**Приказ Минкомсвязи России от 03.06.2019 N 252 (ред. от 11.11.2019) Об утверждении Единых функционально-технических требований по автоматизации приоритетных видов регионального государственного контроля (надзора) в целях внедрения риск-ориентированного подхода**

# Приказ

**МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ**

**И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**ПРИКАЗ**

**от 3 июня 2019 г. N 252**

**ОБ УТВЕРЖДЕНИИ ЕДИНЫХ ФУНКЦИОНАЛЬНО-ТЕХНИЧЕСКИХ ТРЕБОВАНИЙ**

**ПО АВТОМАТИЗАЦИИ ПРИОРИТЕТНЫХ ВИДОВ РЕГИОНАЛЬНОГО**

**ГОСУДАРСТВЕННОГО КОНТРОЛЯ (НАДЗОРА) В ЦЕЛЯХ ВНЕДРЕНИЯ**

**РИСК-ОРИЕНТИРОВАННОГО ПОДХОДА**

В целях организации работы по развитию и внедрению государственной информационной системы "Типовое облачное решение по автоматизации контрольной (надзорной) деятельности, а также в целях предоставления из федерального бюджета субсидий бюджетам субъектов Российской Федерации на поддержку региональных проектов в сфере информационных технологий, направленных на автоматизацию приоритетных видов регионального государственного контроля (надзора) в целях внедрения риск-ориентированного подхода, приказываю:

1. Утвердить прилагаемые Единые функционально-технические [требования](https://sudact.ru/law/prikaz-minkomsviazi-rossii-ot-03062019-n-252/edinye-funktsionalno-tekhnicheskie-trebovaniia-po-avtomatizatsii/) по автоматизации приоритетных видов регионального государственного контроля (надзора) в целях внедрения риск-ориентированного подхода (далее - Требования).

2. Контроль за исполнением настоящего приказа возложить на статс-секретаря - заместителя Министра цифрового развития, связи и массовых коммуникаций Российской Федерации О.Б. Пака

Министр

К.Ю.НОСКОВ

**Таблица 1. Используемые определения и сокращения**

|  |  |
| --- | --- |
| **Сокращение** | **Определение** |
| ABAC | Attribute-Based-Access-Control. Модель контроля доступа к объектам, основанная на анализе правил для атрибутов объектов или субъектов, возможных операций с ними и окружения, соответствующего запросу. |
| RBAC | Role-Based-Access-Control. Стандартная ролевая модель доступа к данным. Позволяет настраивать доступ только на уровне ролей. |
| Авторизация | Авторизация участников информационного взаимодействия - подтверждение наличия у участника информационного взаимодействия прав на получение доступа к инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме.Успешная авторизация означает подтверждение прав субъекта на выполнение запрошенных им операций. |
| Аутентификация | Аутентификация участников информационного взаимодействия - проверка принадлежности участнику информационного взаимодействия введенного им идентификатора, а также подтверждение подлинности идентификатора.Для аутентификации могут использоваться логин и пароль, сертификат электронной подписи и т.д. |
| 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 |
| 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](https://sudact.ru/law/kompleksnye-trebovaniia-k-informatsionnym-sistemam-obespechivaiushchim-vypolnenie/) 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 N 40(6), (далее - Архитектура и Стандарт соответственно). |
| ЕРП | Федеральная государственная информационная система "Единый реестр проверок" |
| Идентификация | Идентификация участников информационного взаимодействия - сравнение идентификатора, вводимого участником информационного взаимодействия в любую из взаимодействующих в рамках автоматизации приоритетных видов регионального государственного контроля (надзора) информационных систем, с идентификатором этого участника, содержащимся в соответствующем базовом информационном ресурсе. |
| 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 |
| 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 в порядке, предусмотренном Федеральным [законом](https://sudact.ru/law/federalnyi-zakon-ot-26122008-n-294-fz-o/) от 26.12.2008 N 294-ФЗ "О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля" и иными нормативными правовыми актами, регулирующими общественные отношения в сфере государственного контроля (надзора), муниципального контроля" |
| НПА | Нормативный правовой акт |
| НСИ | Нормативно-справочная информации. |
| Оператор ФГИС ЕРП | Генеральная прокуратура Российской Федерации |
| Расчетный показатель | Отчетная информация по объектам контроля (надзора), привязанная к отчетным периодам и получаемая путем расчета на основе базовых показателей. |
| СМЭВ | Единая система межведомственного электронного взаимодействия |
| 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 N 12), и предусматривающий три уровня соответствия функциональных возможностей информационных систем: Базовый, Средний, Высокий |
| Субъект безопасности | Клиент или пользователь, который проходит аутентификацию\авторизацию в системе |
| Типовое облачное решение ТОР КНД | Государственная информационная система "Типовое облачное решение по автоматизации контрольной (надзорной) деятельности", созданная в соответствии с [Постановлением](https://sudact.ru/law/postanovlenie-pravitelstva-rf-ot-21042018-n-482/) Правительства Российской Федерации от 21.04.2018 N 482. |
| Токен | Уникальный код с ограниченным сроком жизни, выдается после аутентификации и используется при взаимодействии с остальными участниками системы |

