Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
5) Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи»;
6) Приказ ФСБ России от 27.12.2011 № 795 «Об утверждении Требований к форме квалифицированного сертификата ключа проверки электронной подписи»;
7) Приказ ФСБ России от 27.12.2011 № 796 «Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра»;
8) Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состава 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»;

9) Приказ Федерального агентства правительственной связи и информации от 13.06.2001 № 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» (утверждена);

10) Приказ Министерства цифрового развития, связи и массовый коммуникаций Российской Федерации от 26.01.2021 № 29 «Об утверждении единых функционально-технических требований по автоматизации приоритетных видов регионального государственного контроля (надзора) в целях внедрения риск-ориентированного подхода» (далее – ЕФТТ).

1.5. Изменения (дополнения) в Регламент

Внесение изменений (дополнений) в Регламент, в том числе в приложения к нему, осуществляется Оператором в одностороннем порядке.

Уведомление о внесении изменений (дополнений) в Регламент осуществляется путем публикации на сайте информационного портала ГИС ТОР КНД (https://knd.gov.ru в разделе «Подключение к ГИС ТОР КНД»).

Изменения (дополнения), вносимые в Регламент, кроме изменений (дополнений), вызванных изменениями законодательства Российской Федерации, вступают в силу и становятся обязательными к выполнению по истечению 10 календарных дней с даты их публикации на сайте информационного портала ГИС ТОР КНД.

Изменения (дополнения), вносимые в Регламент в связи с изменением законодательства Российской Федерации, вступают в силу одновременно с вступлением в силу соответствующих нормативных актов.

2. Сведения о способах (вариантах) подключения к ГИС ТОР КНД

ГИС ТОР КНД обеспечивает поддержку защищенного криптографическими методами информационного взаимодействия со следующими типами внешних объектов информатизации (далее – ОИ):

1) ведомственные информационные системы автоматизации контрольно-надзорной деятельности контрольно-надзорного органа (далее – ВИС КНО), представленные в виде совокупности серверного, сетевого и коммутационного оборудования, объединенные в локальную вычислительную сеть КНО или сегменты локально-вычислительной сети КНО;

2) средства вычислительной техники пользователей ГИС ТОР КНД (далее – СВТ), эксплуатируемые отдельно или в составе ОИ КНО, объединенные в локальную вычислительную сеть КНО или сегменты локально-вычислительной сети КНО, предназначенные для непосредственной работы пользователей с ресурсами ГИС ТОР КНД: автоматизированные рабочие места (далее – АРМ) в различных исполнениях (ПЭВМ, моноблок, ноутбук), мобильные устройства (смартфон, планшетный ПК).

Для обеспечения защищенного информационного взаимодействия с ГИС ТОР КНД на стороне ОИ КНО (ВИС КНО, СВТ) требуется реализовать комплекс мероприятий с учетом требований, приведенных в разделе 3 ЕФТТ.

Определены четыре способа (варианта) организации подключения ОИ КНО (ВИС КНО, СВТ) к защищенной сети ГИС ТОР КНД.

Сводная информация с описанием критериев выбора вариантов подключения ОИ КНО к ГИС ТОР КНД приведена в Таблице 1, подробное описание каждого варианта подключения приведено в разделах 3.1–3.4 настоящего Регламента.

Таблица 1 – Сводная информация о вариантах подключения ОИ КНО (ВИС КНО, СВТ) к защищенной сети ГИС ТОР КНД

Основные критерии выбора варианта подключения к ГИС ТОР КНД	Варианты подключения к ГИС ТОР КНД			
	№ 1	№ 2	№ 3	№ 4
Возможность обеспечения защищенного информационного взаимодействия ВИС КНО с ГИС ТОР КНД	+	+	+	-
Возможность защищенной работы пользователей с ресурсами ГИС ТОР КНД со стационарных АРМ	+	+	+	+
Возможность защищенной работы с ГИС ТОР КНД для пользователей со стационарных АРМ, расположенных за пределами контролируемой зоны ОИ КНО[3]	–	+	+	+
Возможность защищенной работы с ГИС ТОР КНД для пользователей с мобильных устройств (смартфоны, планшетные ПК), расположенных за пределами контролируемой зоны ОИ КНО[1]	–	+	+	+
Необходимость подключения ЛВС КНО (сегмента ЛВС КНО) к защищенной сети ГИС ТОР КНД (сеть ViPNet № 12633)	+	+	+[2]	–
Необходимость применения СКЗИ на стороне стационарных АРМ пользователей	–	+	+[3]	+
Необходимость приобретения лицензий СКЗИ для организации защищенного подключения СВТ (АРМ) и мобильных устройств к ГИС ТОР КНД	+	+	+[3]	–

Примечание:

[1] при соблюдении дополнительных организационно-технических требований, приведенных в ЕФТТ;

[2] в рамках межсетевого взаимодействия с сетью ГИС ТОР КНД (ViPNet № 12633);

[3] в зависимости от архитектуры и структуры подключаемой сети ViPNet в рамках межсетевого взаимодействия.

Подключение ОИ КНО (ВИС КНО, СВТ) к ГИС ТОР КНД может осуществляться по каналам сети связи общего пользования (Интернет) при условии обязательного применения на стороне ОИ КНО средств криптографической защиты информации (далее – СКЗИ), реализующих российские алгоритмы шифрования:

1) СКЗИ семейства ViPNet, обеспечивающие защищенное VPN-соединение сетью ViPNet № 12633 ГИС ТОР КНД;
2) СКЗИ, обеспечивающие защищенное TLS-соединение с веб-ресурсами ГИС ТОР КНД.

Для обеспечения защищенного информационного взаимодействия ВИС КНО с ГИС ТОР КНД на стороне ОИ КНО (ВИС КНО) должны применяться СКЗИ семейства ViPNet, подключенные к защищенной сети ГИС ТОР КНД (сеть ViPNet № 12633) согласно варианту № 1 или 2, или СКЗИ семейства ViPNet из состава внешней сети ViPNet, обеспечивающие межсетевое взаимодействие с защищенной сетью ГИС ТОР КНД (ViPNet № 12633) согласно варианту № 3. Информационное взаимодействие ВИС КНО с ГИС ТОР КНД осуществляется только
на основании договора (соглашения) об информационном взаимодействии с оператором ГИС ТОР КНД.

Для организации защищенной работы пользователей с веб-ресурсами ГИС ТОР КНД на стороне АРМ и мобильных устройств (смартфоны, планшетные ПК) могут применяться СКЗИ семейства ViPNet, подключенные к защищенной сети ГИС ТОР КНД (сеть ViPNet № 12633) согласно варианту № 1-3 или СКЗИ, обеспечивающие защищенное TLS-соединение с веб-ресурсами ГИС ТОР КНД согласно варианту подключения № 4.

Выбор варианта подключения к ГИС ТОР КНД и СКЗИ, применяемых на стороне ОИ КНО (ВИС КНО, СВТ) осуществляется в зависимости от целей подключения к ГИС ТОР КНД, территориального расположения ОИ КНО, количества пользователей на стороне ОИ КНО, типов используемых устройств и ОС, пропускной способности канала связи.

Выбор класса СКЗИ (КС1, КС2, КС3), применяемых на стороне ОИ КНО (ВИС КНО, СВТ) осуществляется КНО на основании модели нарушителя безопасности информации. При отсутствии разработанных моделей нарушителей класс СКЗИ может быть определен согласно Методике, приведенной в Приложении 1 к ЕФТТ.

ГИС ТОР КНД не поддерживает защищенное взаимодействие с ОИ КНО (ВИС КНО, СВТ), защищенных с применением СКЗИ, сертифицированных ФСБ России по классу выше КС3.

