МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ

_____ №_____

Москва

О внесении изменений в приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 26.01.2021 № 29 «Об утверждении Единых функционально-технических требований по автоматизации видов регионального государственного контроля (надзора) в целях внедрения риск-ориентированного подхода»

В целях методической поддержки обеспечения субсидий на поддержку региональных проектов в сфере информационных технологий, а также с учетом положений Федерального закона от 31 июля 2020 г. № 248-ФЗ «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации», вступивших в силу с 1 июля 2021 г., предусматривающих возможность передачи информации о контрольных (надзорных) мероприятиях в 2021 году как в единой реестр проверок, так и в единой реестр контрольных (надзорных) мероприятий,

ПРИКАЗЫВАЮ:

1. Внести в Единые функционально-технические требования по автоматизации видов регионального государственного контроля (надзора) в целях внедрения риск-ориентированного подхода, утвержденные приказом Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 26.01.2021 № 29, следующие изменения:

1) раздел «Основные термины, определения и сокращения» изложить в следующей редакции:

«

Сокращение / Термин	**Определение**
Авторизация	Предоставление субъекту доступа прав доступа, а также предоставление доступа в соответствии с установленными правилами управления доступом

АРМ	Автоматизированное рабочее место
Аутентификация	Действия по проверке подлинности субъекта доступа и/или объекта доступа, а также по проверке принадлежности субъекту доступа и/или объекту доступа предъявленного идентификатора доступа и аутентификационной информации
Базовый показатель	Отчетная информация по объектам контроля (надзора), привязанная к отчетным периодам, включая данные о проводимых и планируемых работах в отношении объектов, затратах и пр.
ВИС КНО	Ведомственная информационная система автоматизации контрольно-надзорной деятельности контрольно-надзорного органа
ГИС	Государственная информационная система
ГИС ТОР КНД	Государственная информационная система «Типовое облачное решение по автоматизации контрольной (надзорной) деятельности»
ЕСИА	Федеральная государственная информационная система «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме»
ЕИС КНД	Единая информационная среда контрольной (надзорной) деятельности. Структура ЕИС КНД определена в соответствии с Функциональной архитектурой Единой информационной среды контрольной (надзорной) деятельности и Стандартом информатизации контрольно-надзорной деятельности, утвержденными протоколом заседания Проектного комитета по основному направлению стратегического развития Российской Федерации «Реформа контрольной и надзорной деятельности» от 14.06.2017 № 40(6) (далее – Архитектура и Стандарт соответственно)
ЕРП	Федеральная государственная информационная система «Единый реестр проверок»
ЕРКНМ	Федеральная государственная информационная система «Единый реестр контрольных (надзорных) мероприятий»

ЕФТТ	«Единые функционально-технические требования по автоматизации видов регионального государственного контроля (надзора) в целях внедрения риск-ориентированного подхода»
Идентификация	Действия по присвоению субъектам и объектам доступа идентификаторов и/или по сравнению предъявляемого идентификатора с перечнем присвоенных идентификаторов
Информационная модель, семантическая информационная модель, СИМ	Семантическая структура данных, построенная по принципам онтологического моделирования в соответствии со стандартами консорциума World Wide Web Consortium: RDF, RDFS, OWL, OWL2, SKOS. В онтологическом моделировании используется семантическая структура данных, включающая четыре основных типа сущностей: - классы; - свойства-литералы; - свойства-связи; - экземпляры, или индивидуальные объекты
Информационная система (ИС)	Совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств
ИС ПСД	Единая Государственная платформа сбора данных, промышленного Интернета вещей и инструментов анализа объективных данных о наблюдаемых объектах в составе платформы исполнения Государственных функций. ИС ПСД интегрирована с ГИС ТОР КНД
Клиент	Сервис (программный модуль), который может быть авторизован для работы от имени пользователя или с данными других сервисов
КНО	Контрольно-надзорный орган или организация
Контрольно-надзорная деятельность (КНД)	Деятельность по реализации функций органа исполнительной власти субъекта Российской Федерации при осуществлении государственного контроля (надзора), органа местного самоуправления при осуществлении муниципального контроля
Минцифры России	Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации
НПА	Нормативный правовой акт

НСИ	Нормативно-справочная информация
ОИ	Объект информатизации
Оператор ФГИС ЕРП, ФГИС ЕРКНМ	Генеральная прокуратура Российской Федерации
ПК	Персональный компьютер
ПОИБ	Подсистема обеспечения информационной безопасности
ПЭВМ	Персональная электронно-вычислительная машина
Расчетный показатель	Отчетная информация по объектам контроля (надзора), привязанная к отчетным периодам и получаемая путем расчета на основе базовых показателей
СВТ	Средство вычислительной техники
СЗИ	Средство защиты информации
СКЗИ	Средство криптографической защиты информации
СМЭВ	Единая система межведомственного электронного взаимодействия
СЭП	Средство электронной подписи
Стандарт информатизации КНД	Комплекс требований к информационным системам, входящим в состав единой информационной среды контрольно-надзорной деятельности, направленный на реализацию основных направлений приоритетной программы «Реформа контрольной и надзорной деятельности», утвержденной президиумом Совета при Президенте Российской Федерации по стратегическому развитию и приоритетным программам (протокол от 21.12.2016 №12), и предусматривающий три уровня соответствия функциональных возможностей информационных систем: Базовый, Средний, Высокий
Токен	Уникальный код с ограниченным сроком жизни, выдается после аутентификации и используется при взаимодействии с остальными участниками системы
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

»;

2) в разделе 2:

пункт 2 изложить в следующей редакции:

«2. Доработка существующих ВИС КНО в субъекте Российской Федерации в целях интеграции их с государственными информационными системами в сфере государственного контроля (надзора).»;

в пункте 5 слово «в ЕРП)» заменить словами «в ЕРП или в ЕРКНМ)»;

3) в разделе 4.2:

наименование изложить в следующей редакции:

«Требования по доработке существующих региональных ВИС КНО в целях интеграции с государственными информационными системами в сфере государственного контроля (надзора)»;

абзац первый изложить в следующей редакции:

«В рамках создания ЕИС КНД рекомендуется интегрировать региональные ВИС КНО с ГИС ТОР КНД, ФГИС ЕРП, ФГИС ЕРКНМ в целях автоматизации процессов передачи данных о проверяемых субъектах, проверяемых объектах, данных о проверках в отношении указанных лиц. Интеграция может осуществляться как с одной из перечисленных ГИС, так и с несколькими. Интеграция с ФГИС ЕРП должна быть осуществлена по актуальным видам сведений СМЭВ «Размещение сведений в реестре электронных паспортов контрольно-надзорных мероприятий» версии не ниже 3.0.3 и при необходимости «Сведения из электронных паспортов контрольно-надзорных мероприятий» версии не ниже 1.0.0. Интеграция с ФГИС ЕРКНМ должна быть осуществлена по актуальным видам сведений СМЭВ «Размещение сведений в едином реестре контрольных (надзорных) мероприятий» версии не ниже 6.0.2 и при необходимости «Сведения из электронных паспортов контрольно-надзорных мероприятий» версии не ниже 3.0.1. Актуальные версии видов сведений необходимо уточнить на технологическом портале СМЭВ (https://smev3.gosuslugi.ru/portal/).»;

абзац четвертый изложить в следующей редакции:

«В части требований к защите информации при интеграции с ГИС ТОР КНД руководствоваться положениями раздела 3 настоящих ЕФТТ, при интеграции с ФГИС ЕРП и (или) ФГИС ЕРКНМ руководствоваться требованиями к защите информации СМЭВ 3.х и Оператора ФГИС ЕРП, ФГИС ЕРКНМ.».

2. Контроль за исполнением настоящего приказа возложить на заместителя Министра цифрового развития, связи и массовых коммуникаций Российской Федерации О.Ю. Качанова.

Министр М.И. Шадаев

УТВЕРЖДЕНЫ
приказом Министерства
цифрового развития, связи и массовых
коммуникаций
Российской Федерации
от «26» января 2021 г. № 29

Единые функционально-технические требования по автоматизации видов регионального государственного контроля (надзора) в целях внедрения риск-ориентированного подхода

Содержание

Основные термины, определения и сокращения

Сокращение / Термин	Определение
Авторизация	Предоставление субъекту доступа прав доступа, а также предоставление доступа в соответствии с установленными правилами управления доступом
АРМ	Автоматизированное рабочее место
Аутентификация	Действия по проверке подлинности субъекта доступа и/или объекта доступа, а также по проверке принадлежности субъекту доступа и/или объекту доступа предъявленного идентификатора доступа и аутентификационной информации
Базовый показатель	Отчетная информация по объектам контроля (надзора), привязанная к отчетным периодам, включая данные о проводимых и планируемых работах в отношении объектов, затратах и пр.
ВИС КНО	Ведомственная информационная система автоматизации контрольно-надзорной деятельности контрольно-надзорного органа
ГИС	Государственная информационная система
ГИС ТОР КНД	Государственная информационная система «Типовое облачное решение по автоматизации контрольной (надзорной) деятельности»
ЕСИА	Федеральная государственная информационная система «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме»
ЕИС КНД	Единая информационная среда контрольной (надзорной) деятельности. Структура ЕИС КНД определена в соответствии с Функциональной архитектурой Единой информационной среды контрольной (надзорной) деятельности и Стандартом информатизации контрольно-надзорной деятельности, утвержденными протоколом заседания Проектного комитета по основному направлению стратегического

Сокращение / Термин	Определение
	развития Российской Федерации «Реформа контрольной и надзорной деятельности» от 14.06.2017 № 40(6) (далее – Архитектура и Стандарт соответственно)
ЕРП	Федеральная государственная информационная система «Единый реестр проверок»
ЕРКНМ	Федеральная государственная информационная система «Единый реестр контрольных (надзорных) мероприятий»
ЕФТТ	«Единые функционально-технические требования по автоматизации видов регионального государственного контроля (надзора) в целях внедрения риск-ориентированного подхода»
Идентификация	Действия по присвоению субъектам и объектам доступа идентификаторов и/или по сравнению предъявляемого идентификатора с перечнем присвоенных идентификаторов
Информационная модель, семантическая информационная модель, СИМ	Семантическая структура данных, построенная по принципам онтологического моделирования в соответствии со стандартами консорциума World Wide Web Consortium: RDF, RDFS, OWL, OWL2, SKOS. В онтологическом моделировании используется семантическая структура данных, включающая четыре основных типа сущностей: - классы; - свойства-литералы; - свойства-связи; - экземпляры, или индивидуальные объекты
Информационная система (ИС)	Совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств
ИС ПСД	Единая Государственная платформа сбора данных, промышленного Интернета вещей и инструментов анализа объективных данных о наблюдаемых объектах в составе платформы исполнения Государственных функций. ИС ПСД интегрирована с ГИС ТОР КНД.
Клиент	Сервис (программный модуль), который может быть авторизован для работы от имени пользователя или с данными других сервисов

Сокращение / Термин	Определение
КНО	Контрольно-надзорный орган или организация
Контрольно-надзорная деятельность (КНД)	Деятельность по реализации функций органа исполнительной власти субъекта Российской Федерации при осуществлении государственного контроля (надзора), органа местного самоуправления при осуществлении муниципального контроля
Минцифры России	Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации
НПА	Нормативный правовой акт
НСИ	Нормативно-справочная информация
ОИ	Объект информатизации
Оператор ФГИС ЕРП, ФГИС ЕРКНМ	Генеральная прокуратура Российской Федерации
ПК	Персональный компьютер
ПОИБ	Подсистема обеспечения информационной безопасности
ПЭВМ	Персональная электронно-вычислительная машина
Расчетный показатель	Отчетная информация по объектам контроля (надзора), привязанная к отчетным периодам и получаемая путем расчета на основе базовых показателей
СВТ	Средство вычислительной техники
СЗИ	Средство защиты информации
СКЗИ	Средство криптографической защиты информации
СМЭВ	Единая система межведомственного электронного взаимодействия
СЭП	Средство электронной подписи
Стандарт информатизации КНД	Комплекс требований к информационным системам, входящим в состав единой информационной среды контрольно-надзорной деятельности, направленный на