# 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:

- [Постановление](https://sudact.ru/law/postanovlenie-pravitelstva-rf-ot-21042018-n-482/) Правительства Российской Федерации от 21.04.2018 N 482 "О государственной информационной системе "Типовое облачное решение по автоматизации контрольной (надзорной) деятельности";

- Федеральный [закон](https://sudact.ru/law/federalnyi-zakon-ot-26122008-n-294-fz-o/) от 26.12.2008 N 294-ФЗ "О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля";

- Федеральный [закон](https://sudact.ru/law/federalnyi-zakon-ot-27072010-n-210-fz-ob/) от 27.07.2010 N 210-ФЗ "Об организации предоставления государственных и муниципальных услуг";

- Федеральный [закон](https://sudact.ru/law/federalnyi-zakon-ot-27072006-n-149-fz-ob/) от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации";

- Федеральный [закон](https://sudact.ru/law/federalnyi-zakon-ot-27072006-n-152-fz-o/) от 27.07.2006 N 152-ФЗ "О персональных данных";

- Федеральный [закон](https://sudact.ru/law/federalnyi-zakon-ot-06042011-n-63-fz-ob/) от 06.04.2011 N 63-ФЗ "Об электронной подписи" Государственная [программа](https://sudact.ru/law/postanovlenie-pravitelstva-rf-ot-15042014-n-313/gosudarstvennaia-programma-rossiiskoi-federatsii-informatsionnoe_1/) Российской Федерации "Информационное общество (2011 - 2020 годы)" (утверждена Постановлением Правительства Российской Федерации от 15.04.2014 N 313) - подпрограмма 4 "Информационное государство".

- [Распоряжение](https://sudact.ru/law/rasporiazhenie-pravitelstva-rf-ot-26092017-n-2049-r/) Правительства Российской Федерации от 26.09.2017 N 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";

- [Распоряжение](https://sudact.ru/law/rasporiazhenie-pravitelstva-rf-ot-31012017-n-147-r/) Правительства Российской Федерации от 31.01.2017 N 147-р "Об утверждении целевых моделей упрощения процедур ведения бизнеса и повышения инвестиционной привлекательности субъектов Российской Федерации;

- [Постановление](https://sudact.ru/law/postanovlenie-pravitelstva-rf-ot-08092010-n-697/) Правительства Российской Федерации от 8.09.2010 N 697 "О единой системе межведомственного электронного взаимодействия";

- [Постановление](https://sudact.ru/law/postanovlenie-pravitelstva-rf-ot-17082016-n-806/) Правительства Российской Федерации от 17.08.2016 N 806 "О применении риск-ориентированного подхода при организации отдельных видов государственного контроля (надзора) и внесении изменений в некоторые акты Правительства Российской Федерации";