3. Описание вариантов подключения к ГИС ТОР КНД

3.1. Вариант подключения № 1 к защищенной сети ViPNet

Вариант подключения № 1 подходит как для организации защищенного информационного взаимодействия ВИС КНО с ресурсами ГИС ТОР КНД, так и для обеспечения защищенной работы пользователей с ресурсами ГИС ТОР КНД со стационарных АРМ в рамках локально-вычислительной сети КНО (сегмента ЛВС КНО), расположенной в пределах контролируемой зоны ОИ КНО.

Схема подключения для варианта № 1 приведена на рисунке 1.

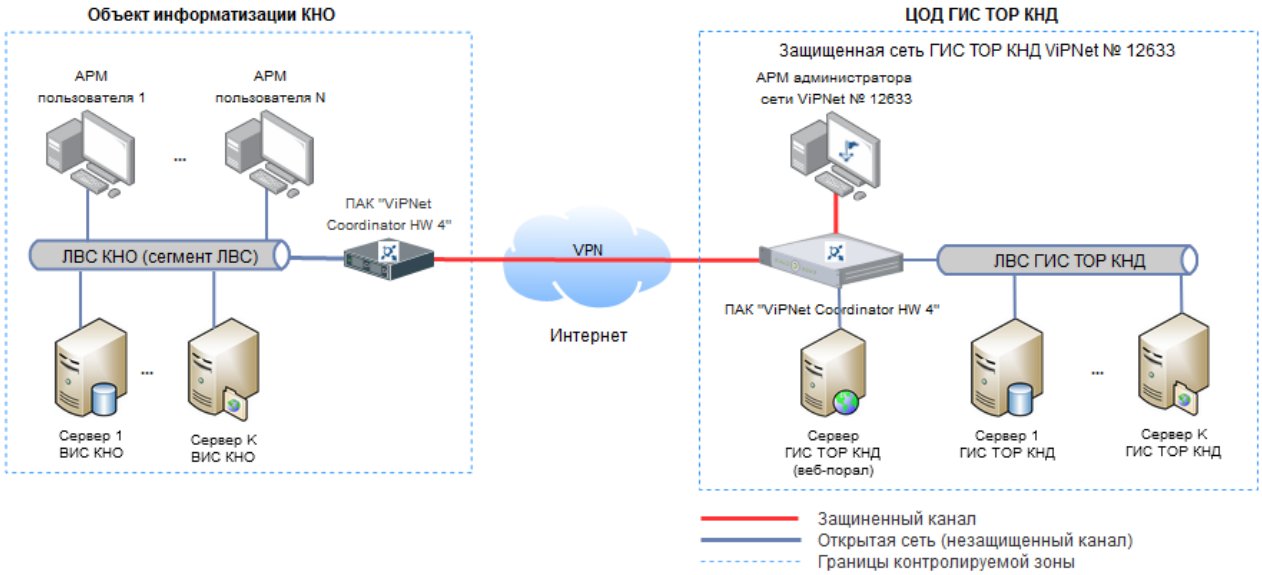

Рисунок 1 – Схема подключения для варианта № 1

Данный вариант предполагает подключение ЛВС КНО (сегмента ЛВС КНО) к защищенной сети ГИС ТОР КНД (сеть ViPNet № 12633) через программно-аппаратный комплекс «ViPNet Coordinator HW 4» (далее – ПАК «ViPNet Coordinator HW 4»), устанавливаемый на стороне ОИ КНО.

ПАК «ViPNet Coordinator HW 4» должен обладать действующим сертификатом соответствия требованиям по безопасности ФСБ России. Выбор модели ПАК «ViPNet Coordinator HW 4» (например, исполнения HW50 A, HW100 C, HW1000) для подключения ЛВС КНО (сегмента ЛВС КНО) к защищенной сети ГИС ТОР КНД (сеть ViPNet № 12633) осуществляется КНО с учетом пропускной способности канала связи и требуемой производительности.

АРМ, с которых пользователи осуществляют работу с ресурсами ГИС ТОР КНД, должны соответствовать требованиям п. 3.5.1 ЕФТТ.

Администрирование ПАК «ViPNet Coordinator HW 4» на стороне КНО осуществляется специалистами КНО, назначенными приказом руководителя КНО.

Данный вариант подключения не подходит при наличии на стороне КНО мобильных устройств пользователей (смартфоны, планшетные ПК) или АРМ пользователей, расположенных за пределами контролируемой зоны ОИ КНО, для которых требуется обеспечить защищенную работу с ресурсами ГИС ТОР КНД. В целях обеспечения защищенной работы пользователей с ресурсами ГИС ТОР КНД со стационарных АРМ или мобильных устройств, расположенных за пределами контролируемой зоны ОИ КНО, рекомендуется применять другие варианты подключения (варианты подключения № 2, 3 или 4).

3.2. Вариант подключения № 2 к защищенной сети ViPNet

Вариант подключения № 2 подходит как для организации защищенного информационного взаимодействия ВИС КНО с ресурсами ГИС ТОР КНД, так и для обеспечения защищенной работы пользователей с ресурсами ГИС ТОР КНД со стационарных АРМ и мобильных устройств (смартфоны, планшеты), эксплуатируемых в составе территориально-распределенного ОИ КНО.

Схема подключения по варианту № 2 приведена на рисунке 2.