Сокращение / Термин	Определение
	реализацию основных направлений приоритетной программы «Реформа контрольной и надзорной деятельности», утвержденной президиумом Совета при Президенте Российской Федерации по стратегическому развитию и приоритетным программам (протокол от 21.12.2016 №12), и предусматривающий три уровня соответствия функциональных возможностей информационных систем: Базовый, Средний, Высокий
Токен	Уникальный код с ограниченным сроком жизни, выдается после аутентификации и используется при взаимодействии с остальными участниками системы
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

1. Нормативно-правовые основания автоматизации контрольно-надзорной деятельности

Основаниями для автоматизации контрольно-надзорной деятельности и внедрения риск-ориентированного подхода в целом и реализации рассматриваемых в настоящих требованиях мероприятий в частности являются следующие нормативно-правовые документы:

– Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;

– Федеральный закон от 26.12.2008 № 294-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля»;

– Федеральный закон от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг»;

– Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи»;

– Федеральный закон от 31.07.2020 № 247-ФЗ «Об обязательных требованиях в Российской Федерации»;

– Федеральный закон от 31.07.2020 № 248-ФЗ «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации»;

– постановление Правительства Российской Федерации от 08.09.2010 № 697 «О единой системе межведомственного электронного взаимодействия»;

– постановление Правительства Российской Федерации от 08.06.2011 № 451 «Об инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме»;

– постановление Правительства Российской Федерации от 28.11.2011 № 977 «О федеральной государственной информационной системе «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме»;

– постановление Правительства Российской Федерации от 28.12.2011 № 1184 «О мерах по обеспечению перехода федеральных органов исполнительной власти и органов государственных внебюджетных фондов на межведомственное информационное взаимодействие в электронном виде»;

– постановление Правительства Российской Федерации от 09.02.2012 № 111 «Об электронной подписи, используемой органами исполнительной власти и органами местного самоуправления при организации электронного взаимодействия между собой, о порядке ее использования, а также об установлении требований к обеспечению совместимости средств электронной подписи»;

– постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– постановление Правительства Российской Федерации от 22.12.2012 № 1382 «О присоединении информационных систем организаций к инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме»;

– постановление Правительства Российской Федерации от 19.11.2014 № 1222 «О дальнейшем развитии единой системы межведомственного электронного взаимодействия»;

– постановление Правительства Российской Федерации от 06.07.2015 № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем, и дальнейшего хранения содержащейся в их базах данных информации»;

– постановление Правительства Российской Федерации от 18.04.2016 № 323 «О направлении запроса и получении на безвозмездной основе, в том числе в электронной форме, документов и (или) информации органами государственного контроля (надзора), органами муниципального контроля при организации и проведении проверок от иных государственных органов, органов местного самоуправления либо подведомственных государственным органам или органам местного самоуправления организаций, в распоряжении которых находятся эти документы и (или) информация, в рамках межведомственного информационного взаимодействия»;

– постановление Правительства Российской Федерации от 17.08.2016 № 806 «О применении риск-ориентированного подхода при организации отдельных видов государственного контроля (надзора) и внесении изменений в некоторые акты Правительства Российской Федерации»;

– постановление Правительства Российской Федерации от 21.04.2018 № 482 «О государственной информационной системе «Типовое облачное решение по автоматизации контрольной (надзорной) деятельности»;

– Государственная программа Российской Федерации «Информационное общество (2011 – 2020 годы)» (утверждена постановлением Правительства Российской Федерации от 15.04.2014 № 313), подпрограмма 4 «Информационное государство»;

– распоряжение Правительства Российской Федерации от 19.04.2016 № 724-р об утверждении перечня документов и (или) информации, запрашиваемых и получаемых в рамках межведомственного информационного взаимодействия органами государственного контроля (надзора), органами муниципального контроля (надзора) при организации и проведении проверок от иных государственных органов, органов местного самоуправления либо организаций, в распоряжении которых находятся эти документы и (или) информация;

– распоряжение Правительства Российской Федерации от 17.05.2016 № 934-р об утверждении основных направлений разработки и внедрения системы оценки результативности и эффективности контрольно-надзорной деятельности;

– распоряжение Правительства Российской Федерации от 31.01.2017 № 147-р об утверждении целевых моделей упрощения процедур ведения бизнеса и повышения инвестиционной привлекательности субъектов Российской Федерации;

– распоряжение Правительства Российской Федерации от 26.09.2017 № 2049-р об утверждении плана мероприятий («дорожной карты») по созданию, развитию и вводу в эксплуатацию информационной системы «Типовое облачное решение по автоматизации контрольной (надзорной) деятельности» на 2017 – 2019 годы;

– приказ Минкомсвязи России от 27.12.2010 № 190 «Об утверждении Технических требований к взаимодействию информационных систем в единой системе межведомственного электронного взаимодействия»;

– приказ ФСБ России от 27.12.2011 № 795 «Об утверждении Требований к форме квалифицированного сертификата ключа проверки электронной подписи»;

– приказ ФСБ России от 27.12.2011 № 796 «Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра»;

– приказ ФСТЭК России от 02.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

– приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

– 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»;

2. Цели и задачи выполнения работ по автоматизации контрольно-надзорной деятельности

В соответствии с государственной программой Российской Федерации «Информационное общество (2011 – 2020 годы)», утвержденной постановлением Правительства Российской Федерации от 15.04.2014 № 313 (в редакции постановления Правительства Российской Федерации от 30.12.2018 № 1761) (далее – Программа), целевым индикатором, соотнесенным с автоматизацией КНД, определена доля проверок, осуществляемых по приоритетным видам регионального государственного контроля (надзора), информация о которых вносится в единый реестр проверок с использованием единой системы межведомственного электронного взаимодействия, в общем количестве указанных проверок.

Для достижения указанного показателя предоставляются субсидии из федерального бюджета в целях софинансирования расходных обязательств субъектов Российской Федерации, связанных с реализацией проектов (мероприятий), направленных на становление информационного общества в субъектах Российской Федерации, предусмотренных в государственных программах субъектов Российской Федерации. Проектом (мероприятием), направленным на становление информационного общества в субъектах Российской Федерации, в соответствии с пунктом 3 приложения № 2 к Программе является автоматизация приоритетных видов регионального государственного контроля (надзора) в целях внедрения риск-ориентированного подхода и дистанционного контроля.

Автоматизация КНД КНО субъекта Российской Федерации возможна на базе как локального, разработанного адресно для КНО субъекта Российской Федерации, существующего информационного решения – ВИС КНО, так и на базе централизовано предоставляемого решения на базе ГИС ТОР КНД.

Рекомендуемые мероприятия по автоматизации приоритетных видов регионального государственного контроля (надзора) в целях внедрения риск-ориентированного подхода и/или дистанционного контроля предполагают детализацию по следующим направлениям автоматизации КНД в рамках ЕИС КНД:

1. Разработка независимо-компилируемых программных модулей (плагинов), динамически подключаемых к государственной информационной системы «Типовое облачное решение по автоматизации контрольно-надзорной деятельности» (далее – ГИС ТОР КНД) и публикации их в Национальном фонде алгоритмов и программ (НФАП).
2. Доработка существующих ВИС КНО в субъекте Российской Федерации с целью интеграции их с государственными информационными системами в сфере государственного контроля (надзора).
3. Закупка автоматизированных рабочих мест, в том числе переносных, и другого оборудования для штатных единиц по должностям, предусматривающим выполнение функций по контролю (надзору) в субъекте Российской Федерации для обеспечения работы в ГИС ТОР КНД или ВИС КНО.

4. Обеспечение соответствия требованиям безопасности ВИС КНО и (или) автоматизированных рабочих мест, в том числе переносных, обеспечивающих выполнение функций по контролю (надзору) в субъекте Российской Федерации.

5. Закупка, установка и настройка средств удаленной фиксации состояний объектов контроля (надзора), включая технические средства и программное обеспечение связи и организации (или подключения) к сети передачи данных, в целях сбора и использования сведений с указанных средств фиксации в ГИС ТОР КНД или ВИС КНО для планирования, проведения и аудита контрольно-надзорных мероприятий в субъекте Российской Федерации (до вступления в силу ФЗ № 248 и положений по видам надзора сведения с указанных средств фиксации могут использоваться для целей тестирования технологии дистанционного мониторинга без проведения контрольно-надзорных мероприятий, требующих регистрации в ЕРП или в ЕРКНМ)».

6. Разработка агентов и/или иного интеграционного программного обеспечения для подключения источников данных к ИС ПСД.

7. Закупка, разработка и внедрение внешних расчетных систем и сервисов, для осуществления поддержки принятия решений в рамках обработки инцидентов.

8. Разработка, доработка и внедрение отраслевых прикладных сервисов по видам контроля (надзора) в ИС ПСД.

9. Внедрение ГИС ТОР КНД, включая работы по:

9.1. Обучению с целью создания центра компетенции по направлению «Автоматизация контрольной (надзорной) деятельности».

9.2 Обучению администраторов настройке процессов контроля и надзора в соответствии с региональной практикой.

9.3 Настройке процессов контроля и надзора в соответствии с региональной практикой.

Уполномоченный орган субъекта Российской Федерации определяет состав мероприятий с учетом целесообразности их реализации. При определении направлений автоматизации также учитывается, на базе какой информационной системы ранее была осуществлена автоматизации КНД по конкретному виду контроля (надзора).

3. Требования по защите информации в ГИС ТОР КНД

3.1. Общие сведения об организации защиты информации в ГИС ТОР КНД

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

– Требования о защите информации, не составляющей государственной тайны, содержащейся в государственных информационных системах, утвержденные приказом ФСТЭК России от 11.02.2013 № 17 – по второму классу защищенности;

– Требования к защите персональных данных при их обработке в информационных системах персональных данных, утвержденные постановлением Правительства Российской Федерации от 01.11.2012 № 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 ГИС ТОР КНД является российское юридическое лицо, определенное по результатам конкурсной процедуры, заключившее государственный контракт с Оператором (далее – эксплуатирующая организация).

ГИС ТОР КНД размещена в ЦОД на площадке эксплуатирующей организации.

В составе ГИС ТОР КНД реализована и функционирует подсистема обеспечения информационной безопасности (далее – ПОИБ), в состав которой входят средства защиты информации (далее – СЗИ), сертифицированные по требованиям безопасности информации ФСТЭК России, а также средства криптографической защиты информации (далее – СКЗИ) и средства электронной подписи (далее – СЭП), сертифицированные по требованиям безопасности ФСБ России.

Администрирование СЗИ, СКЗИ и СЭП из состава ПОИБ ГИС ТОР КНД, размещенной в ЦОД, осуществляется специалистами эксплуатирующей организации.