- [Постановление](https://sudact.ru/law/postanovlenie-pravitelstva-rf-ot-18042016-n-323/) Правительства Российской Федерации от 18.04.2016 N 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](https://sudact.ru/law/postanovlenie-pravitelstva-rf-ot-08062011-n-451/) Правительства Российской Федерации от 8.06.2011 N 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](https://sudact.ru/law/postanovlenie-pravitelstva-rf-ot-28122011-n-1184/) Правительства Российской Федерации от 28.12.2011 N 1184 "О мерах по обеспечению перехода федеральных органов исполнительной власти и органов государственных внебюджетных фондов на межведомственное информационное взаимодействие в электронном виде";

- [Постановление](https://sudact.ru/law/postanovlenie-pravitelstva-rf-ot-19112014-n-1222/) Правительства Российской Федерации от 19.11.2014 N 1222 "О дальнейшем развитии единой системы межведомственного электронного взаимодействия";

- [Постановление](https://sudact.ru/law/postanovlenie-pravitelstva-rf-ot-22122012-n-1382/) Правительства Российской Федерации от 22.12.2012 N 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](https://sudact.ru/law/postanovlenie-pravitelstva-rf-ot-09022012-n-111/) Правительства Российской Федерации от 9.02.2012 N 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";

- [Распоряжение](https://sudact.ru/law/rasporiazhenie-pravitelstva-rf-ot-17052016-n-934-r/) Правительства Российской Федерации от 17.05.2016 N 934-р "Об утверждении основных направлений разработки и внедрения системы оценки результативности и эффективности контрольно-надзорной деятельности";

- [Распоряжение](https://sudact.ru/law/rasporiazhenie-pravitelstva-rf-ot-19042016-n-724-r/) Правительства Российской Федерации от 19.04.2016 N 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";

- [Приказ](https://sudact.ru/law/prikaz-fstek-rossii-ot-11022013-n-17/) ФСТЭК России от 02.02.2013 N 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах";

- [Постановление](https://sudact.ru/law/postanovlenie-pravitelstva-rf-ot-01112012-n-1119/) Правительства Российской Федерации от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных";

- [Приказ](https://sudact.ru/law/prikaz-fstek-rossii-ot-18022013-n-21/) ФСТЭК России от 18.02.2013 N 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных";

- [Приказ](https://sudact.ru/law/prikaz-fsb-rossii-ot-10072014-n-378/) ФСБ России от 10.07.2014 N 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";

- [Приказ](https://sudact.ru/law/prikaz-fsb-rf-ot-27122011-n-795/) ФСБ России от 27.12.2011 N 795 "Об утверждении Требований к форме квалифицированного сертификата ключа проверки электронной подписи";

- [Приказ](https://sudact.ru/law/prikaz-fsb-rf-ot-27122011-n-796/) ФСБ России от 27.12.2011 N 796 "Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра";

- [Приказ](https://sudact.ru/law/prikaz-minkomsviazi-rf-ot-27122010-n-190/) Минкомсвязи России от 27.12.2010 N 190 "Об утверждении Технических требований к взаимодействию информационных систем в единой системе межведомственного электронного взаимодействия".

- [Постановление](https://sudact.ru/law/postanovlenie-pravitelstva-rf-ot-06072015-n-676/) Правительства Российской Федерации от 6.07.2015 N 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";

- "Базовая [модель](https://sudact.ru/law/bazovaia-model-opredeleniia-kriteriev-i-kategorii-riska/) определения критериев и категорий риска" (утв. протоколом заседания проектного комитета от 31.03.2017 N 19(3)), (вместе с "Требованиями к обоснованию предлагаемых федеральными органами исполнительной власти - участниками приоритетной программы "Реформа контрольной и надзорной деятельности" категорий риска (классов опасности) и критериев риска в отношении осуществляемых ими видов государственного контроля (надзора)").