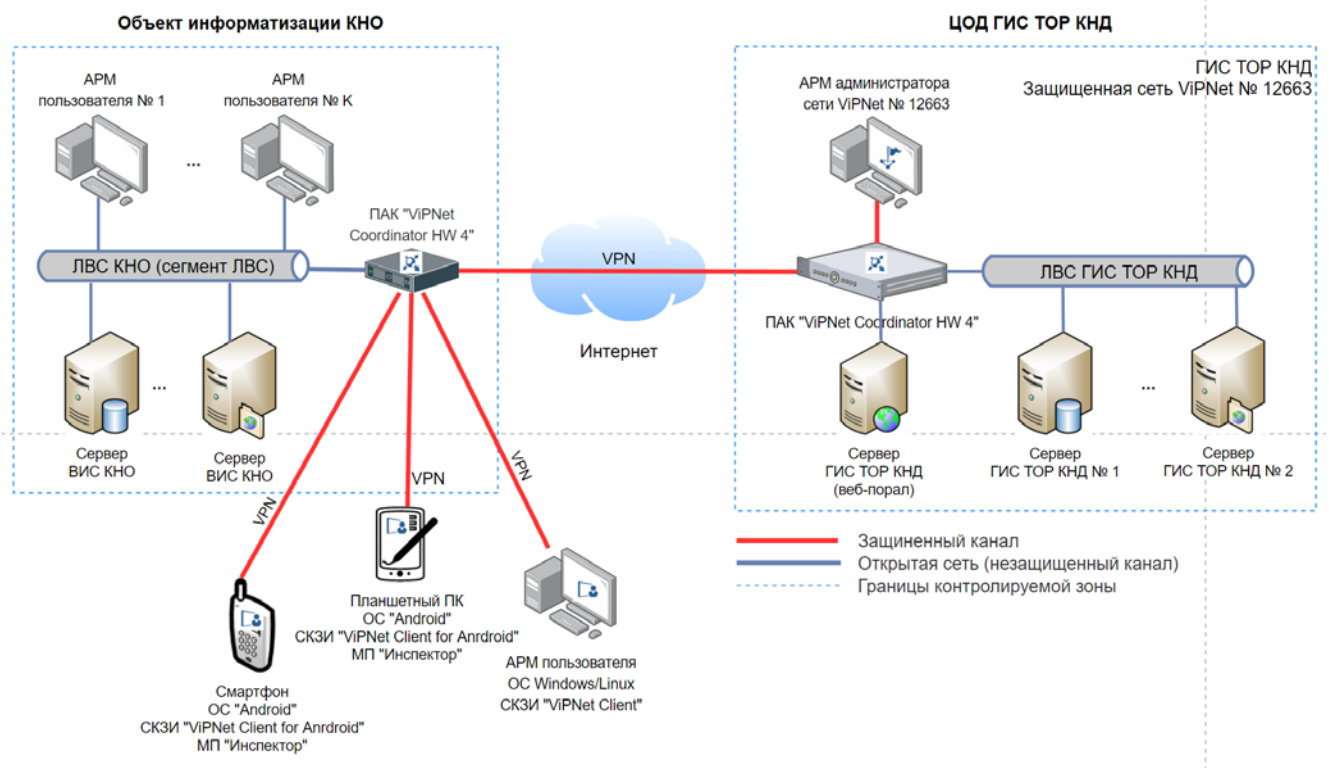

Рисунок 2 – Схема подключения для варианта № 2

В рамках данного варианта обеспечивается подключение ЛВС КНО (сегмента ЛВС КНО) в защищенную сеть ГИС ТОР КНД (сеть ViPNet № 12633) с применением центрального узла доступа КНО, реализованного на базе ПАК «ViPNet Coordinator HW 4», сертифицированного
по требованиям безопасности ФСБ России.

Выбор модели ПАК «ViPNet Coordinator HW 4» (исполнения HW50 A, HW100 C, HW1000 и т.п.) для подключения ЛВС КНО (сегмента ЛВС КНО) к защищенной сети ГИС ТОР КНД
(сеть ViPNet № 12633) осуществляется КНО с учетом пропускной способности канала связи, требуемой производительности, а также количества АРМ и мобильных устройств, расположенных за пределами контролируемой зоны ОИ КНО, которые планируется подключить с применением программного обеспечения СКЗИ «ViPNet Client».

Вариант подключения № 2 отличается от варианта подключения № 1 необходимостью применения на стороне АРМ и мобильных устройств пользователей, расположенных за пределами контролируемой зоны ОИ КНО, программного обеспечения СКЗИ «ViPNet Client» в целях защиты канала связи до центрального узла доступа КНО (ПАК «ViPNet Coordinator HW 4»).

Подключение к защищенной сети ГИС ТОР КНД (сеть ViPNet № 12633) для АРМ и мобильных устройств, расположенных за пределами контролируемой зоны ОИ КНО обеспечивается через центральный узел доступа КНО (ПАК «ViPNet Coordinator HW 4») с применением программного обеспечения СКЗИ «ViPNet Client», сертифицированного по требованиям безопасности ФСБ России:

1) СКЗИ «ViPNet Client 2 for Android» – для мобильных устройств (смартфоны, планшетные ПК), функционирующих под управлением ОС Android;
2) СКЗИ «ViPNet Client 4» – для АРМ, функционирующих под управлением ОС семейства Windows;
3) СКЗИ «ViPNet Client 4 for Linux» – для АРМ, функционирующих под управлением ОС семейства Linux.

АРМ пользователей, осуществляющие работу с ресурсами ГИС ТОР КНД должны соответствовать требованиям п. 3.5.1 ЕФТТ. Применяемые на стороне АРМ операционные системы семейства Windows и (или) Linux должны быть совместимы с версиями СКЗИ «ViPNet Client».

Мобильные устройства (смартфоны, планшетные ПК) под управлением ОС Android, должны соответствовать требованиям п. 3.5.2 ЕФТТ. Применяемые на стороне мобильных устройств версии ОС Android должны быть совместимы с СКЗИ «ViPNet Client» и МП «Инспектор».

Администрирование ПАК «ViPNet Coordinator HW 4», а также СКЗИ «VIPNet Client» на стороне АРМ и мобильных устройств осуществляется специалистами КНО, назначенными приказом руководителя КНО.

3.3. Вариант подключения № 3 к защищенной сети ViPNet

Вариант подключения № 3 применяется для организации информационного взаимодействия ВИС КНО с ресурсами ГИС ТОР КНД и обеспечения защищенной работы пользователей с ресурсами ГИС ТОР КНД при наличии на стороне ОИ КНО собственной защищенной сети ViPNet, для которой может быть настроено межсетевое взаимодействие с защищенной сетью ГИС ТОР КНД ViPNet № 12633.

Схема подключения для варианта № 3 приведена на рисунке 3.

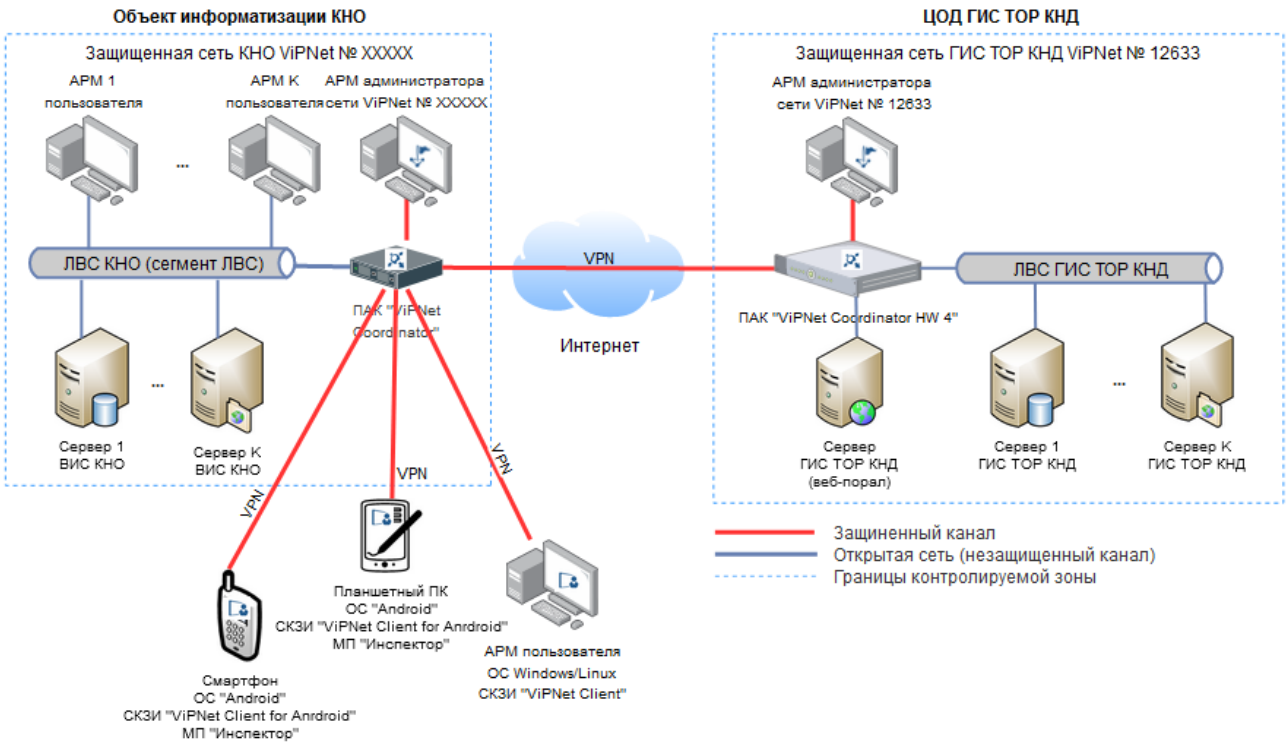

Рисунок 3 – Схема подключения для варианта № 3

Межсетевое взаимодействие защищенной сети ГИС ТОР КНД ViPNet № 12633 с другими внешними сетями ViPNet может быть обеспечено только при условии построения внешней сети ViPNet с применением СКЗИ семейства ViPNet, сертифицированных ФСБ России

по классу не выше КС3 (КС1, КС2 или КС3).