3.2. Общие требования по защите информации для внешних объектов информатизации при подключении к ГИС ТОР КНД

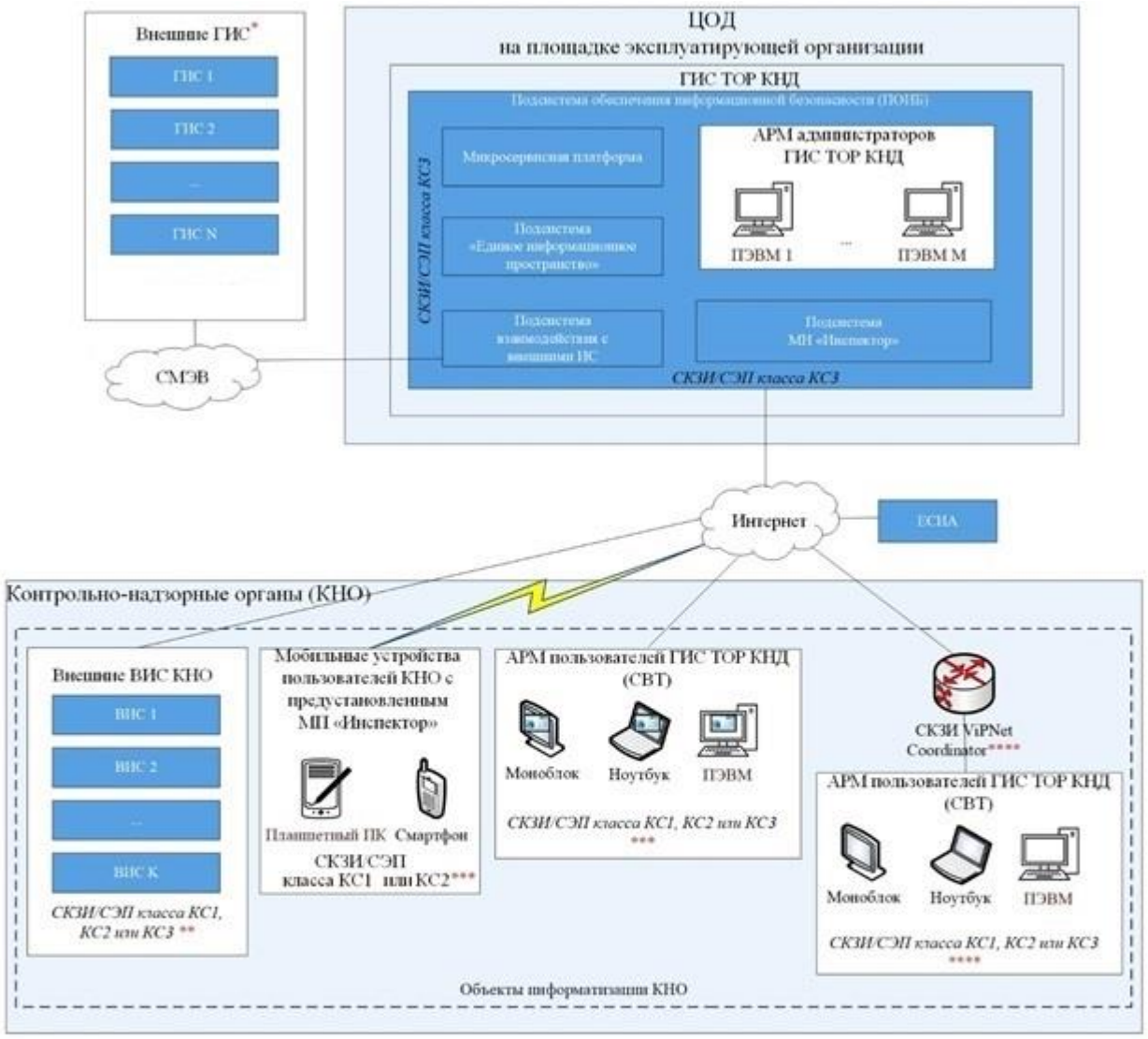
Внешними типовыми объектами информатизации (далее – ОИ), с которыми ГИС ТОР КНД обеспечивает поддержку защищенного информационного взаимодействия, являются:

– внешние государственные информационные системы (далее – ГИС);

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

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

На рисунке 1 приведены внешние типовые ОИ, с которыми ГИС ТОР КНД обеспечивает поддержку защищенного информационного взаимодействия.



Примечание
* К ГИС ТОР КНД запрещается подключение внешних ГИС с применением СКЗИ выше класса КС3.
** Класс СКЗИ для ВИС КНО определяется на основании моделей нарушителей безопасности информации ВИС КНО, в случае их отсутствия — согласно приложению к настоящим ЕФТТ.
*** Класс СКЗИ, применяемых на стороне СВТ (мобильных устройств и АРМ пользователей), определяется на основании моделей нарушителей безопасности информации на объекты информатизации КНО, в состав которых входят СВТ, в случае их отсутствия – согласно приложению к настоящим ЕФТТ.
**** Класс СКЗИ, применяемых на СВТ в составе объекта информатизации КНО, функционирующего в составе защищенной сети КНО на базе технологии ViPNet, определяется на основании моделей нарушителей на объект информатизации КНО, в случае их отсутствия, согласно приложению к настоящим ЕФТТ.

Рисунок 1. Схема организации защищенного информационного взаимодействия ГИС ТОР КНД с внешними типовыми ОИ

Для обеспечения защищенного информационного взаимодействия вышеперечисленных внешних ОИ с ГИС ТОР КНД на стороне ОИ требуется реализовать комплекс мероприятий с учетом требований действующего законодательства Российской Федерации и подзаконных нормативных правовых актов в области защиты информации, предъявляемых к конкретному ОИ в зависимости от класса защищенности ОИ и (или) уровней защищенности обрабатываемых на ОИ персональных данных (в случае осуществления обработки персональных данных на ОИ), актуальных угроз безопасности информации и возможностей потенциальных нарушителей, а также с учетом требований, приведенных в настоящих ЕФТТ.

Организация работ по защите информации на стороне вышеперечисленных ОИ осуществляется собственниками ОИ (операторами, владельцами).

При реализации КНО комплекса мероприятий по защите информации на ОИ рекомендуется:

– провести классификацию ОИ в соответствии с требованиями действующего законодательства Российской Федерации и подзаконных нормативных правовых актов в области защиты информации, с учетом обрабатываемой на ОИ информации, установить класс (категорию) защищенности ОИ и (или) уровень защищенности обрабатываемой информации (уровень защищенности персональных данных, в случае обработки персональных данных на ОИ);

– выполнить работы по моделированию угроз и нарушителей безопасности информации для ОИ, в т.ч. с учетом сведений, приведенных в настоящих ЕФТТ;

– сформировать требования к системе (подсистеме) защиты информации ОИ с учетом требований действующего законодательства Российской Федерации и подзаконных нормативных правовых актов в области защиты информации, актуальных угроз безопасности информации и установленного класса (категорию) защищенности ОИ и (или) уровня защищенности обрабатываемой информации (персональных данных, в случае обработки персональных данных на ОИ));

– разработать проектные решения на систему (подсистему) защиты информации ОИ, проектную и эксплуатационную документацию, а также комплект организационно-распорядительной документации по защите информации с учетом сведений, приведенных в настоящих ЕФТТ;

– осуществить внедрение СЗИ на ОИ, а также СКЗИ/СЭП с учетом разработанной проектной и эксплуатационной документацией на систему (подсистему) защиты информации ОИ и требований, приведенных в настоящих ЕФТТ;

– обеспечить внедрение на ОИ комплекса организационных и технических мер защиты, направленных на противодействие актуальным угрозам безопасности информации и возможностям потенциальных нарушителей, с учетом требований, предъявленных в настоящих ЕФТТ;

– провести обучение пользователей и лиц, ответственных за администрирование СЗИ/СКЗИ/СЭП, в составе ОИ;

– провести аттестацию ОИ на соответствие требованиям действующего

законодательства Российской Федерации и подзаконных нормативных правовых актов в области защиты информации.

Комплекс работ по защите информации на стороне КНО может быть выполнен самостоятельно или с привлечением специализированных организаций, обладающих лицензиями ФСТЭК и (или) ФСБ России:

– лицензия ФСТЭК России на деятельность по технической защите конфиденциальной информации на выполнение работ и (или) услуг согласно подпунктам «б», «г», «д», «е» пункта 4 Положения о лицензировании деятельности по технической защите конфиденциальной информации, утвержденного постановлением Правительства Российской Федерации от 03.02.2012 № 79;

– лицензия ФСБ России на деятельность по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя) на выполнение работ (оказание услуг) согласно пунктам 2, 12, 13, 20, 21 приложения к Положению о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя), утвержденному постановлением Правительства Российской Федерации от 16.04.2012 № 313.

Информационное взаимодействие внешних ОИ с ГИС ТОР КНД допускается при условии соблюдения на стороне ОИ требований по защите информации, приведенных в настоящих ЕФТТ.

К ГИС ТОР КНД запрещается подключение следующих ОИ:

– ОИ, в которых обрабатываются сведения, составляющие государственную тайну;

– ОИ, потенциальные нарушители которых обладают возможностями, перечисленными в пунктах 16, 17 и 18 приказа ФСБ России от 27.12.2011 г. № 796

«Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра»;

– ОИ, потенциальные нарушители которых обладают возможностями, перечисленными в пунктах 13 и 14 приказа 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».

3.3. Требования к организации защищенного взаимодействия внешних ГИС с ГИС ТОР КНД

Взаимодействие внешних ГИС, за исключением ЕСИА и ИС ПСД, с ГИС ТОР КНД допускается только по каналам связи СМЭВ v3 (не ниже), защищенных с применением СКЗИ/СЭП в соответствии с Методическими рекомендациями по работе с Единой системой межведомственного электронного взаимодействия (актуальные версии методических рекомендаций размещены на технологическом портале СМЭВ по адресу https://smev3.gosuslugi.ru/portal/), и при соблюдении следующих условий:

– при наличии договора (соглашения) об информационном взаимодействии с оператором (обладателем, владельцем) внешней ГИС либо при установлении необходимости такого взаимодействия нормативным правовым актом;

– при наличии подтверждения выполнения во внешней ГИС требований о защите информации (наличие аттестата соответствия требованиям по безопасности информации или иного подтверждения).

Взаимодействие ГИС ТОР КНД с ЕСИА должно осуществляться в соответствии с Методическими рекомендациями по использованию Единой системы идентификации и аутентификации (актуальные версии методических рекомендаций размещены на портале Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации по адресу https://digital.gov.ru/ru/documents/).

3.4. Требования к организации защищенного взаимодействия ВИС КНО с ГИС ТОР КНД

Взаимодействие ВИС КНО с ГИС ТОР КНД допускается по каналам сети связи общего пользования (Интернет) при соблюдении следующих условий:

– наличие на стороне ВИС КНО СКЗИ семейства ViPNet, обеспечивающего криптографическую защиту канала связи при работе с ресурсами ГИС ТОР КНД через сеть связи общего пользования (Интернет);

– предоставление услуг по доступу к сети связи общего пользования (Интернет) на основании заключенных КНО договоров с операторами связи (юридическими лицами или индивидуальными предпринимателями,

зарегистрированными на территории Российской Федерации, оказывающими услуги связи на основании соответствующей лицензии в соответствии с Федеральным законом от 07.07.2003 № 126-ФЗ «О связи»);

– наличие договора (соглашения) об информационном взаимодействии с оператором (обладателем, владельцем) ВИС КНО либо при установлении необходимости такого взаимодействия нормативным правовым актом;

– наличие подтверждения выполнения в ВИС КНО требований о защите информации (наличие аттестата соответствия требованиям по безопасности информации или иного подтверждения).

В целях организации защищенного взаимодействия ВИС КНО с ГИС ТОР КНД требуемый для применения в ВИС КНО класс СКЗИ (КС1, КС2, или КС3) определяется оператором ВИС КНО на основании разработанной для ВИС КНО модели нарушителя безопасности информации.

ГИС ТОР КНД не поддерживает защищенное взаимодействие с ВИС КНО, защищенных с применением СКЗИ семейства ViPNet, сертифицированных ФСБ России по классу выше КС3.

В случае отсутствия у операторов ВИС КНО разработанных для ВИС КНО моделей нарушителей безопасности информации требуемый класс СКЗИ для подключения к ГИС ТОР КНД, а также перечень необходимых для реализации организационно-технических мер по защите информации на стороне ВИС КНО может быть определен оператором ВИС КНО согласно Методике, приведенной в приложении к настоящим ЕФТТ.

Требования по организации защищенного взаимодействия ВИС КНО к ГИС ТОР КНД с применением СКЗИ семейства ViPNet приведены в Регламенте подключения к защищенной сети государственной информационной системы «Типовое облачное решение по автоматизации контрольной (надзорной) деятельности» (актуальные редакции размещаются на портале ГИС ТОР КНД по адресу https://knd.gov.ru в разделе Документы / Подключение к ГИС ТОР КНД).

Администрирование СЗИ, СКЗИ и СВТ, эксплуатируемых в составе ВИС КНО, должны осуществлять сотрудники КНО, назначенные руководителем КНО.