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

В соответствии с государственной [программой](https://sudact.ru/law/postanovlenie-pravitelstva-rf-ot-15042014-n-313/gosudarstvennaia-programma-rossiiskoi-federatsii-informatsionnoe_1/) Российской Федерации "Информационное общество (2011 - 2020 годы)", утвержденной постановлением Правительства Российской Федерации от 15.04.2014 N 313 (в редакции постановления Правительства Российской Федерации от 30.12.2018 N 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 [п. 3](https://sudact.ru/law/postanovlenie-pravitelstva-rf-ot-15042014-n-313/gosudarstvennaia-programma-rossiiskoi-federatsii-informatsionnoe_1/prilozhenie-n-2_3/) Приложения 2 Программы является автоматизация приоритетных видов регионального государственного контроля (надзора) в целях внедрения риск-ориентированного подхода.

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 ТОР КНД.

Рекомендуемые мероприятия по автоматизации приоритетных видов регионального государственного контроля (надзора) в целях внедрения риск-ориентированного подхода 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 - ТОР КНД) и публикации их в Национальном фонде алгоритмов и программ (НФАП).

2. Доработка существующих региональных ведомственных информационных систем автоматизации контрольно-надзорной деятельности (далее - ВИС КНО) в субъекте Российской Федерации с целью интеграции их с ТОР КНД и (или) Федеральной государственной информационной системой "Единый реестр проверок" (ФГИС ЕРП).

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 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 средств удаленной фиксации состояний объектов контроля (надзора) в целях сбора и использования сведений с указанных средств фиксации в ТОР КНД или ВИС КНО для планирования, проведения и аудита контрольно-надзорных мероприятий в субъекте Российской Федерации.

6. Внедрение ТОР КНД, включая работы по:

6.1. Обучению с целью создания центра компетенции по направлению "Автоматизация контрольной (надзорной) деятельности";

6.2 Обучению администраторов настройке процессов контроля и надзора в соответствии с региональной практикой;

6.3 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 так же учитывается на базе какой информационной системы ранее была осуществлена автоматизации КНД по конкретному виду контроля (надзора).

# 3.1.1. 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.

# 3.1.2. 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](https://sudact.ru/law/prikaz-minkomsviazi-rossii-ot-16092013-n-248/metodicheskie-ukazaniia-o-poriadke-formirovaniia/) о порядке формирования и использования информационного ресурса национального фонда алгоритмов и программ для электронных вычислительных машин (утв. приказом Министерства связи и массовых коммуникаций Российской Федерации от 16.09.2013 N 248).

Также необходимо осуществить передачу разработанных модулей в репозиторий Минкомсвязи России с подтверждением соответствующими актами (формы и перечень документов предоставляются Минкомсвязью России) совместимости с 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.

# 3.1.3. Общие требования к программным модулям

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

Программный модуль должен быть разработан на языке Java, JavaScript, Python 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 ТОР КНД, должен соответствовать требованиям [Постановления](https://sudact.ru/law/postanovlenie-pravitelstva-rf-ot-06072015-n-676/) Правительства Российской Федерации от 06.07.2015 N 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 в соответствии со спецификацией диагностического сервиса, размещенной на портале knd.minsvyaz.ru в разделе "Документы/Субсидия из федерального бюджета".

Модель здоровья программного модуля должна быть согласована со стороны Минкомсвязи 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.

# 3.1.4. 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 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 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. Требования к структуре межотраслевых реестров субъектов и объектов, а также их наполнению приведены на портале knd.minsvyaz.ru в разделе "Документы/Субсидия из федерального бюджета".

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, основанных на экспертизе конкретного КНО на основе статистических данных.

2.3. Оценки ожидаемого ущерба охраняемым ценностям, основанных 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. Управления пользовательскими интерфейсами ввода данных в ТОР КНД, например, заполнения чек-листов и формирования отчетов, характерных для сложившейся практики КНД в конкретном КНО.