3.4. Вариант подключения № 4 без подключения к защищенной сети ViPNet

Данный вариант подключения предназначен только для организации защищенной работы с веб-ресурсами ГИС ТОР КНД с СВТ пользователей (АРМ, мобильных устройств) без необходимости подключения к защищенной сети ГИС ТОР КНД ViPNet № 12633:

1) АРМ в различных исполнениях (ПЭВМ, моноблок, ноутбук), функционирующих под управлением ОС семейства Windows или Linux с применением СКЗИ через веб-браузер;
2) мобильных устройств (смартфоны, планшетные ПК) под управлением ОС «Аврора» или ОС «Android» с применением СКЗИ через МП «Инспектор».

Для обеспечения защищенной работы пользователей с веб-ресурсами ГИС ТОР КНД на стороне СВТ пользователей (АРМ, мобильных устройствах) применяются СКЗИ, обеспечивающие возможность установления криптографически защищенного TLS-соединения с веб-сервером ГИС ТОР КНД (порталом), в режиме односторонней аутентификацией веб-сервера.

При установлении TLS-соединения с веб-сервером на стороне СВТ пользователей осуществляется аутентификация веб-сервера ГИС ТОР КНД по сертификату формата x509 v3, по результатам успешной аутентификации веб-сервера осуществляется шифрование трафика в рамках установленного TLS-соединения между СВТ и веб-сервером ГИС ТОР КНД (веб-порталом).

Данный вариант подключения не подходит для организации защищенного информационного взаимодействия ВИС КНО с ГИС ТОР КНД.

Схема подключения СВТ пользователей (АРМ и мобильных устройств) для варианта № 4 приведена на рисунке 4.

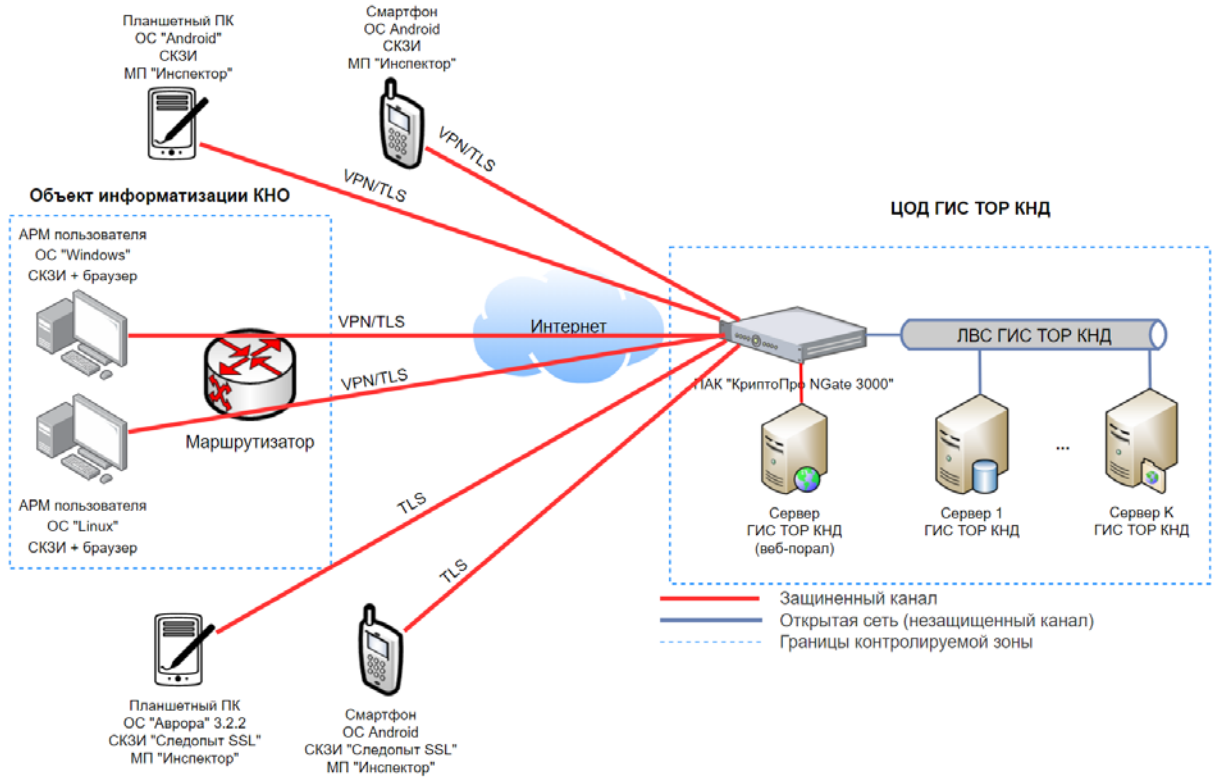

Рисунок 4 – Схема подключения для варианта № 4

Работа пользователей на АРМ с веб-ресурсами ГИС ТОР КНД должна осуществляться через веб-браузер с обязательным применением СКЗИ, совместимых с СКЗИ «Криптографический сетевой программный комплекс «КриптоПро NGate» версия 1.0 (исполнение 4)» на базе аппаратной платформы NGate 3000, применяемом на стороне серверной части ГИС ТОР КНД.

Работа пользователей с мобильных устройств (смартфоны, планшетные ПК) с веб-ресурсами ГИС ТОР КНД должна осуществляться только через мобильное приложение «Инспектор» (далее – МП «Инспектор») с обязательным применением СКЗИ, применяемом на стороне серверной части ГИС ТОР КНД. Подключение мобильных устройств для защищенной работы с ресурсами ГИС ТОР КНД через мобильные браузеры из состава мобильных ОС не допускается.

АРМ пользователей, с которых пользователи осуществляют работу с ресурсами ГИС ТОР КНД, должны соответствовать требованиям п. 3.5.1 ЕФТТ. Применяемые на стороне АРМ операционные системы семейства Windows и (или) Linux должны быть совместимы СКЗИ.

Мобильные устройства (смартфоны, планшетные ПК) под управлением ОС Android, должны соответствовать требованиям п. 3.5.2 ЕФТТ. Применяемые на стороне мобильных устройств версии ОС Android должны быть совместимы с СКЗИ и МП «Инспектор».

Подробное описание перечня СКЗИ для применения на различных типах пользовательских устройств (АРМ, мобильные устройства) и операционных систем (Windows, Linux, Android, Аврора) приведено в п.3.4.1–3.4.4 настоящего Регламента.

3.4.2. Требования к организации подключения АРМ пользователей под управлением ОС семейства Windows без подключения к защищенной сети ViPNet ГИС ТОР КНД

Перечень поддерживаемых СКЗИ, применяемых на стороне АРМ под управлением ОС семейства Windows совместно с плагином ППО «КриптоПро ЭЦП Browser Plug-in» версия 2.0.14071 (далее – плагин для веб-браузера) в целях обеспечения защищенного доступа к веб-ресурсам ГИС ТОР КНД через веб-браузер:

1) СКЗИ «КриптоПро CSP» версия 4.0 (исполнение 1-Base, исполнение 2-Base, исполнение 3-Base);
2) СКЗИ «КриптоПро CSP» версия 5.0 (исполнение 1-Base, исполнение 2-Base, исполнение 3-Base).