3.5. Общие требования к организации защищенного взаимодействия СВТ пользователей с ГИС ТОР КНД

Для работы пользователей с ресурсами ГИС ТОР КНД допускается применение следующих СВТ, эксплуатируемых на стороне КНО отдельно или в составе ОИ КНО (ВИС КНО):

– АРМ в различном исполнении: ПЭВМ, моноблок, ноутбук;

– мобильные устройства: смартфоны, планшетные ПК.

При доступе к ресурсам ГИС ТОР КНД пользователей (сотрудников КНО) с СВТ могут использоваться проводные каналы связи, подключенные к сети общего пользования (Интернет), при соблюдении следующих условий:

– наличие на стороне СВТ СКЗИ, обеспечивающего криптографическую защиту канала связи при работе с ресурсами ГИС ТОР КНД через сеть связи общего пользования (Интернет);

– предоставление услуг по доступу к сети связи общего пользования (Интернет) на основании заключенных КНО договоров с операторами связи (юридическими лицами или индивидуальными предпринимателями, зарегистрированными на территории Российской Федерации, оказывающими услуги связи на основании соответствующей лицензии в соответствии с Федеральным законом от 07.07.2003 № 126-ФЗ «О связи»);

– наличие подтверждения выполнения на СВТ, эксплуатируемых в составе ОИ КНО (ВИС КНО), требований к защите информации (наличие аттестата соответствия требованиям по безопасности информации или иного подтверждения).

Пользователи (сотрудники КНО), планирующие работать с ресурсами ГИС ТОР КНД, должны являться представителями зарегистрированного в ЕСИА КНО и обладать действующей (зарегистрированной) учетной записью ЕСИА. Регистрация пользователей (сотрудников КНО) для работы с ГИС ТОР КНД и предоставление полномочий по доступу к ресурсам ГИС ТОР КНД осуществляется в соответствии с Порядком предоставления доступа (актуальные редакции размещаются на портале ГИС ТОР КНД по адресу https://knd.gov.ru разделе Документы/Подключение к ГИС ТОР КНД).

Пользователи ГИС ТОР КНД (сотрудники КНО) получают доступ к ГИС ТОР КНД согласно присвоенным ролям доступа после успешного прохождения процедуры аутентификации в ЕСИА, а также идентификации и авторизации в прикладном программном обеспечении (модуль защиты прикладного программного обеспечения) из состава ПОИБ ГИС ТОР КНД.

Защита информации, передаваемой по каналам связи, подключенным к сети общего пользования (Интернет), между ГИС ТОР КНД и СВТ, входящими в состав ОИ КНО (ВИС КНО), с которых пользователи ГИС ТОР КНД (сотрудники КНО) осуществляют информационное взаимодействие с ресурсами ГИС ТОР КНД, должна обеспечиваться путем применения СКЗИ на стороне СВТ, совместимых с СКЗИ, применяемыми в ГИС ТОР КНД, а также путем реализации на стороне ОИ КНО (ВИС КНО), в состав которых входят СВТ комплекса организационно-технических мер защиты информации, направленных на противодействие возможностям потенциальных нарушителей безопасности информации.

СКЗИ, применяемые на СВТ в составе ОИ КНО (ВИС КНО), должны быть сертифицированы в системе сертификации ФСБ России на соответствие требованиям нормативного документа «Требования к средствам криптографической защиты информации, предназначенные для защиты информации, не содержащей сведений, составляющих государственную тайну» по классу КС1, КС2 или КС3.

Необходимый класс СКЗИ для применения на СВТ должен быть уточнен КНО на основании моделей нарушителей безопасности информации ОИ, в состав которых входят СВТ пользователей.

В случае отсутствия разработанных моделей нарушителей безопасности информации на ОИ, в состав которых входят СВТ пользователей, требуемый класс СКЗИ для подключения к ГИС ТОР КНД, а также перечень необходимых для

реализации на стороне КНО организационно-технических мер по защите информации может быть определен КНО согласно Методике, приведенной в приложении к настоящим ЕФТТ.

Администрирование СЗИ, СКЗИ и СВТ, эксплуатируемых на стороне КНО, входящих в состав ОИ КНО (ВИС КНО), должны осуществлять сотрудники КНО, назначенные руководителем КНО.

Ответственные сотрудники КНО, назначенные руководителем КНО, должны обеспечивать соблюдение требований эксплуатационной документации на СКЗИ, применяемых на СВТ в составе ОИ КНО (ВИС КНО), в том числе организовывать необходимые мероприятия и исследования, предусмотренные эксплуатационной документацией на СКЗИ.

3.5.1. Требования к АРМ пользователей ГИС ТОР КНД для реализации защищенного взаимодействия с ГИС ТОР КНД

Для работы пользователей с ресурсами ГИС ТОР КНД могут применяться АРМ в различных исполнениях (ПЭВМ, моноблок, ноутбук), обеспечивающие возможность работы пользователей через веб-браузер по каналам связи сети общего пользования (Интернет), защищенных с применением программных СКЗИ.

Для реализации защищенного взаимодействия с ресурсами ГИС ТОР КНД на стороне АРМ пользователей могут применяться следующие программные СКЗИ:

СКЗИ, обеспечивающие криптографическую защиту передаваемой информации при работе пользователей с веб-ресурсами ГИС ТОР КНД в рамках установленного TLS-соединения с применением российских криптографических алгоритмов;

СКЗИ, обеспечивающие криптографическую защиту передаваемой информации при работе с ГИС ТОР КНД в рамках установленного VPN-соединения по технологии ViPNet с применением российских криптографических алгоритмов;

СКЗИ, обеспечивающие защиту передаваемой информации при работе пользователей с веб-ресурсами ГИС ТОР КНД в рамках установленного TLS-соединения с применением российских криптографических алгоритмов, должны быть совместимы с операционными системами и веб-браузерами, установленными на АРМ пользователя, а также с СКЗИ, эксплуатируемыми в составе ПОИБ ГИС ТОР КНД;

СКЗИ, обеспечивающие защиту передаваемой информации при работе пользователей с ГИС ТОР КНД в рамках установленного VPN-соединения по технологии ViPNet с применением российских криптографических алгоритмов, должны быть совместимы с операционными системами, установленными на АРМ пользователя, а также с СКЗИ, эксплуатируемыми в составе ПОИБ ГИС ТОР КНД.

В случае, если при взаимодействии АРМ пользователя с ГИС ТОР КНД предъявлены требования к обеспечению юридической значимости электронных документов согласно пункту 3.6 настоящих ЕФТТ, вместо СКЗИ допускается применение СЭП при условии соответствия СЭП требованиям к СКЗИ, приведенным в настоящем разделе, и требованиям к СЭП, приведенным в пункте 3.6 настоящих ЕФТТ.

Требования к организации защищенного подключения АРМ пользователей к ГИС ТОР КНД с применением СКЗИ, а также перечень поддерживаемых СКЗИ для установления защищенного подключения с ГИС ТОР КНД приведены в Регламенте подключения к защищенной сети государственной информационной системы «Типовое облачное решение по автоматизации контрольной (надзорной) деятельности» (актуальные редакции размещаются на портале ГИС ТОР КНД по адресу https://knd.gov.ru в разделе Документы / Подключение к ГИС ТОР КНД)

В случае наличия подключения АРМ пользователей к эксплуатируемой на стороне КНО защищенной сети, реализованной на базе технологии ViPNet с применением программно-аппаратных комплексов «ViPNet Coordinator», требований по обязательному применению СКЗИ на АРМ пользователей не предъявляется.

3.5.2. Требования к мобильным устройствам пользователей для реализации защищенного взаимодействия с ГИС ТОР КНД

Для работы с ресурсами ГИС ТОР КНД через специально разработанное приложение «МП Инспектор» могут применяться мобильные устройства на базе смартфонов или планшетных ПК.

Доступ пользователей (сотрудников КНО) к ресурсам ГИС ТОР КНД с применением мобильных устройств (смартфоны, планшетные ПК) может осуществляться по беспроводным каналам связи, подключенным к сети связи общего пользования (Интернет) только при совместном использовании мобильного приложения МП «Инспектор» с программным СКЗИ, установленным на мобильном устройстве.

Для обеспечения криптографической защиты информации между мобильным устройством и ГИС ТОР КНД, на стороне мобильного устройства должны применяться программные СКЗИ, совместимые с операционной системой мобильного устройства и мобильным приложением МП «Инспектор».

При организации доступа пользователей к ресурсам ГИС ТОР КНД с применением мобильных устройств на стороне КНО должны быть выполнены следующие организационно-технические меры защиты информации:

– обеспечение информационного взаимодействия мобильных устройств с ресурсами ГИС ТОР КНД только через мобильное приложение МП «Инспектор»;

– предоставление услуг связи для подключения мобильных устройств к ресурсам ГИС ТОР КНД по беспроводным каналам связи, подключенным к сети связи общего пользования (Интернет), должно осуществляться КНО на основании заключенных договоров между КНО и операторами подвижной радиотелефонной связи (юридическими лицами или индивидуальными предпринимателями, зарегистрированными на территории Российской Федерации, оказывающими услуги связи на основании соответствующей лицензии в соответствии с Федеральным законом от 07.07.2003 № 126-ФЗ «О связи»);

– соблюдение требований, приведенных в эксплуатационной документации на СКЗИ (формуляр, правила пользования и т.п.);

– запрет применения для доступа к ресурсам ГИС ТОР КНД личных

мобильных устройств пользователей (сотрудников КНО);

– организация хранения мобильных устройств в нерабочее время только в опечатываемых сейфах/шкафах с протоколированием процедур вскрытия/опечатывания в соответствующем журнале;

– при использовании мобильного устройства за пределами контролируемой зоны ОИ КНО (ВИС КНО) сотрудник КНО обязан обеспечивать сохранность мобильного устройства, не допускать оставление мобильного устройства без контроля или использование мобильного устройства другими лицами.

Требования к организации защищенного подключения мобильных устройств пользователей к ГИС ТОР КНД с применением СКЗИ, а также перечень поддерживаемых СКЗИ для установления защищенного подключения мобильных устройств с ГИС ТОР КНД приведены в Регламенте подключения к защищенной сети государственной информационной системы «Типовое облачное решение по автоматизации контрольной (надзорной) деятельности» (актуальные редакции размещаются на портале по адресу https://knd.gov.ru)

3.6. Требования по обеспечению юридической значимости электронных документов передаваемых между АРМ пользователей ГИС ТОР КНД и ГИС ТОР КНД

В случае установленных требований по обеспечению юридической значимости электронных документов (данных), передаваемых пользователями КНО в ГИС ТОР КНД, или при наличии требований по реализации юридически значимого электронного документооборота в рамках утвержденных технологических процессов обработки информации между КНО и оператором ГИС ТОР КНД на стороне АРМ пользователей должна применяться усиленная квалифицированная электронная подпись (далее – УКЭП) и средства электронной подписи (далее – СЭП) в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи».

На АРМ пользователей должны применяться СЭП, удовлетворяющие требованиям приказа ФСБ России от 27.12.2011 № 796 «Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра», обеспечивающие реализацию следующих возможностей:

– создание и проверка электронной подписи с применением российских криптографических алгоритмов ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012;

– возможность создания отсоединенной электронной подписи для файлов (данных) в формате XMLdsig и CMS;

– совместимость с применяемыми на стороне АРМ пользователей версиями ОС и браузеров;

– возможность вызова процедуры создания/проверки электронной подписи из браузера на АРМ;

– совместимость с применяемыми СКЗИ/СЭП на стороне ГИС ТОР КНД (в части проверки УКЭП).

На АРМ пользователей допускается применение СЭП, реализованных в виде программного обеспечения или программно-аппаратных комплексов. Допускается использование в качестве СЭП функциональных ключевых носителей, обеспечивающих возможность хранения ключей электронной подписи и сертификатов УКЭП и соответствующих требованиям к СЭП, перечисленным в настоящем разделе ЕФТТ.

Требуемый класс СЭП для применения на стороне АРМ пользователей определяется КНО на основании разработанной модели нарушителя безопасности информации.