4. Интеграции с внешними по отношению к 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. Информационные системы "Открытого правительства" всех уровней.

4.4.2. Информационные системы 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 Минкомсвязью России. Данные требования, в процессе согласования, могут быть изменены для обеспечения покрытия требований нескольких потребителей.

# 3.1.5. Требования по обеспечению информационной безопасности

Для защиты информации, находящейся под управлением в модуле, от несанкционированного доступа, должны использоваться следующие средства:

- идентификация пользователя средствами ЕСИА (при доступе к ресурсам ТОР КНД);

- процедуры аутентификации на основе OAuth2 и Open ID Connect;

- идентификация пользователя встроенными средствами идентификации операционной системы или другими системными средствами - ПК или устройства (при отсутствии доступа к ТОР КНД);

- проверка полномочий пользователя средствами модуля при применимости;

- разграничение доступа пользователей на уровне задач и информационных массивов к общедоступной и конфиденциальной информации на основании ролевой модели (RBAC и/или ABAC) средствами модуля при применимости;

Программные и/или аппаратные средства, используемые для наложения и проверки электронной подписи, должны иметь сертификат соответствия ФСБ России на соответствие требованиям к средствам компьютерной защиты информации для криптографической защиты информации, не содержащей сведений, составляющих государственную тайну. Функционал использования электронной подписи должен удовлетворять требованиям ГОСТ Р 34.10-2012.

Используемые средства защиты информации должны удовлетворять требованиям нормативно-правовых актов Российской Федерации, включая требования ФСТЭК (Гостехкомиссии) России и ФСБ России.

# 3.1.6. 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](https://sudact.ru/law/prikaz-minkomsviazi-rossii-ot-16102015-n-405/metodicheskie-rekomendatsii-po-sovershenstvovaniiu-polzovatelskikh/) по совершенствованию пользовательских интерфейсов, утвержденными Приказом Минкомсвязи России от 16.10.2015 N 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 N 406пр.

# 3.2. Требования по доработке существующих региональных ВИС КНО с целью интеграции с ТОР КНД и (или) ФГИС ЕРП

В рамках создания ЕИС КНД рекомендуется интегрировать региональные ВИС КНО с ТОР КНД и с ФГИС ЕРП в целях автоматизации процессов передачи данных о проверяемых субъектах, проверяемых объектах, данных о проверках в отношении указанных лиц. 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. 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.

В настоящее время в рамках обеспечения возможности взаимодействия ТОР КНД с внешними информационными системами вне СМЭВ 3.0 доступны следующие механизмы:

- Получение справочников из ТОР КНД;

- Получение из ТОР КНД перечня субъектов, имеющихся в реестре;

- Отправка в ТОР КНД данных по новым субъектам;

- Получение из ТОР КНД перечня объектов, имеющихся в реестре;

- Отправка в ТОР КНД данных по новым объектам;

- Отправка в ТОР КНД сведений о КНМ;

- Получение из ТОР КНД информации о субъектах, объектах и КНМ;

- Получение реестра шаблонов проверочных листов из ТОР КНД;

- Получения реестра ОТ из ТОР КНД;

- Получение реестра типовых ПЭиР из ТОР КНД;

- Сервис внешнего управления реестром ПЭиР ТОР КНД;

- Передача из РПГУ/Портала КНО в ТОР КНД обращений граждан;

- Получение из ТОР КНД сведений об обязательных требованиях;

- Размещение в ТОР КНД сведений об обязательных требованиях;

- Получение из ТОР КНД сведений о проверочных листах;

- Размещение в ТОР КНД сведений о проверочных листах;

- Получение из ТОР КНД сведений о показателях эффективности и результативности КНД;

- Размещение в ТОР КНД сведений о показателях эффективности и результативности КНД.