Перечень поддерживаемых плагином ППО «КриптоПро ЭЦП Browser Plug-in» версия 2.0.13771 веб-браузеров:

1) Яндекс.Браузер версия не ниже 17.9.1;
2) Internet Explorer версия не ниже 8.0.6001;
3) Chromium-Gost версия не ниже 91.0.

Перечень поддерживаемых СКЗИ, применяемых на стороне АРМ под управлением ОС семейства Windows совместно с плагином ППО «TRUST Plugin» в целях обеспечения защищенного доступа к веб-ресурсам ГИС ТОР КНД через веб-браузер:

1) СКЗИ «КриптоПро CSP» версия 4.0 (исполнение 1-Base, исполнение 2-Base, исполнение 3-Base);
2) СКЗИ «КриптоПро CSP» версия 5.0 (исполнение 1-Base, исполнение 2-Base, исполнение 3-Base);
3) СКЗИ «ViPNet CSP 4.2» (вариант исполнения 5).

Перечень поддерживаемых плагином ППО «TRUST Plugin» веб-браузеров:

1) Яндекс.Браузер версия не ниже 17.9.1;
2) Chromium-Gost версия не ниже 91.0.

В качестве СКЗИ, применяемого на АРМ под управлением ОС семейства Windows для обеспечения защищенного доступа к веб-ресурсам ГИС ТОР КНД через веб-браузер, не требующего установки плагина для веб-браузера возможно применять СКЗИ «КриптоПро NGate Клиент» версия 1.0 (исполнение 7), функционирующего совместно со следующими веб-браузерами:

1) Яндекс.Браузер версия не ниже 17.9.1;
2) Internet Explorer версия не ниже 8.0.6001;
3) Chromium-Gost версия не ниже 91.0;
4) Спутник «Браузер» версия не ниже 5.3.5380.0.

Версии ОС Windows и веб-браузеров, применяемых на стороне АРМ пользователей должны быть совместимы с планируемыми к применению СКЗИ и плагином для веб-браузера (для СКЗИ, функционирующего совместно с плагином для веб-браузера).

3.4.3. Требования к организации подключения АРМ пользователей под управлением ОС семейства Linux без подключения к защищенной сети ViPNet ГИС ТОР КНД

Перечень поддерживаемых СКЗИ, функционирующих на стороне АРМ под управлением ОС семейства Linux совместно с плагином ППО «КриптоПро ЭЦП Browser Plug-in» версия 2.0.13771 для веб-браузера для обеспечения защищенного доступа к веб-ресурсам ГИС ТОР КНД:

1) СКЗИ «КриптоПро CSP» версия 4.0 (исполнение 1-Base, исполнение 2-Base);
2) СКЗИ «КриптоПро CSP» версия 5.0 (исполнение 1-Base, исполнение 2-Base).

Перечень поддерживаемых плагином ППО «КриптоПро ЭЦП Browser Plug-in» веб-браузеров:

1) Спутник «Браузер» версия не ниже 5.3.5357.0.

В качестве СКЗИ, применяемого на АРМ под управлением ОС семейства Linux для обеспечения защищенного доступа к веб-ресурсам ГИС ТОР КНД через веб-браузер, не требующего установки плагинов для веб-браузера возможно применять СКЗИ «КриптоПро NGate Клиент» версия 1.0 (исполнение 6), функционирующего совместно со следующими веб-браузерами:

1) Спутник «Браузер» версия не ниже 5.3.5357.0;

2) Chromium-Gost версия не ниже 91.0.

Версии ОС Linux и веб-браузеров, применяемых на стороне АРМ пользователей должны быть совместимы с планируемыми к применению СКЗИ и плагином для веб-браузера (для СКЗИ, функционирующего совместно с плагином для веб-браузера).

3.4.4. Требования к организации защищенного подключения мобильных устройств под управлением ОС Android без подключения к защищенной сети ViPNet ГИС ТОР КНД

Для организации защищенного подключения мобильных устройств под управлением ОС Аврора к ресурсам ГИС ТОР КНД на стороне мобильных устройств должна применяться ОС Аврора версии не ниже 3.2.2 (сертификат ФСТЭК России № 4220, срок действия до 10.02.2025) совместно СКЗИ «Следопыт SSL» из состава ОС (сертификат ФСБ СФ/114-3741 , срок действия до 26.08.2022) и средствами антивирусной защиты, совместимым с ОС.

В качестве средства антивирусной защиты, совместимого с ОС Аврора версии не ниже 3.2.2 и СКЗИ «Следопыт SSL» может применяться САВЗ «Kaspersky Endpoint Security for AURORA» (сертификат ФСТЭК № 4235 от 21.05.2020, срок действия до 21.05.2025).

3.4.5. Требования к организации защищенного подключения мобильных устройств под управлением ОС Android без подключения к защищенной сети ViPNet ГИС ТОР КНД

Для организации защищенного подключения к ресурсам ГИС ТОР КНД с применением мобильных устройств под управлением ОС Android на стороне мобильных устройств должны применяться ОС Android версии 8 и выше (или иные, в соответствии с документом «КриптоПро NGate. Формуляр») совместно СКЗИ «КриптоПро NGate Клиент» версия 1.0 (исполнение 5) и средством антивирусной защиты, совместимых с версией ОС Android.

В качестве средства антивирусной защиты, совместимое с ОС Android и СКЗИ «КриптоПро NGate Клиент» версия 1.0 (исполнение 5) может применяться САВЗ «Kaspersky Endpoint Security 10 для Android» (сертификат ФСТЭК № 3754, срок действия до 23.06.2025).

4. Требования к работе со средствами электронной подписи на АРМ пользователей

На стороне серверной части ГИС ТОР КНД реализованы средства электронной подписи (далее – СЭП), обеспечивающие функции по автоматизированной проверке усиленной квалифицированной электронной подписи (далее – УКЭП) для файлов (данных), подписанных и загружаемых пользователями ГИС ТОР КНД со стационарных АРМ через веб-браузер.

Для возможности проверки УКЭП на стороне серверной части ГИС ТОР КНД, поступающие от пользователей файлы (данные) должны быть предварительно подписаны УКЭП на стороне АРМ пользователей.

Процедура создания УКЭП для файлов (данных) должна осуществляться непосредственно на стационарных АРМ пользователей через веб-браузер с применением специализированного плагина для веб-браузера и средств электронной подписи (далее – СЭП), удовлетворяющих требованиям п. 3.6 ЕФТТ.

В качестве СЭП на АРМ могут применяться СКЗИ, совместимые с версиями ОС, веб-браузеров и плагинами для веб-браузеров, приведенных в п. 3.4.1–3.4.2 настоящего Регламента.

5. Порядок подключения к защищенной сети ГИС ТОР КНД

5.1. Порядок подключения к защищенной сети ViPNet (для варианта № 1 и № 2)

Подключение участников информационного взаимодействия к защищенной сети ГИС ТОР КНД (ViPNet № 12633) для варианта № 1 (п. 3.1 настоящего Регламента) и варианта № 2 (п. 3.2 настоящего Регламента) осуществляется в следующем порядке:

1) Заявитель (КНО) осуществляет закупку программного обеспечения или программно-аппаратного комплекса ViPNet;

2) участник информационного взаимодействия (далее – заявитель в лице Координатора региона) направляет в адрес:

   а) оператора Заявку на подключение к защищенной сети ГИС ТОР КНД в официальном порядке за подписью координатора региона;

   б) эксплуатирующей организации Заявка направляется с зарегистрированного электронного адреса Координатора региона на электронный адрес СТП с приложением скан-копии официально зарегистрированной Заявки на подключение к защищенной сети ГИС ТОР КНД оператору и исходных текстовых файлов Заявки.