В случае отсутствия разработанных моделей нарушителей безопасности информации требуемый класс СЭП, а также перечень необходимых для реализации на стороне КНО организационно-технических мер по защите информации может быть определен КНО согласно Методике, приведенной в приложении к настоящим ЕФТТ.

Администрирование СЗИ, СКЗИ/СЭП и СВТ, эксплуатируемых на стороне АРМ, входящих в состав ОИ КНО (ВИС КНО), должны осуществлять сотрудники КНО, назначенные руководителем КНО.

Ответственные сотрудники КНО, назначенные руководителем КНО, должны обеспечивать соблюдение требований эксплуатационной документации на СКЗИ/СЭП, применяемых на АРМ в составе ОИ КНО (ВИС КНО), в том числе организовывать необходимые мероприятия и исследования, предусмотренные эксплуатационной документацией на СКЗИ/СЭП.

4. Требования к реализации мероприятий

4.1. Требования по разработке независимо-компилируемых программных модулей (плагинов), динамически подключаемых к ГИС ТОР КНД

Под плагинами, динамически подключаемыми к ГИС ТОР КНД, понимаются независимо-компилируемые модули, дополняющие функциональность ГИС ТОР КНД, выполненные в виде образов Docker- контейнеров.

При разработке технического задания на разработку плагинов требуется удостовериться, что функциональность планируемого к разработке плагина не предусмотрена в ГИС ТОР КНД. Это должно быть выполнено при проведении согласования тематики доработки и функционала плагина с Минцифры России на предмет дублирования функционала.

4.1.1. Требования к патентной чистоте

При разработке должны использоваться только такие объекты интеллектуальной собственности, права на которые приобретены (получены) и используются без нарушений прав на интеллектуальную собственность третьих лиц. Это требование должно обеспечивать соблюдение авторских, смежных, патентных и иных прав.

4.1.2. Требования по размещению в Национальном фонде алгоритмов и программ

Разработанные программные модули (плагины) передаются в Национальный фонд алгоритмов и программ (далее – НФАП) в соответствии с установленным порядком (см. Методические указания о порядке формирования и использования информационного ресурса национального фонда алгоритмов и программ для электронных вычислительных машин, утвержденные приказом Министерства связи и массовых коммуникаций Российской Федерации от 16.09.2013 № 248).

Также необходимо осуществить передачу разработанных модулей в репозиторий Минцифры России с подтверждением соответствующими актами (формы и перечень документов предоставляются Минцифры России) совместимости с ГИС ТОР КНД.

Исходные коды разработанных модулей выкладываются в НФАП в составе:

- исходного кода программного модуля (плагина);
- сторонних библиотек, используемых при разработке и функционировании программного модуля;
- исполняемых файлов (где применимо).

Исходные коды должны быть переданы в НФАП полном объеме.

4.1.3. Общие требования к программным модулям

При разработке программных модулей (плагинов) используемые архитектурные решения не должны нарушать функциональность и работу ГИС ТОР КНД и должны основываться на принципах масштабируемости и отказоустойчивости.

Программный модуль должен быть разработан на языке Java, JavaScript, Python, Ruby on Rails и производных.

В комплекте программного модуля должна поставляться программная документация согласно ГОСТ серии 34 (Стандарты информационной технологии, РД50-34.698-90) и серии 19 (Единая система программной документации). Порядок создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации программных модулей (плагинов), подключаемых к ГИС ТОР КНД, должен соответствовать требованиям постановления Правительства Российской Федерации от 06.07.2015 № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации».

При закупке стороннего лицензионного программного обеспечения для реализации программных модулей (плагинов) необходимо отдавать приоритет программному обеспечению российского производства либо программному обеспечению на основе открытых исходных кодов (open-source, лицензия GLU/GPL, Apache License 2.0).

Программные модули не должны исключать возможность масштабирования по производительности и объему обрабатываемой информации без модификации ее программного обеспечения путем модернизации используемого комплекса технических средств. Программный модуль (плагин) должен создаваться в парадигме сервисно-ориентированной архитектуры, реализовывать публичное API в соответствии со спецификацией OpenAPI 3.0.

Программный модуль не должен накладывать ограничения на возможность горизонтального масштабирования, т.е. должен позволять работать нескольким экземплярам в одном пространстве данных.

Программные модули должны поддерживать процедуры мониторинга и предоставлять информацию о текущем состоянии своих процессов.

Модель здоровья программного модуля должна быть согласована со стороны Минцифры России. Программные модули должны поддерживать балансировку нагрузки без необходимости в привязке клиентов к экземплярам сервиса и быть безсессионными.

Сервис должен поддерживать процедуры идентификации и аутентификации с использованием токена ЕСИА в рамках технологии OAuth2, при условии необходимости аутентификации при использовании сервиса.

Программные модули должны собираться по технологии Maven или NPM. Результатом сборки должен являться образ Docker-контейнера. При сборке модуля должно происходить комплексное автоматическое юнит-тестирование.

4.1.4. Назначение независимо-компилируемых программных модулей (плагинов)

В рамках исполнения требований данного ЕФТТ субъекты – получатели субсидий могут принять участие в разработке дополнительных внешних региональных модулей (плагинов), расширяющих функциональность ГИС ТОР КНД, в части автоматизации исполнения контрольно-надзорных функций. Каждый

субъект должен провести анализ процессов, требующих дополнительной автоматизации, имеющих узкую специфику для данного субъекта и не реализованную в ГИС ТОР КНД. Примером таких модулей могут быть:

1. Модули, реализующие специальные алгоритмы сбора и/или обработки данных позволяющие эффективно использовать результаты создания реестра субъектов и объектов при выявлении межотраслевых связей и для последующего расчета риск-ориентированных показателей с учетом их взаимовлияния. Типовые требования к структуре межотраслевых реестров субъектов и объектов, а также их наполнению приведены на портале knd.gov.ru в разделе «Документы / Субсидия из федерального бюджета» (актуализация требований не позднее 01.03.2021).

2. Реализации моделей расчетов, например:

2.1. Управление критериями (факторами) расчета ожидаемого ущерба охраняемым ценностям, применяемыми в конкретном КНО.

2.2. Оценки ожидаемого ущерба охраняемым ценностям, основанные на экспертизе конкретного КНО на основе статистических данных.

2.3. Оценки ожидаемого ущерба охраняемым ценностям, основанные на автоматическом выявления зависимостей в наборе критериев (факторов) риска с использованием методов многофакторного анализа или машинного обучения на основе исторических данных о результатах проверок.

3. Управление пользовательскими интерфейсами ввода данных в ГИС ТОР КНД, например, заполнения чек-листов и формирования отчетов, характерных для сложившейся практики КНД в конкретном КНО.

4. Интеграции с внешними по отношению к ГИС ТОР КНД информационными системами, используемыми КНО в своей деятельности, в том числе, но не ограничиваясь:

4.1. Действующими ведомственными ИС, ИС органов государственной власти и местного самоуправления, муниципальными, региональными или ведомственными реестрами и БД НСИ, используемыми для осуществления КНД, поддержки принятия решений при КНД, формирования отчетности всех уровней по результатам КНД в соответствии с приоритетами и сложившейся практикой конкретного КНО.

4.2. Действующими ИС поднадзорных лиц.

4.3. Поставщиками данных объективного контроля – средствами удаленной фиксации состояния объектов (датчиками) и агрегаторами данных с них.

4.4. Системами взаимодействия с гражданами и организациями, в том числе, но не ограничиваясь:

4.4.1. Информационными системами «Открытого правительства» всех уровней.

4.4.2. Информационными системами по приему, обработке и анализу обращений граждан.

Данный перечень не является строго обязательным для субъекта, а носит рекомендательный характер, субъект может самостоятельно определять целевое назначение разрабатываемых модулей. В первую очередь рекомендуется разрабатывать модули, использование которых возможно несколькими регионами.

В целях избегания финансирования реализации однотипного функционала, тематики доработки и функционала плагина должны согласовываться с Минцифры России. Данные требования в процессе согласования могут быть изменены для обеспечения покрытия требований нескольких потребителей.

4.1.5. Требования по обеспечению информационной безопасности

В части требований по обеспечению информационной безопасности при интеграции с ГИС ТОР КНД руководствоваться положениями, приведенными в разделе 3 настоящих ЕФТТ.

4.1.6. Требования к эргономике и общедоступности

Взаимодействие пользователей с прикладным программным обеспечением, входящим в состав модуля, должно осуществляться посредством визуального графического интерфейса (GUI).

Все надписи экранных форм, а также сообщения, выдаваемые пользователю (кроме системных сообщений), должны быть на русском языке.

Программные модули должны обеспечивать корректную обработку аварийных ситуаций, вызванных неверными действиями пользователей, неверным форматом или недопустимыми значениями входных данных. В указанных случаях система должна выдавать пользователю соответствующие сообщения, после чего возвращаться в рабочее состояние, предшествовавшее неверной (недопустимой) команде или некорректному вводу данных.

Дополнительные экранные формы должны проектироваться с учетом требований унификации:

− все экранные формы пользовательского интерфейса должны быть выполнены в едином графическом дизайне, с одинаковым расположением основных элементов управления и навигации;

− для обозначения сходных операций должны использоваться сходные графические значки, кнопки и другие управляющие (навигационные) элементы. Термины, используемые для обозначения типовых операций (добавление информационной сущности, редактирование поля данных), а также последовательности действий пользователя при их выполнении, должны быть унифицированы;

− внешнее поведение сходных элементов интерфейса (реакция на наведение указателя «мыши», переключение фокуса, нажатие кнопки) должны реализовываться одинаково для однотипных элементов.

При разработке программных модулей дополнительно к основным требованиям к интерфейсу могут быть применены следующие требования:

− экранные формы пользовательского интерфейса должны быть настроены с использованием репозитория элементов веб-дизайна «Единого портала государственных и муниципальных услуг (функций)».

При выполнении работ следует руководствоваться Методическими рекомендациями по совершенствованию пользовательских интерфейсов, утвержденными приказом Минкомсвязи России от 16.10.2015 № 405, и Методическими рекомендациями по информированию граждан о преимуществах

получения государственных и муниципальных услуг в электронной форме, утвержденными протоколом заседания подкомиссии по использованию информационных технологий при предоставлении государственных и муниципальных услуг Правительственной комиссии по использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности от 14.10.2015 № 406пр.

4.2. Требования по доработке существующих региональных ВИС КНО с целью интеграции с государственными информационными системами в сфере государственного контроля (надзора)

В рамках создания ЕИС КНД рекомендуется интегрировать региональные ВИС КНО с ГИС ТОР КНД, ФГИС ЕРП, ФГИС ЕРКНМ в целях автоматизации процессов передачи данных о проверяемых субъектах, проверяемых объектах, данных о проверках в отношении указанных лиц. Интеграция может осуществляться как с одной из перечисленных ГИС, так и с несколькими. Интеграция с ФГИС ЕРП должна быть осуществлена по актуальным видам сведений СМЭВ «Размещение сведений в реестре электронных паспортов контрольно-надзорных мероприятий» версии не ниже 3.0.3 и при необходимости «Сведения из электронных паспортов контрольно-надзорных мероприятий» версии не ниже 1.0.0. Интеграция с ФГИС ЕРКНМ должна быть осуществлена по актуальным видам сведений СМЭВ «Размещение сведений в едином реестре контрольных (надзорных) мероприятий» версии не ниже 6.0.2 и при необходимости «Сведения из электронных паспортов контрольно-надзорных мероприятий» версии не ниже 3.0.1.Актуальные версии видов сведений необходимо уточнить на технологическом портале СМЭВ (https://smev3.gosuslugi.ru/portal/)..

Решение по интеграции ВИС КНО принимается уполномоченными лицами субъекта Российской Федерации.

Спецификация программных интерфейсов взаимодействия с ГИС ТОР КНД и описание единой модели данных ГИС ТОР КНД, в соответствии с которой формируются получаемые из ГИС ТОР КНД (или передаваемые в ГИС ТОР КНД) сведения, размещены на портале knd.gov.ru в разделе «Документы / Субсидия из федерального бюджета» (актуализация документа не позднее 01.03.2021).