Спецификация программных интерфейсов взаимодействия с ТОР КНД, и описание единой модели данных ТОР КНД, в соответствии с которой формируются получаемые из ТОР КНД (или передаваемые в ТОР КНД) сведения размещены на портале knd.minsvyaz.ru в разделе "Документы/Субсидия из федерального бюджета".

В соответствии с "[Требованиями](https://sudact.ru/law/prikaz-fstek-rossii-ot-11022013-n-17/trebovaniia-o-zashchite-informatsii-ne/) о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах" (утверждены приказом ФСТЭК России от 11.02.2013 N 17) и "[Требованиями](https://sudact.ru/law/postanovlenie-pravitelstva-rf-ot-01112012-n-1119/#fkzDPMCByiQr) к защите персональных данных при их обработке в информационных системах персональных данных" (утверждены постановлением Правительства Российской Федерации от 01.11.2012 N 1119) для ТОР КНД установлен 2 класс защищенности государственной информационной системы и 3 уровень защищенности персональных данных, и в соответствии с методическим документом "[Меры](https://sudact.ru/law/metodicheskii-dokument-mery-zashchity-informatsii-v-gosudarstvennykh/) защиты информации в государственных информационных системах" (утвержден ФСТЭК России от 11.02.2014) установлены следующие требования для организации информационного взаимодействия ТОР КНД с внешними информационными системами:

1. Информационное взаимодействие ТОР КНД с внешними информационными системами осуществляется с использованием средств криптографической защиты каналов связи (не ниже класса КС3) совместимых с СКЗИ семейства ViPNet. Актуальную версию используемых СКЗИ с необходимо согласовать с оператором ТОР КНД.

2. Информационное взаимодействие осуществляется на основании договора (соглашения) об информационном взаимодействии с оператором (обладателем, владельцем) внешней информационной системы.

3. Оператору (обладателю, владельцу) внешней информационной системы необходимо наличие подтверждения выполнения во внешней информационной системе требований по защите информации (наличие аттестата соответствия требованиям по безопасности информации или иное подтверждение).

В случае интеграции с ФГИС ЕРП необходимо руководствоваться требованиями к защите информации СМЭВ 3.x и Оператора ФГИС ЕРП.

**Минимальные рекомендуемые требования для стационарных АРМ**

:

|  |  |
| --- | --- |
| 1. Размер и разрешение экрана 19" | 1600 x 900 |
| 2. Тип и частота процессора: | 2.0 ГГц |
| 3. Тип и объем оперативной памяти | DDR3 4 Гб |
| 4. Тип и объем дисков | SATA 512 Гб |

**Минимальные рекомендуемые требования для переносных АРМ**

:

|  |  |
| --- | --- |
| 1. Размер и разрешение экрана 14" | 1920 x 1080 |
| 2. Тип и частота процессора: | 2.0 ГГц |
| 3. Тип и объем оперативной памяти | DDR3 4 Гб |
| 4. Объем дисков | 256 Гб |

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

Стационарное рабочее место пользователя должно иметь возможность подключения к многофункциональному устройству, обеспечивающему печать и сканирование документов.

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

**Минимальные требования для мобильных АРМ**

:

|  |  |  |
| --- | --- | --- |
| **-** | Размер экрана | 5 - 6,5/8 - 10,4 дм |
| **-** | Объем оперативной памяти | не менее 3/4 Гб |
|  |
| **-** | Объем стационарной памяти | не мене 64/64 Гб |
| **-** | Разрешение экрана | 1280 \* 800/1920 \* 1080 |
| **-** | Поддерживаемые сети | **3G, 4G, LTE, WiFi** |
| **-** | Возможность установки microSD карт памяти | **да/да** |
| **-** | Объемом карты памяти не менее | **64/64 Гб** |
| **-** | Наличие и поддержка систем геопозициониров (GPS, GPS-A, ГЛОНАСС) | **да/да** |
| **-** | Диапазон рабочих температур | **-20****+60 °C** |
| **-** | Разрешение основной камеры | **от 8 МП.** |

Мобильные АРМ могут использоваться только как переносной накопитель для сбора информации, но не для передачи ее в последующем по беспроводным каналам связи.