   Заявка на подключение к защищенной сети ViPNet № 12633 ГИС ТОР КНД включает в себя:

   а) официальное письмо, адресованное оператору;

   б) анкета на подключение к защищенной сети ViPNet № 12633 ГИС ТОР КНД (приложение № 1 к Регламенту);

   в) копия приказа о назначении ответственного пользователя СКЗИ;

Примечание: Заявка подается для каждой внешней информационной системы по отдельности.

3) эксплуатирующая организация в течение 10-и рабочих дней со дня получения заявки на подключение к защищенной сети ГИС ТОР КНД, проводит оценку оснований для подключения заявителя к защищенной сети ГИС ТОР КНД и технической возможности подключения к защищенной сети ViPNet ГИС ТОР КНД;

4) эксплуатирующая организация направляет решение о подключении заявителя к защищенной сети ГИС ТОР КНД по электронной почте в адрес заявителя и оператора в течение 3-х рабочих дней со дня принятия указанного решения.

Примечание: Эксплуатирующая организация имеет право отказать заявителю в подключении к защищенной сети ViPNet № 12633 ГИС ТОР КНД.

Возможными причинами отказа могут являться:

а) запрашиваемые сведения предоставлены не в полном объеме;

б) класс применяемых средств криптографической защиты информации выше КС3.

Решение об отказе в подключении заявителя к защищенной сети ViPNet № 12633 ГИС ТОР КНД направляется на электронный адрес заявителя и оператора в течение 5-и рабочих дней со дня принятия указанного решения;

5) при положительном решении эксплуатирующая организация проводит формирование файла дистрибутива (DST) и направляет ключевую информацию заявителю посредством фельдъегерской связи в течение 10-х рабочих дней со дня принятия указанного решения.

5.2. Порядок организации межсетевого взаимодействия защищенной сети ViPNet ГИС ТОР КНД с другими сетями ViPNet (для варианта № 3)

Организация межсетевого взаимодействия с защищенной сетью ViPNet ГИС ТОР КНД для варианта № 3 (п. 3.3 настоящего Регламента) выполняется в следующем порядке:

1) заявитель осуществляет закупку необходимого программного обеспечения или программно-аппаратного комплекса ViPNet;

2) участник информационного взаимодействия (далее – заявитель в лице Координатора региона) направляет в адрес:

а) оператора Заявку на организацию межсетевого взаимодействия с защищенной сетью ViPNet № 12633 ГИС ТОР КНД в официальном порядке за подписью координатора региона;

б) эксплуатирующей организации заявка направляется с зарегистрированного электронного адреса Координатора региона на электронный адрес СТП с приложением скан-копии официальной зарегистрированной Заявки на организацию межсетевого взаимодействия с защищенной сетью ГИС ТОР КНД оператору и исходных текстовых файлов Заявки.

Заявка на организацию межсетевого взаимодействия с защищенной сетью ViPNet № 12633 ГИС ТОР КНД включает в себя:

а) официальное письмо, адресованное оператору;

б) анкета на подключение к защищенной сети ViPNet № 12633 (приложение № 1 к Регламенту);

в) копия приказа о назначении ответственного пользователя СКЗИ.

Примечание: Заявка подается для каждой внешней информационной системы по отдельности.

3) эксплуатирующая организация в течение 10-и рабочих дней со дня получения заявки, проводит оценку оснований для организации межсетевого взаимодействия с защищенной сетью ViPNet № 12633 и проверку технической возможности подключения к защищенной сети ViPNet № 12633 ГИС ТОР КНД;

4) эксплуатирующая организация направляет решение о подключении заявителя к защищенной сети ViPNet № 12633 ГИС ТОР КНД по электронной почте в адрес заявителя и оператора в течение 3-х рабочих дней со дня принятия указанного решения.

Примечание: Эксплуатирующая организация имеет право отказать заявителю в подключении к защищенной сети ViPNet № 12633 ГИС ТОР КНД.

Возможными причинами отказа могут являться:

а) запрашиваемые сведения предоставлены не в полном объеме;

б) класс применяемых средств криптографической защиты информации выше КС3.

Решение об отказе в подключении заявителя к защищенной сети ViPNet № 12633 ГИС ТОР КНД направляется на электронный адрес заявителя и оператора в течение 5-и рабочих дней со дня принятия указанного решения;

5) администратор безопасности защищенной сети ViPNet № 12633 ГИС ТОР КНД осуществляет формирование индивидуального симметричного межсетевого мастер ключа;

6) администратору сторонней сети ViPNet по защищенному каналу передаются экспортные файлы;

7) администратор сторонней сети ViPNet осуществляет настройку межсетевого канала;

8) администратор безопасности защищенной сети ViPNet № 12633 ГИС ТОР КНД осуществляет ответный экспорт из сторонней сети ViPNet;

9) по результатам оформляется протокол установления межсетевого взаимодействия (форма протокола приведена в приложении 2 к Регламенту). Протокол оформляется в двух экземплярах и передается для подписи заявителю почтовым отправлением.

10) Заявитель возвращает подписанный экземпляр протокола эксплуатирующей организации.

5.3. Порядок подключения устройств пользователей для работы с веб-ресурсами ГИС ТОР КНД без подключения к защищенной сети ViPNet (для варианта № 4)

Подключение устройств пользователей к ГИС ТОР КНД (для варианта 4) различается в зависимости от типов устройств пользователей (АРМ, мобильные устройства) и применяемых операционных систем в порядке, определён в п. 5.3.1–5.3.4 настоящего Регламента.

5.3.1. Порядок подключения АРМ пользователей под управлением ОС семейства Windows для работы с веб-ресурсами ГИС ТОР КНД без подключения к защищенной сети ViPNet ГИС ТОР КНД

Для организации защищенной работы АРМ с веб-ресурсами ГИС ТОР КНД, на стороне АРМ пользователя необходимо:

1) Обеспечить соответствие АРМ требованиям п. 3.5 и 3.5.1 ЕФТТ;

2) Установить и настроить СКЗИ (п. 3.4.1 настоящего Регламента), совместимое с ОС и веб-браузером;

3) Установить плагин для веб-браузера, совместимый с СКЗИ и веб-браузером (в случае применения СКЗИ, функционирующего через веб-браузер совместно с плагином для веб-браузера);

4) Установить сертификаты веб-сервера (сертификаты x509 v3 расположены по адресу https://knd.gov.ru/document/connect):

   а) Для установки в хранилище СКЗИ «КриптоПро CSP» версия 5.0 (исполнение 1-Base, исполнение 2-Base, исполнение 3-Base) необходимо:

      1. Открыть приложение «КриптоПро CSP», далее вкладка «Сервис», нажать кнопку «Установить личный сертификат»;
      2. В открывшемся окне с помощью кнопки «Обзор» выбрать необходимый сертификат, нажать «Далее»;
      3. Проверить правильность заполнения полей, нажать «Далее»;

4. В открывшемся окне поставить маркер рядом с «Найти контейнер автоматически», убедиться, что было определено хранилище, нажать «Далее»;
5. В открывшемся окне нажать «Обзор» и выбрать хранилище сертификатов из списка предложенных («Личное» – для пользовательских сертификатов, «Доверенные корневые центры сертификации» – для корневых сертификатов), нажать «Ок», проверить наличие маркера у пункта «Установить сертификат (цепочку сертификатов) в контейнер», нажать далее;

б) Для установки в хранилище сертификатов на АРМ (требуется установленная СКЗИ «КриптоПро CSP» версия 5.0 (исполнение 1-Base, исполнение 2-Base, исполнение 3-Base)) необходимо:

1. Двойным нажатием левой кнопки мыши открыть файл, чтобы вызвать приложение «Мастер импорта сертификатов»;
2. В открывшемся окне поставить маркер рядом с вариантом «Текущий пользователь», нажать «Далее»;
3. В открывшемся окне в поле «Имя файла» указать расположение требуемого файла с помощью кнопки «Обзор», нажать «Далее»;
4. В открывшемся окне при необходимости указать пароль для закрытого ключа в соответствующем окне, нажать «Далее»;
5. В открывшемся окне поставить маркер «Автоматически определить хранилище на основе типа сертификата», нажать «Далее»;
6. Проверить информацию в поле «Были указаны следующие параметры», нажать «Готово»;
7. В открывшемся окне СКЗИ «КриптоПро CSP» выбрать из предложенных носитель для создания контейнера, нажать «ОК»;
8. В открывшемся окне установить пароль для контейнера в поле «Новый пароль», повторить его в поле «Повторите ввод», нажать «ОК»;
9. В открывшемся окне в поле «Введите пароль» ввести ранее установленный пароль, нажать «ОК», появится окно «Импорт успешно выполнен».