В части требований к защите информации при интеграции с ГИС ТОР КНД руководствоваться положениями раздела 3 настоящих ЕФТТ, при интеграции с ФГИС ЕРП и (или) ФГИС ЕРКНМ руководствоваться требованиями к защите информации СМЭВ 3.х и Оператора ФГИС ЕРП, ФГИС ЕРКНМ.

4.3. Требования к автоматизированным рабочим местам ГИС ТОР КНД, в том числе переносным, для обеспечения работы в ГИС ТОР КНД или ВИС КНО

При автоматизации КНД каждый сотрудник КНО должен быть обеспечен автоматизированным рабочим местом (далее – АРМ). При проведении контрольно-надзорных мероприятий выделяют три типа рабочих мест:

- Стационарный АРМ;
- Переносной АРМ;
- Мобильный АРМ (смартфон или планшетный ПК).

Требования, предъявляемые к техническим характеристикам АРМ, определяются исходя из требований технической документации информационной системы, на базе которой осуществлена (осуществляется) автоматизация КНД по конкретному виду контроля (надзора) и типа АРМ.

При подключении АРМ к ГИС ТОР КНД необходимо обеспечить соответствие требованиям по защите информации, приведенным в подпункте 3.5.1 пункта 3.5 настоящих ЕФТТ.

Приведенные ниже рекомендации для АРМ устанавливают минимальный порог технических требований, который может быть изменен в сторону повышения на основании запроса КНО, в интересах которого осуществляется закупка.

АРМ должны поддерживать операционные системы из перечня:

- Linux OS;
- Microsoft Windows (версии 8.1, 10);
- Android (для мобильного АРМ);
- Aurora (для мобильного АРМ).

На АРМ должен быть установлен минимум один браузер из перечня:

- Google Chrome,
- Yandex Browser,
- Mozilla Firefox,
- Opera,
- Safari,
- Edge.

Минимальные требования для стационарных АРМ:

Размер и разрешение экрана 19”	1600x900
Тип и частота процессора:	2.0 ГГц
Тип и объем оперативной памяти	DDR3 4 Гб
Тип и объем дисков	SATA 512 Гб

Минимальные требования для переносных АРМ:

Размер и разрешение экрана 14”	1920x1080
Тип и частота процессора:	2.0 ГГц
Тип и объем оперативной памяти	DDR3 4 Гб
Объем дисков	256 Гб

АРМ пользователей должны иметь возможность подключения и доступа к ГИС ТОР КНД посредством авторизации через ЕСИА.

Стационарный АРМ пользователя должен иметь возможность подключения к многофункциональному устройству, обеспечивающему печать и сканирование документов.

При выборе АРМ должны учитываться требования по защите информации, приведенные в подпункте 3.5.1 пункта 3.5 настоящих ЕФТТ.

Для обеспечения работы существующей ВИС КНО или ГИС ТОР КНД допустимо использование оборудования, уже эксплуатируемого в составе действующей инфраструктуры субъекта Российской Федерации.

Минимальные требования для мобильных АРМ:

Общие технические параметры устройства на Android (не менее):

Размер экрана (смартфон / планшет)	8-10,4 дюйм
Размер экрана (смартфон)	4-7 дюйм
Объем оперативной памяти	3 Гб
Объем стационарной памяти	32 Гб
Разрешение экрана не менее	1920*1080
Поддерживаемые сети	3G, 4G, LTE, WiFi
Возможность установки microSD карт памяти	да
Объемом карты памяти не менее	64 Гб
Наличие и поддержка систем геопозиционирования (GPS, GPS-A, ГЛОНАСС)	да
Разрешение основной камеры	от 8 МП.

Общие технические параметры устройства на Aurora (не менее):

Размер экрана (смартфон / планшет)	8-10,4 дюйм
Размер экрана (смартфон)	4-7 дюйм
Объем оперативной памяти	не менее 2 Гб
Объем стационарной памяти	не менее 16 Гб
Разрешение экрана	1920*1080
Поддерживаемые сети	3G, 4G, LTE, WiFi
Возможность установки microSD карт памяти	да
Объемом карты памяти не менее	64 Гб
Наличие и поддержка систем геопозиционирования (GPS-A, ГЛОНАСС)	да
Разрешение основной камеры	от 5 МП.

На мобильные АРМ (смартфоны или планшетные ПК) должны быть предустановлены:

а) для конфигурации мобильных АРМ с ОС Android:

- операционная система Android 7.x, 8.x. и другие версии;
- набор программного обеспечения для работы с типами файлов содержащих текстовую, числовую и графическую информацию (офисное программное обеспечение) и СКЗИ, обеспечивающие криптографически защищенное VPN/TLS-соединение между мобильным устройством и серверной частью ГИС ТОР КНД, удовлетворяющее требованиям в подпункта 3.5.2 пункта 3.5 настоящих ЕФТТ;

б) для конфигурации мобильных АРМ с ОС Аврора (SailfishOS):

- операционная система Aurora (SailfishOS), набор программного обеспечения для работы с типами файлов содержащих текстовую, числовую и графическую информацию (офисное программное обеспечение) и встроенный в мобильное приложение МП «Инспектор» СКЗИ, обеспечивающее криптографически защищенное VPN/TLS-соединение между мобильным

приложением «МП Инспектор» и серверной частью ГИС ТОР КНД, удовлетворяющее требованиям подпункта 3.5.2 пункта 3.5 настоящих ЕФТТ.

При выборе мобильных АРМ должны учитываться требования по защите информации, приведенные в подпункте 3.5.2 пункта 3.5 настоящих ЕФТТ.

Используемые мобильные АРМ должны обладать ресурсом аккумуляторов, которые обеспечивает работу на протяжении всего времени проведения проверки (не менее 8 часов в день в смешанном режиме).

Также при закупке мобильных АРМ, при необходимости, рекомендуется в том числе учитывать климатические условия фактической эксплуатации и потребности КНО в части применения мобильных АРМ в рамках организации и осуществления КНД.

В качестве дополнительных требований к мобильным АРМ могут предъявляться (при условии необходимости и обоснованности закупки):

Объем карты памяти не менее	256 Гб
Разъем POGO-Pin: 14 pin, USB, UART TTL, питание 5В, ток не меньше 1А, 5В, зарядка, размещение на задней стороне устройства	да
Диапазон рабочих температур	-20 ~ +60 °С
Аккумулятор: съемный, морозостойкий	от 26,6 Втч
Класс защиты	от IP 67
Корпус устройства: ударопрочный пластик и наличие демпфирующих бамперов на углах устройства	да
Разрешение фронтальной камеры	от 5 МП.

Также в состав программно-технического комплекса может входить мобильный принтер для мобильных и переносных АРМ.

Все закупаемое оборудование должно обладать гарантийным сроком эксплуатации не менее 3-х лет.

При закупках лицензий необходимо исполнять требования по импортозамещению, где это применимо.

При определении количества закупаемого оборудования рекомендуется учитывать необходимость наличия подменного фонда на случай утери, поломки, выхода из строя устройств в размере не более 5% от закупаемых устройств.

4.4. Требования к закупаемым средствам удаленной фиксации состояний объектов контроля (надзора)

При осуществлении контрольно-надзорной деятельности КНО может задействовать средства удаленной фиксации состояний объектов контроля (далее – устройства) в целях сбора данных и использования их для проведения аудита и планирования контрольно-надзорных мероприятий и дистанционного контроля в отношении указанных объектов.

В рамках реализации данного мероприятия могут быть приобретены устройства и предусмотрены работы и (или) услуги по сборке, монтажу, установке, подключению и настройке устройств, включая технические средства и программное обеспечение связи и организации (или подключения к) сети передачи

данных, а также приобретены и (или) созданы программно-аппаратные комплексы (далее — ПАК) для удаленной фиксации и управления состоянием объектов контроля (надзора), включающие устройства, и предусмотрены работы и (или) услуги по предпроектному обследованию объектов контроля в целях установки устройств, проектированию, сборке, настройке, монтажу, установке, подключению ПАК, ознакомлению или обучению специалистов КНО, интеграции с ВИС КНО и/или с ИС ПСД, сервисами, реестрами, базами данных, иным программным обеспечением.

К сбору, передаче и использованию сведений от средств удаленной фиксации предъявляются следующие типовые требования:

- обеспечена возможность автоматизировано получать данные с датчиков устройств (средств удаленной фиксации) в машиночитаемом формате через аппаратный интерфейс устройств, в том числе с применением контроллеров, обеспечивающих передачу данных по сети передачи данных, а также через программный интерфейс (API) устройства или связанного с ним сервиса при наличии;

- в составе документации к устройству должна быть спецификация датчиков, включающая:

описание режимов их работы;

описание структуры формируемых устройством пакетов данных;

способы подключения устройства к сети передачи данных;

описание способов и протоколов настройки режимов работы устройства вручную и/или через удаленное подключение;

описание протоколов передачи информации с указанием способа организации информационного обмена (данные направляются в удаленное соединение или предоставляется сервис для подключения для запроса или приема данных);

- устройства должны предоставлять данные с датчиков с устанавливаемой периодичностью;

- устройства должны синхронизироваться со службами глобального времени самостоятельно или требовать такой синхронизации от подключаемых сервисов сбора данных;

- устройства должны быть оснащены часами реального времени;

- все передаваемые данные с датчиков должны снабжаться обязательной временной отметкой;

- обеспечена возможность чтения информации с датчиков в режиме, близкому к реальному времени, скорость получения информации может зависеть от рассматриваемой области применения;

- опционально для обеспечения достоверности данных от датчиков устройство должно:

  - периодически или в составе пакета данных от датчиков предоставлять данные о напряжении питания;
  - быть оснащено датчиком открытия корпуса или опломбировано после установки;

- при оснащении устройства датчиком открытия корпуса, данные с него должны включаться в состав общего пакета данных с датчиков;
- содержать датчики контроля кражи устройства и передачи данных от них в составе пакетов от датчиков или в отдельных пакетах. К таким датчикам относятся: GPS/ГЛОНАСС датчик, Акселерометр и иные датчики позволяющие сделать вывод о перемещении устройства из места установки;

- автономные устройства должны обеспечивать бесперебойную работу в течение заявленных сроков эксплуатации.

Перечень устройств, требуемые технические характеристики, состав передаваемых данных и протоколы информационного обмена устанавливаются локальными стандартами (системой стандартов) и регламентами, определяющими порядок оказания соответствующих услуг по мониторингу объектов.

Пример перечня требований к датчикам приведен на портале knd.gov.ru в разделе «Документы / Субсидия из федерального бюджета».

Для передачи телеметрических данных в ИС ПСД могут быть использованы следующие протоколы:

- MQTT (англ. *message queuing telemetry transport*) — упрощенный сетевой протокол, работающий поверх TCP/IP, ориентированный для обмена сообщениями между устройствами по принципу издатель-подписчик. MQTT является также, как и HTTP, транспортным протоколом, что означает, что для настройки информационного обмена используется определенная спецификация;

- HTTP(S) (англ. *HyperText Transfer Protocol)* — «протокол передачи гипертекста») — протокол прикладного уровня передачи данных, время используется для передачи произвольных данных, является транспортным протоколом, что означает, что для настройки информационного обмена используется определенная спецификация.

Для подключения средств удаленной фиксации могут использоваться различные технологии, принятые в сфере деятельности, в которой ведется мониторинг объектов и передача данных, например, но не ограничиваясь:

- NB-IoT (Narrow Band Internet of Things) – стандарт сотовой связи для устройств телеметрии с низкими объемами обмена данными;

- LoRa/LoRaWAN – технология беспроводной связи, предназначена для организации низкоскоростного обмена данными недорогих батарейных устройств на относительно большие расстояния;

- GSM (2G/3G/LTE) – стандарт сотовой связи разных поколений;

- Широкополосный доступ в Интернет.

В рамках реализации мероприятия должна быть обеспечена передача информации, получаемой от устройств, для использования в ИС ПСД или ВИС КНО для планирования и проведения контрольных (надзорных) мероприятий и иных мероприятий.