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).

Устройства должны быть обеспечены встроенной фотокамерой (для мобильных АРМ) или web-камеры (для переносных АРМ).

В состав программно-технического комплекса может входить мобильный принтер для мобильных и переносных АРМ, операционная система, набор программного обеспечения для работы с типами файлов, содержащими текстовую, числовую и графическую информацию (офисное программное обеспечение).

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.

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

.

Данное мероприятие направлено на обеспечение требований информационной безопасности ВИС КНО при автоматизации КНД и (или) автоматизированных рабочих мест, в том числе переносных, обеспечивающих выполнение функций по контролю (надзору) в субъекте Российской Федерации (далее - клиент) при подключении к ВИС КНО или ТОР КНД.

1. При обеспечении требований информационной безопасности рекомендуется:

1.1. Выполнить работы по формированию требований к системе защиты информации ВИС КНО, моделированию угроз безопасности информации, разработке проектных решений на систему защиты информации ВИС КНО и организационно-распорядительной документации по защите информации, обрабатываемой в ВИС КНО.

1.2. Осуществить создание системы защиты информации ВИС КНО, нейтрализующей актуальные угрозы безопасности информации. Система защиты информации ВИС КНО должна включать в себя организационные и технические меры защиты, определенные с учетом актуальных угроз безопасности информации.

1.3. Обеспечить реализацию соответствующих технических и организационных мер по защите информации, включая внедрение системы защиты информации ВИС КНО, в соответствии с требованиями законодательства Российской Федерации и подзаконных нормативных правых актов в области защиты информации, в том числе:

- "[Состав и содержание](https://sudact.ru/law/prikaz-fstek-rossii-ot-18022013-n-21/#tGkQHLvv3VY1) организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных" (утверждены приказом ФСТЭК России от 18.02.2013 N 21);

- "[Требования](https://sudact.ru/law/postanovlenie-pravitelstva-rf-ot-01112012-n-1119/#fkzDPMCByiQr) к защите персональных данных при их обработке в информационных системах персональных данных" (утверждены постановлением Правительства Российской Федерации от 1.11.2012 N 1119);

- "[Состав и содержание](https://sudact.ru/law/prikaz-fsb-rossii-ot-10072014-n-378/#KcF2HsEDsQNJ) организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности" (утверждены приказом Федеральной службы безопасности Российской Федерации от 10.07.2014 N 378);

- "[Инструкция](https://sudact.ru/law/prikaz-fapsi-ot-13062001-n-152-ob/#VjkXfHcPeQmm) об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну" (утверждена приказом Федерального агентства правительственной связи и информации от 13.06.2001 N 152).

Если ВИС КНО помимо информационных систем персональных данных относится также к государственным информационным системам, реализация соответствующих технических и организационных мер по защите информации, включая внедрение системы защиты информации ВИС КНО, помимо вышеуказанного в данном пункте настоящих требований законодательства Российской Федерации и подзаконных нормативных правых актов в области защиты информации, обеспечивается, в том числе в соответствии с "[Требованиями](https://sudact.ru/law/prikaz-fstek-rossii-ot-11022013-n-17/trebovaniia-o-zashchite-informatsii-ne/) о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах" (утверждены Приказом ФСТЭК России от 02.02.2013 N 17).

1.4. Обеспечить защиту информации в ходе эксплуатации ВИС КНО в соответствии с эксплуатационной документацией на систему защиты информации ВИС КНО и организационно-распорядительными документами по защите информации.

Эксплуатационная документация на систему защиты информации ВИС КНО и организационно-распорядительные документы по защите информации могут корректироваться в ходе управления (администрирования) системой защиты информации ВИС КНО, в том числе с помощью рекомендуемых к использованию средств автоматизированной разработки документации по защите информации и поддержки документов в актуальном состоянии.