5) Для осуществления подключения с использованием Яндекс.Браузер необходимо наличие установленного СКЗИ «КриптоПро CSP». Чтобы активировать возможность подключения с использованием ГОСТ:

а) Открыть настройки браузера, открыть вкладку «Системные»;

б) Установить маркер «Подключаться к сайтам, использующим шифрование ГОСТ».

5.3.2. Порядок подключения АРМ пользователей под управлением ОС семейства Linux для работы с веб-ресурсами ГИС ТОР КНД без подключения к защищенной сети ViPNet ГИС ТОР КНД

Для организации защищенной работы АРМ под управлением ОС семейства Linux с веб-ресурсами ГИС ТОР КНД, на стороне АРМ пользователя необходимо:

1) Обеспечить соответствие АРМ требованиям п. 3.5 и 3.5.1 ЕФТТ.
2) Установить и настроить СКЗИ (см п. 3.4.2 настоящего регламента), совместимое с ОС и веб-браузером. Для этого необходимо:
   а) Загрузить совместимую версию СКЗИ «КриптоПро CSP» версия 5.0 (исполнение 1-Base, исполнение 2-Base, исполнение 3-Base) в формате .tgz;
   б) Разархивировать файл при помощи команды «`sudo tar -xvf <название_файла>.tgz`;
   в) Выполнить установку при помощи команды «`sudo sh install_gui.sh`»;
   г) В открывшемся окне мастера установки нажать кнопку «Далее» для продолжения установки;
   д) В открывшемся окне выбрать пункт «Установить пакеты CSP», нажать «ОК»;
   е) В открывшемся окне выбора устанавливаемых пакетов нажать «Да»;
   ж) В открывшемся окне выбрать пункт «Базовые», нажать «ОК» и в открывшемся меню установить маркеры для всех подпунктов с помощью кнопки «Пробел», нажать «ОК», после установки появится окно с уведомлением об успешной установке, нажать «ОК»;
   з) В открывшемся окне выбрать пункт «Другие», нажать «ОК» и в открывшемся меню установить маркеры для всех подпунктов с помощью кнопки «Пробел» (обязательно наличие маркера пункта «cprocsp-rdr-gui-gtk»), нажать «ОК», после установки появится окно с уведомлением об успешной установке, нажать «ОК»;
   и) В открывшемся окне выбрать пункт «Считыватели», нажать «ОК» и в открывшемся меню установить маркеры для всех подпунктов с помощью кнопки «Пробел», нажать «ОК», после установки появится окно с уведомлением об успешной установке, нажать «ОК»;

3) Установить плагин для веб-браузера, совместимый с СКЗИ и веб-браузером (в случае применения СКЗИ, функционирующего через веб-браузер совместно с плагином для веб-браузера).

4) Установить сертификаты веб-сервера (сертификаты x509 v3 расположены по адресу https://knd.gov.ru/document/connect), добавив их в СКЗИ «КриптоПро CSP» версия 5.0 (исполнение 1-Base, исполнение 2-Base, исполнение 3-Base) на АРМ для этого необходимо:

   а) Установить корневой сертификат с разрешением .crt, для этого необходимо:

      1. Поместить требуемый файл в папку пользователя;
      2. Выполнить команду «`sudo /opt/cprocsp/bin/amd64/certmgr -inst -cert -file /Путь/до/папки/название_сертификата.crt -store uRoot`».

   б) Установить пользовательский сертификат с разрешением .cer, для этого необходимо:

      1. Поместить требуемый файл в папку пользователя;
      2. Выполнить команду «`sudo /opt/cprocsp/bin/amd64/certmgr -inst -cert -file /Путь/до/папки/название_сертификата.cer -store uMy`».

Для проверки установки сертификатов выполнить команду «`/opt/cprocsp/bin/amd64/certmgr -list`».

5.3.3. Порядок подключения мобильных устройств под управлением ОС Android для работы с веб-ресурсами ГИС ТОР КНД без подключения к защищенной сети ViPNet ГИС ТОР КНД

Для организации защищенной работы мобильных устройств под управлением ОС Android с веб-ресурсами ГИС ТОР КНД, на стороне мобильного устройства пользователя необходимо:

1) Установить приложение «МП Инспектор на устройство, для этого необходимо:

   а) Загрузить установочный файл с расширением .APK на устройство;

   б) Убедиться в отсутствии на устройстве других версий приложения;

   в) С помощью приложения «Файлы» открыть папку, в которую загружен установочный файл;

г) Нажать на необходимый файл, в открывшемся окне нажать «Продолжить»;

д) В открывшемся окне нажать «Установить».

2) Установить корневой сертификат безопасности в память устройства, для этого необходимо:

а) Загрузить корневой сертификат в хранилище устройства;

б) Открыть меню установки сертификатов (Настройки > WI-FI > Настройки Wi-FI > Расширенные настройки > установка сертификатов;

в) Выбрать папку, содержащую сертификат;

г) Выбрать необходимый сертификат, ввести PIN-код устройства, указать название сертификата, нажать «ОК»

5.3.4. Порядок подключения мобильных устройств под управлением ОС Аврора для работы с веб-ресурсами ГИС ТОР КНД без подключения к защищенной сети ViPNet ГИС ТОР КНД

Для организации защищенной работы мобильных устройств под управлением ОС Аврора с веб-ресурсами ГИС ТОР КНД, на стороне мобильного устройства требуется установка приложения «МП Инспектор». Установка приложений на устройства под управлением ОС Аврора производится компанией разработчиком ОС – ООО «Открытая Мобильная Платформа».

Для организации защищенной работы мобильных устройств под управлением ОС Аврора с веб-ресурсами ГИС ТОР КНД, на стороне мобильного устройства пользователя требуется добавление корневого сертификата безопасности, для этого необходимо:

1) Добавление корневого сертификата возможно только с использованием суперпользователя. Для настройки суперпользователя необходимо:

а) На мобильном устройстве открыть Настройки, далее перейти во раздел «Система» и открыть «Режим разработчика»;

б) На странице «Режим разработчика» нажать на «режим Разработчика»;

в) В открывшейся странице «Условия разработчика» необходимо подтвердить принятие условий;

г) В странице «Режим разработчика» необходимо открыть «Удаленное соединение»;

д) В открывшемся поле необходимо задать пароль для суперпользователя или нажать кнопку «заполнение» для автоматической генерации пароля;

е) Нажать «Сохранить»;

2) Для добавления корневого сертификата на устройство необходимо:

а) Подключить мобильное устройство к ПК через USB-кабель, на мобильном устройстве во всплывающем окне выбрать режим «Протокол передачи мультимедиа (MTP);

б) Корневой сертификат необходимо поместить с ПК на устройство в папку «название устройства»/Mass storage/Downloads;

в) На устройстве открыть приложение «Терминал» и зайти как суперпользователь:

1. Ввести команду «`devel-su`»;
2. Система запросит пароль, ввести ранее установленный пароль, нажать кнопку «ввод»;

г) Ввести команду «`cp Download/название_сертификата.crt /etc/pki/ca-trust/source/anchors/название_сертификата.crt`»;

д) Нажать «ввод»;

е) Ввести команду «`update-ca-trust`» для обновления списка добавленных сертификатов.