При сопряжении с ВИС КНО (ГИС ТОР КНД) КНО субъекта Российской Федерации допустимо использовать только протоколы и стандарты, не являющиеся уникальной разработкой производителя датчиков.

Возможные типы применяемых устройств:

– сенсорные устройства (термопары и температурные датчики, датчики влажности, датчики давления, Акселерометры, датчики вибрации, газоанализаторы, датчики тока и на эффекте Холла, фотоэлектрические датчики, датчики PIR, активные датчики, датчики MEMS и др.);

– интеллектуальные оконечные точки IIoT;

– исполнительные устройства и устройства вывода информации;

– устройства ввода информации (извещатели);

– источники энергии и устройства управления электропитанием;

– устройства подключения или организации сети передачи данных, включая базовые станции радиосети и соответствующее программное обеспечения для диспетчеризации и сбора данных.

Итоговые требования к работам и (или) услугам по проектированию, монтажу, инсталляции и настройке устройств и (или) приобретение и (или) созданию программно-аппаратного комплекса устанавливаются уполномоченными лицами субъекта Российской Федерации исходя из целей и задач автоматизации КНД.

4.5. Требования по внедрению ГИС ТОР КНД

4.5.1. Требования по организации обучения с целью создания центра компетенции по направлению «Автоматизация контрольной (надзорной) деятельности»

В целях повышения эффективности мероприятий по автоматизации КНД в субъектах Российской Федерации целесообразно организовать обучение заинтересованных лиц, деятельность которых сопряжена с реализацией контрольно-надзорных функций, с целью создания центра компетенции по направлению «Автоматизация контрольной (надзорной) деятельности». Обучение проводится по типовой программе, которая может быть адаптирована под специфику конкретного региона, на базе специализированных учебных центров субъекта Российской Федерации либо иных организаций, обладающих компетенциями по обучению в указанном направлении. Компетентность обозначенных организаций устанавливается на основании таких критериев, как наличие лицензий на ведение образовательной деятельности по требуемому направлению, и\или, наличия практического опыта проведения соответствующих образовательных мероприятий (семинары, конференции и т.д.), подтвержденного документально (отзывы, благодарственные письма, отчеты о проведении и т.д.).

Также мероприятия по указанному направлению обучения могут включать:

− организацию круглых столов/рабочих групп по обсуждению проблем автоматизации КНД, целей и задачах по развитию КНД, обсуждение конкретных текущих проблем и возможных способов их решения;

− организацию семинаров по порядку и методологии сбора данных для настройки процессов КНД в ГИС ТОР КНД, включая разработку показателей отчетности.

В результате реализации мероприятия сотрудниками КНО и иными уполномоченными лицами субъекта Российской Федерации должны быть приобретены компетенции по:

− разработке спецификаций, включающих общие сведения о виде контроля и контрольной функции, сведения об оргструктуре КНО, сведения о текущей практике осуществления контроля (надзора) и предложения по интеграции, для настройки реестров и справочников для КНО, осуществляющих контрольно-надзорную деятельность. Перечень вопросов предлагаемой спецификации, а также форма описания бизнес-процессов приведены на портале (Цифровой стандарт КНД) knd.gov.ru в разделе «Документы / Субсидия из федерального бюджета»;

− анализу процессов контрольно-надзорной деятельности КНО для настройки реестров и справочников в ГИС ТОР КНД и формирования перечня показателей отчетности;

− формированию направлений совершенствования организационно-управленческой среды реализации КНД в субъекте Российской Федерации, включающих:

разработку рекомендаций по доработке нормативно-правовой и регламентной базы в субъекте Российской Федерации по конкретному виду КНД;

разработку рекомендаций по реструктуризации организационных структур КНО в соответствии с действующим законодательством всех уровней;

проектирование и описание процессов КНД КНО в формализованном виде, построение семантических моделей процессов;

разработку рекомендаций по оптимизации процессов КНД в рамках КНО в рамках действующего законодательства, включая анализ форм отчетности, выделение показателей: справочных, базовых и расчетных, дедупликации показателей, разработки СИМ объектов отчетности в объеме, необходимом для сбора данной отчетности;

− работе с данными, включающей в себя: проверку качества данных (проверки на непротиворечивость, полноту, актуальность, достоверность), анализ данных и разработку требований к динамическим моделям определения рисков (классов опасности).

Перечень компетенций может быть расширен по решению уполномоченных лиц субъекта Российской Федерации по согласованию с оператором ГИС ТОР КНД.

Перечень лиц, привлекаемых к обучению по указанному направлению, определяется уполномоченными лицами субъекта Российской Федерации.

По результатам проведения обучения и создания центра компетенций вместе с отчетными документами о расходовании средств по мероприятию необходимо предоставить копии спецификации, а также описания бизнес-процессов указанных выше по всем приоритетным видам регионального контроля (надзора), требующих автоматизации в ГИС ТОР КНД.

4.5.2. Требования по обучению администраторов настройке процессов контроля и надзора в соответствии с региональной практикой

Для реализации мероприятий по настройке процессов контроля и надзора в соответствии с регламентами КНО субъекта Российской Федерации требуется провести обучение лиц, осуществляющих администрирование ГИС ТОР КНД в КНО, и иных уполномоченных лиц настройке процессов контроля и надзора в ГИС ТОР КНД. Программы обучения указанных выше лиц должны включать разделы по одному или нескольким направлениям, перечисленным ниже:

− работа с конструктором бизнес-процессов проведения плановых и внеплановых проверок ГИСТОР КНД;

− настройка перечня показателей форм отчетности (справочных, базовых, расчетных);

− настройка семантической информационной модели объектов для формирования реестров проверяемых объектов по видам контроля;

− настройка подсистемы обеспечения информационной безопасности;

− настройка печатных форм документов;

− импорт/экспорт данных из внешних систем посредством файловых выгрузок, средствами универсальных механизмов настройки форматов загрузки -.xls, -.xml;

− работа с настройками графиков, выведенных на устройство визуализации и отчетов;

− подключение внешних хранилищ.

В результате обучения лицами, прошедшими обучение, должны быть приобретены в полном объеме либо частично (при разделении полномочий указанных лиц по участию в автоматизации КНО) следующие компетенции:

− разработка новых и(или) корректировка в ГИС ТОР КНД существующих бизнес-процессов по региональному контролю (надзору), включая работы по сбору данных для настройки бизнес-процессов;

− расширение состава семантических моделей реестров субъектов и объектов;

− корректировка или настройка новых выходных печатных и(или) отчетных форм;

− вывод дополнительной статистической информации на устройство визуализации руководителя в виде графиков, диаграмм и таблиц;

− доработка и первичное наполнение справочников;

− реализация интеграции с региональными сервисами СМЭВ 3.0 (не ниже), сведения которых необходимы для региональных видов контроля (надзора);

− настройка интеграции ГИС ТОР КНД с внешними информационными системами, встроенными механизмами для регулярного сбора информации для ее актуализации;

− настройка загрузки данных из внешних источников.

Перечень компетенций может быть расширен по решению уполномоченных лиц субъекта Российской Федерации по согласованию с оператором ГИС ТОР КНД.

4.5.3. Требования по настройке процессов контроля и надзора в соответствии с региональной практикой

Работы по настройке процессов контроля и надзора в соответствии с региональной практикой должны проводиться на локальном личном кабинете ГИС ТОР КНД и включать в себя одну или несколько работ по настройке ГИС ТОР КНД из перечисленных ниже:

− разработка новых и(или) корректировка в ГИС ТОР КНД существующих бизнес-процессов по региональному контролю (надзору), включая работы по сбору данных для настройки бизнес-процессов;

− расширение состава семантических моделей реестров субъектов и объектов;

− корректировка или настройка новых выходных печатных и(или) отчетных форм;

− вывод дополнительной статистической информации на устройство визуализации руководителя в виде графиков, диаграмм и таблиц;

− доработка и первичное наполнение справочников Системы;

− реализация интеграции с региональными сервисами СМЭВ 3.0, сведения которых необходимы для региональных видов контроля (надзора);

− настройка интеграции ГИС ТОР КНД с внешними информационными системами, встроенными механизмами для сбора информации по:

− субъектам и объектам;

− показателям эффективности и результативности;

− категориям риска и классам опасности.

− однократная загрузка данных из внешних источников в части:

− субъектов и объектов;

− обязательных требований;

− проверочных листов;

− категорий риска и классов опасности;

− паспортов и карточек проверки.

Перечень работ может быть расширен по решению уполномоченных лиц субъекта Российской Федерации по согласованию с оператором ГИС ТОР КНД.

ПРИЛОЖЕНИЕ

Методика определения класса СКЗИ/СЭП, применяемых на стороне КНО при подключении к ГИС ТОР КНД

Настоящим приложением следует руководствоваться в целях определения требуемого класса СКЗИ/СЭП в случае отсутствия моделей нарушителей безопасности информации на ОИ КНО (ВИС КНО), в состав которых входят СВТ (АРМ пользователей или мобильные устройства), с помощью которых внешние пользователи ГИС ТОР КНД (далее – пользователи, сотрудники КНО) планируют осуществлять удаленный доступ к ресурсам ГИС ТОР КНД или для ВИС КНО, которые планируют обеспечивать информационное взаимодействие с ГИС ТОР КНД по каналам связи, подключенным к сети связи общего пользования (Интернет).

Настоящее приложение разработано с учетом модели нарушителя ГИС ТОР КНД и требований нормативных документов ФСБ России:

– приказ ФСБ России от 27.12.2011. № 796 «Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра»;

– 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».

Определение требуемого класса СКЗИ/СЭП для применения на стороне ОИ КНО (ВИС КНО) при подключении к ГИС ТОР КНД должна выполнять комиссия из числа сотрудников, назначенных руководителем КНО. В состав комиссии должны входить лица, обладающие опытом работы в области информационных технологий и защиты информации и (или) прошедшие переподготовку (повышение квалификации) в области защиты информации.

В таблице приведен совокупный перечень возможностей потенциальных нарушителей по подготовке к проведению и реализации атак на СВТ пользователей, входящих в состав ОИ КНО (ВИС КНО), а также требуемые классы применяемых на стороне ОИ КНО (ВИС КНО) СКЗИ/СЭП, обеспечивающие противодействие возможностям потенциальных нарушителей безопасности информации.