3) Для проверки добавления сертификата необходимо:

а) Открыть настройки устройства;

б) Перейти в раздел «Безопасность» и открыть вкладку «Сертификаты»;

в) В открывшемся окне выбрать «TLS Сертификаты»;

г) Найти в списке сертификатов необходимый или воспользоваться поиском по названию в верхней части экрана.

Для осуществления работы необходимо установленное приложение «МП Инспектор». Для его использования необходимо:

1) Открыть приложение, нажав на иконку «Инспектор» в основном меню;

2) В открывшемся приложении ввести учетные данные пользователя (логин и пароль), нажать «Войти».

6. Требования по обеспечению информационной безопасности ОИ КНО

Для ОИ КНО (ВИС КНО, СВТ), подключаемых к ГИС ТОР КНД, должны выполняться требования по безопасности информации в соответствии с нормативными правовыми актами в области защиты информации, документацией на используемые средства защиты информации и средства криптографической защиты информации, а также с учетом положений раздела 3 ЕФТТ.

Приложение № 1
к Регламенту подключения к
защищенной сети государственной
информационной системы
«Типовое облачное решение
по автоматизации контрольно-надзорной
деятельности»

Анкета на подключение к защищенной сети ViPNet № 12633 ГИС ТОР КНД

1. Заполненную анкету с копией приказа о назначении ответственного пользователя СКЗИ необходимо направить приложением к официальному письму на имя директора Департамента проектов цифровой трансформации Минцифры России – Качанова Олега Юрьевича.

2. Копию официального письма, анкеты и приказа о назначении ответственного пользователя СКЗИ, а также текстовые файлы документов необходимо направить с зарегистрированного электронного адреса Координатора региона на электронный адрес службы технической поддержки ГИС ТОР КНД «kndsupport@voskhod.ru» (копия на «knd@digital.gov.ru»).

1. Общие сведения об Организации

1.	Наименование региона	
2.	Полное наименование организации	
3.	Сокращенное наименование организации	
4.	ИНН	
5.	ОГРН	
6.	Юридический адрес организации	
7.	Фактический (почтовый) адрес организации	
8.	Телефон организации	
9.	ФИО сотрудника, ответственного за подключение к защищенной сети ГИС ТОР КНД	
10.	Контактный телефон сотрудника (технического специалиста), ответственного за подключение	
11.	Адрес электронной почты сотрудника (технического специалиста), ответственного за подключение	
12.	Часы работы по московскому времени	
13.	Наименование и ОГРН оператора связи, реквизиты заключенного договора на оказание услуг сети связи общего пользования (Интернет)	
14.	Цель подключения к защищенной сети ГИС ТОР КНД: 1. Обеспечение защищенного информационного взаимодействия ВИС КНО с ресурсами ГИС ТОР	

	КНД 2. Организация защищенной работы пользователей с ресурсами ГИС ТОР КНД 3. Обеспечение защищенного информационного взаимодействия ВИС КНО с ресурсами ГИС ТОР КНД и организация защищенной работы пользователей с ресурсами ГИС ТОР КНД	

2. Сведения о технических средствах, имеющихся у Организации для подключения к защищенной сети ViPNet № 12633 ГИС ТОР КНД

15.	Планируемый вариант подключения к защищенной сети ViPNet № 12633 в соответствии с разделом 3 Регламента (Вариант 1, Вариант 2, Вариант 3)	
16.	Модель (исполнение) ViPNet Coordinator	
17.	Количество ViPNet Coordinator	
18.	Класс защиты ViPNet Coordinator (КС1, КС2, или КС3)	
19.	Количество ViPNet Client (для АРМ)	
20.	Версия ViPNet Client (для АРМ)	
21.	Класс защиты ViPNet Client для АРМ (КС1, КС2 или КС3)	
22.	Количество ViPNet Client (для мобильных устройств)	
23.	Версия ViPNet Client (для мобильных устройств)	
24.	Класс защиты ViPNet Client для мобильных устройств (КС1, КС2 или КС3)	
25.	Номер сторонней сети ViPNet *(для варианта № 3)*	
26.	Класс защищенности сторонней сети ViPNet (КС1, КС2 или КС3) *(для Варианта 3)*	

3. Сведения о внешней информационной системе КНО (ВИС КНО)

для варианта № 1,2,3

27.	Наименование ведомственной информационной системы КНО	
28.	Класс защищенности, в соответствии с Приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»	
29.	Уровень защищенности персональных данных в соответствии с Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»	
30.	Реквизиты договора (соглашения) об информационном взаимодействии с оператором ГИС ТОР КНД	
31.	Сведения о документе, подтверждающим выполнение в ВИС КНО требований по защите информации: номер и дата выдачи аттестата соответствия (или иного документа, подтверждающего соответствие ВИС КНО требованиям о защите информации), срок действия и наименование организации, выдавшей документ	

4. Сведения о пользователях, допущенных к работе с СКЗИ

Пользователи ViPNet Client (*для варианта 1,2*)

№	ФИО	Подразделение	Должность	Электронная почта	Контактный телефон	
1.						

Администратор безопасности, сетевой администратор (*для варианта 1,2*)

№	ФИО	Подразделение	Должность	Электронная почта	Контактный телефон	
1.						

Администратор сети ViPNet, сетевой администратор (*для варианта 3*)

№	ФИО	Подразделение	Должность	Электронная почта	Контактный телефон	
1.						

Пользователи СКЗИ на АРМ и мобильных устройствах (*для варианта 4*)

№	ФИО	Подразделение	Должность	Электронная почта	Контактный телефон	Тип устройства (АРМ, Моб.устройства)
1.						

Должность Подпись ФИО

Приложение № 2
к Регламенту подключения к
защищенной сети государственной
информационной системы
«Типовое облачное решение
по автоматизации контрольно-надзорной
деятельности»

Форма протокола установления межсетевого взаимодействия ViPNet

1. Межсетевое взаимодействие устанавливается между следующими сетями:

Номер сети	**Наименование владельца сети, ОГРН**	**Наименование пользователя сети, ОГРН**

1. Передача начального и ответного экспорта между сетями № _____ и № _____ осуществлялась через специалиста, уполномоченного на данные действия.

2. При установлении межсетевого взаимодействия, были произведены импорты справочников главных абонентов сети.

3. Смена межсетевых ключей, изменение состава АП, участвующих в межсетевом взаимодействии, производится после предварительного согласования средствами взаимного экспорта/импорта, о чем администраторы защищенных сетей уведомляют друг друга с помощью ПО ViPNet [Клиент] [Делова почта] с указанием производимых изменений.

4. Стороны обязуются без предварительного согласия не производить изменений в настройках и структуре защищенных сетей, которые могут привести к нарушению межсетевого взаимодействия.

Администратор безопасности
эксплуатирующей организации

ФИО

подпись

Администратор безопасности
внешней информационной системы

ФИО

подпись

Лист регистрации изменений

№	Дата	Изменение	Присвоенная версия