Таблица – Возможности потенциальных нарушителей безопасности информации и требуемые классы СКЗИ/СЭП на стороне ОИ КНО (ВИС КНО), СВТ пользователей:

№ п/п	Возможности потенциальных нарушителей безопасности информации (для ОИ КНО, ВИС КНО, СВТ пользователей)	Требуемый класс СКЗИ/СЭП
1	Возможность самостоятельного создания способов атак, подготовки и проведения атак, без привлечения специалистов в области разработки и анализа средств криптографической защиты информации (далее – СКЗИ) и средств электронной подписи (далее – СЭП)	КС1
2	Возможность осуществления действий на различных этапах жизненного цикла СЭП и СКЗИ, в т.ч. на этапах разработки (модернизации), производства, хранения, транспортировки, ввода в эксплуатацию (пусконаладочные работы), эксплуатации	КС1
3	Возможность проведение атаки извне пространства, в пределах которого осуществляется контроль за пребыванием и действиями лиц и (или) транспортных средств (из-за пределов контролируемой зоны)	КС1
4	Возможность проведения на этапах разработки (модернизации), производства, хранения, транспортировки и ввода в эксплуатацию (пусконаладочных работ) СКЗИ/СЭП следующих атак: - внесение несанкционированных изменений в СКЗИ/СЭП и (или) в компоненты аппаратных и программных средств, совместно с которыми штатно функционируют СКЗИ/СЭП и в совокупности представляющие среду функционирования СКЗИ/СЭП (далее – СФ), которые способны повлиять на выполнение предъявляемых к СКЗИ/СЭП требований, в том числе с использованием вредоносных программ; - внесение несанкционированных изменений в документацию на СКЗИ/СЭП и на компоненты СФ	КС1
5	Возможность проведения атак на этапе эксплуатации СКЗИ/СЭП на следующие объекты защиты: - документация на СКЗИ/СЭП и на компоненты СФ; - защищаемые электронные документы (защищаемую информацию); - ключевая, аутентифицирующая и парольная информация СКЗИ/СЭП; - СКЗИ/СЭП и его программные и аппаратные компоненты; - аппаратные средства, входящие в СФ, включая микросхемы с записанным микрокодом BIOS, осуществляющей	КС1

№ п/п	Возможности потенциальных нарушителей безопасности информации (для ОИ КНО, ВИС КНО, СВТ пользователей)	Требуемый класс СКЗИ/СЭП
	инициализацию этих средств (далее – аппаратные компоненты СФ); - программные компоненты СФ, включая программное обеспечение BIOS; - данные, передаваемые по каналам связи; - помещения, в которых находится совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем (далее – СВТ), на которых реализованы СКЗИ/СЭП и СФ	
6	Возможность получения из находящихся в свободном доступе источников, включая информационно-телекоммуникационные сети, доступ к которым не ограничен определенным кругом лиц, следующей информации: - общие сведения об информационной системе, в которой используется СКЗИ/СЭП (назначение, состав, оператор, объекты, в которых размещены ресурсы информационной системы); - сведения об информационных технологиях, базах данных, аппаратных средствах, ПО, используемых в информационной системе совместно с СКЗИ/СЭП, за исключением сведений, содержащихся только в конструкторской документации на информационные технологии, базы данных, аппаратные средства, ПО, используемые в информационной системе совместно с СКЗИ/СЭП; - содержание конструкторской документации на СКЗИ/СЭП; - сведения о физических мерах защиты объектов, в которых размещены СКЗИ/СЭП; - сведения о мерах по обеспечению контролируемой зоны объектов информационной системы, в которой используются СКЗИ/СЭП; - сведения о мерах по разграничению доступа в помещения, в которых находятся СВТ, на которых реализованы СКЗИ/СЭП и СФ; - содержание находящейся в свободном доступе документации на аппаратные и программные компоненты СКЗИ/СЭП и СФ; - общие сведения о защищаемой информации, используемой в процессе эксплуатации СКЗИ/СЭП; - все возможные данные, передаваемые в открытом виде по каналам связи, не защищенным от несанкционированного	КС1

№ п/п	Возможности потенциальных нарушителей безопасности информации (для ОИ КНО, ВИС КНО, СВТ пользователей)	Требуемый класс СКЗИ/СЭП
	доступа к информации организационно-техническими мерами; - сведения о каналах связи, по которым передается защищаемая СКЗИ/СЭП информация; - сведения обо всех проявляющихся в каналах связи, не защищенных от несанкционированного доступа к информации организационно-техническими мерами и техническими мерами, нарушениях правил эксплуатации СКЗИ/СЭП и СФ, неисправностях и сбоях аппаратных компонентов СКЗИ/СЭП и СФ; - сведения, получаемые в результате анализа любых сигналов от аппаратных компонентов СКЗИ/СЭП и СФ, которые может перехватить нарушитель	
7	Возможность использования: - находящихся в свободном доступе или используемых за пределами контролируемой зоны аппаратных средств и ПО, включая аппаратные и программные компоненты СКЗИ/СЭП и СФ; - специально разработанных аппаратных средств и ПО	КС1
8	Возможность использования на этапе эксплуатации в качестве каналов атаки (среды переноса от субъекта к объекту, от объекта к субъекту) действий, осуществляемых при подготовке и (или) проведении атаки: - каналов связи, не защищенных от несанкционированного доступа к информации организационно-техническими мерами (как вне контролируемой зоны, так и в ее пределах), по которым передается защищаемая СКЗИ/СЭП информация; - каналов распространения сигналов, сопровождающих функционирование СКЗИ/СЭП и СФ	КС1
9	Возможность проведения атак из информационно-телекоммуникационных сетей, доступ к которым не ограничен определенным кругом лиц	КС2
10	Возможность использования на этапе эксплуатации аппаратных средств и ПО из состава средств информационной системы, используемых на местах эксплуатации СКЗИ/СЭП (далее – штатные средства) и находящихся за пределами контролируемой зоны	КС2
11	Возможность проведения атаки при нахождении как вне пределов, так и в пределах контролируемой зоны	КС2
12	Возможность получения в рамках предоставленных полномочий, а также в результате наблюдений следующей	КС2

№ п/п	Возможности потенциальных нарушителей безопасности информации (для ОИ КНО, ВИС КНО, СВТ пользователей)	Требуемый класс СКЗИ/СЭП
	информации: - сведения о физических мерах защиты объектов, в которых размещены ресурсы информационной системы; - сведения о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы информационной системы; - сведения о мерах по разграничению доступа в помещения, в которых находятся СВТ, на которых реализованы СКЗИ/СЭП и СФ	
13	Возможность использования штатных средств, ограниченная мерами, реализованными в информационной системе, в которой используются СКЗИ/СЭП, и направленными на предотвращение и пресечение несанкционированных действий	КС2
14	Возможность физического доступа к СВТ, на которых реализованы СКЗИ/СЭП и СФ	КС3
15	Возможность располагать аппаратными компонентами СКЗИ/СЭП, ограниченная мерами, реализованными в информационной системе, в которой используется СКЗИ/СЭП, и направленными на предотвращение и пресечение несанкционированных действий	КС3

Определение требуемого класса СКЗИ/СЭП для применения на стороне ОИ КНО (ВИС КНО) и СВТ пользователей (сотрудников КНО), входящих в состав ОИ КНО (ВИС КНО), осуществляют ответственные лица, назначенные руководителем КНО, на основании экспертного анализа совокупности приведенных в пунктах 1–15 таблицы возможностей потенциальных нарушителей безопасности информации.

В случае, если для подготовки и проведения атак на ОИ КНО (ВИС КНО), в состав которых входят СВТ, с которых пользователи осуществляют удаленный доступ к ресурсам ГИС ТОР КНД, потенциальными нарушителями может быть использована любая из возможностей, приведенная в строках 1–8 таблицы, и не используется ни одна из возможностей, приведенная в строках 9–15 таблицы, на стороне ОИ КНО (ВИС КНО) должны применяться СКЗИ/СЭП класса КС1.

В случае, если для подготовки и проведения атак на ОИ КНО (ВИС КНО), в состав которых входят СВТ, с которых пользователи осуществляют удаленный доступ к ресурсам ГИС ТОР КНД, потенциальными нарушителями может быть использована любая из возможностей, приведенная в строках 9–13 таблицы, и не используется ни одна из возможностей, приведенная в строках 14-15 таблицы, на стороне ОИ КНО (ВИС КНО) должны применяться СКЗИ/СЭП класса КС2, либо СКЗИ/СЭП класса КС1 совместно с реализацией комплекса организационно-

технических мер защиты информации, направленных на нейтрализацию возможностей, приведенных в строках 9–13 таблицы, в составе:

– организация пропускного и внутриобъектового режима по адресу расположения ОИ КНО (ВИС КНО), в состав которого входят СКЗИ/СЭП и СВТ, с которых осуществляется удаленный доступ к ресурсам ГИС ТОР КНД;

– организация контролируемой зоны на ОИ КНО (ВИС КНО), в состав которых входят СКЗИ/СЭП и СВТ, с которых осуществляется удаленный доступ к ресурсам ГИС ТОР КНД, и применяемые СКЗИ/СЭП;

– регламентация, предоставление и контроль прав (полномочий) сотрудников КНО по доступу к настройкам оборудования, СКЗИ/СЭП, программного обеспечения СВТ в составе ОИ КНО (ВИС КНО), с которых осуществляется удаленный доступ к ресурсам ГИС ТОР КНД, с учетом принципа минимальной достаточности;

– утверждение руководителем КНО списка лиц, допущенных в помещения, в которых размещены СКЗИ/СЭП и СВТ в составе ОИ КНО (ВИС КНО), с которых осуществляется удаленный доступ к ресурсам ГИС ТОР КНД, а также правил доступа в указанные помещения в рабочее время, нерабочее время и в нештатных ситуациях;

– контроль доступа лиц в помещения, в которых размещены СВТ в составе ОИ КНО (ВИС КНО), с которых осуществляется удаленный доступ к ресурсам ГИС ТОР КНД и применяемые СКЗИ/СЭП;

– исключение пребывания в помещениях, в которых размещены СКЗИ/СЭП и средства СВТ в составе ОИ КНО (ВИС КНО), с которых осуществляется удаленный доступ к ресурсам ГИС ТОР КНД, сотрудников сторонних организаций, а также сотрудников технических, обслуживающих и иных вспомогательных служб (электрики, уборщицы, сантехники и т.п.) в отсутствие контроля со стороны лиц, допущенных в указанные помещения;

– применение средств межсетевого экранирования и обнаружения вторжений на ОИ (ВИС КНО), в состав которых входят СКЗИ/СЭП и СВТ, с которых осуществляется удаленный доступ к ресурсам ГИС ТОР КНД;

– учет и контроль вноса/выноса СКЗИ/СЭП и СВТ в составе ОИ КНО (ВИС КНО), с которых осуществляется удаленный доступ к ресурсам ГИС ТОР КНД, за пределы контролируемой зоны ОИ КНО (ВИС КНО).

В случае, если для подготовки и проведения атак на ОИ КНО (ВИС КНО), в состав которых входят СВТ, с которых внешние непривилегированные пользователи осуществляют удаленный доступ к ресурсам ГИС ТОР КНД, потенциальными нарушителями может быть использована любая из возможностей, приведенная в строках 14-15 таблицы, на стороне ОИ КНО (ВИС КНО) должны применяться СКЗИ/СЭП класса КС3, либо СКЗИ/СЭП класса КС2 совместно с реализацией нижеперечисленных организационно-технических мер защиты информации, либо СКЗИ/СЭП класса КС1 совместно с реализацией комплекса организационно-технических мер защиты информации, приведенных в предыдущем абзаце и следующих нижеперечисленных дополнительных организационно-технических мер защиты информации, в составе:

– оборудование помещений, в которых размещены СКЗИ/СЭП и СВТ в составе ОИ КНО (ВИС КНО), с которых осуществляется удаленный доступ к ресурсам ГИС ТОР КНД, системой охранной сигнализации, средствами контроля доступа, надежными дверьми и замками с опечатывающими устройствами;

– контроль доступа лиц к применяемым СКЗИ/СЭП и СВТ в составе ОИ КНО (ВИС КНО), с которых осуществляется удаленный доступ к ресурсам ГИС ТОР КНД;

– контроль (опечатывание) неиспользуемых портов ввода-вывода и интерфейсов, а также корпусов СВТ в составе ОИ КНО (ВИС КНО), на которых установлены СКЗИ/СЭП и с которых осуществляется удаленный доступ к ресурсам ГИС ТОР КНД;

– контроль состава (целостности) СКЗИ/СЭП, программного и аппаратного обеспечения СВТ в составе ОИ КНО (ВИС КНО), с которых осуществляется удаленный доступ к ресурсам ГИС ТОР КНД;

– регистрация и учет действий сотрудников КНО, осуществляющих взаимодействие с ресурсами ГИС ТОР КНД с применением СКЗИ/СЭП и СВТ в составе ОИ КНО (ВИС КНО), с которых осуществляется удаленный доступ к ресурсам ГИС ТОР КНД.

Результаты определения требуемого класса СКЗИ/СЭП для применения на стороне ОИ КНО при подключении к ГИС ТОР КНД должны быть зафиксированы в отдельном документе, утвержденном руководителем КНО и подписанным членами комиссии.

Реализация организационно-технических мер защиты информации на стороне КНО на ОИ согласно установленному классу СКЗИ/СЭП должна быть обеспечена КНО до подачи заявки на подключение к ГИС ТОР КНД согласно Регламенту подключения к защищенной сети государственной информационной системы «Типовое облачное решение по автоматизации контрольной (надзорной) деятельности» (актуальные редакции размещаются на портале ГИС ТОР КНД по адресу https://knd.gov.ru).

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