При обеспечении информационной безопасности клиента ВИС КНО следует руководствоваться вышеприведенными требованиями как рекомендованными. Актуальные требования к обеспечению информационной безопасности клиента ВИС КНО необходимо уточнить у оператора ВИС КНО.

2. При подключении к ТОР КНД требуется обеспечить криптографическую защиту каналов связи с использованием сертифицированных средств криптографической защиты информации не ниже класса КС3, совместимых с средствами криптографической защиты информации ViPNet Coordinator версии 4.x, используемых в ТОР КНД. Если в органах исполнительной власти уже осуществляется взаимодействие со сторонними системами посредством сети VipNet, то для взаимодействия с ТОР КНД необходимо использовать ее.

3. При подключении к ТОР КНД требуется обеспечить защиту стационарных АРМ, переносных АРМ, входящих в состав ВИС КНО, с использованием комплектов сертифицированных средств защиты информации для ВИС КНО или ТОР КНД:

- Сертифицированными средствами защиты информации от несанкционированного доступа, реализующими требования, предъявляемые нормативно-правовыми актами Российской Федерации в области защиты информации. Выбранные средства защиты информации должны удовлетворять требованиям, предъявляемым к обеспечению защищенности государственных информационных класса К2 (не ниже) и к обеспеченности третьего уровня защищенности персональных данных (не ниже).

Данные средства защиты могут включать в свой состав модули контроля устройств, доверенной загрузки, персонального межсетевого экрана, средства обнаружения вторжений.

- Сертифицированными ФСБ или ФСТЭК России средствами антивирусной защиты, реализующими требования, предъявляемые нормативно-правовыми актами уполномоченных федеральных органов исполнительной власти Российской Федерации в области защиты информации к обеспечению третьего уровня защищенности персональных данных (не ниже), и при необходимости к обеспечению защищенности государственных информационных систем класса К2 (не ниже).

Абзацы четвертый - пятый исключены. - Приказ Минкомсвязи России от 11.11.2019 N 707.

- Средство квалифицированной электронной подписи, ее проверки и доверенной визуализации подписываемого документа.

# 3.5. 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 - датчики) в целях сбора данных и использования их для проведения аудита и планирования контрольно-надзорных мероприятий, и дистанционного контроля в отношении указанных объектов.

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

- обеспечена возможность автоматизировано получать данные с датчиков в формате пригодном для проведения анализа через API датчика;

- датчики должны предоставлять данные с устанавливаемой периодичностью;

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

- датчики должны обеспечивать возможность получения данных о текущем состояния (включен/выключен) и настройки через API;

- датчики должны обеспечивать бесперебойную работу в течение заявленных сроков эксплуатации.

Перечень датчиков, 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.minsvyaz.ru в разделе "Документы/Субсидия из федерального бюджета".

Для передачи данных могут быть использованы различные стандарты и протоколы, принятые в сфере деятельности в которой ведется мониторинг объектов и передача данных, например:

- DICOM (Digital Imaging and Communications in Medicine) - медицинский отраслевой стандарт создания, хранения, передачи и визуализации цифровых медицинских изображений и документов обследованных пациентов.

- EGTS - протокол EGTS (Era Glonass Telematics Standard) - протокол обмена данными автомобильной системы/устройства вызова экстренных оперативных служб с инфраструктурой системы экстренного реагирования при авариях.

- SNMP (Simple Network Management Protocol) - стандартный интернет-протокол для управления устройствами в IP-сетях на основе архитектур TCP/UDP.

- 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.

- OPC Unified Architecture (англ. Унифицированная архитектура OPC) - спецификация, определяющая передачу данных в промышленных сетях и взаимодействие устройств в них.

При сопряжении с ВИС КНО (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 тока и на эффекте Холла, фотоэлектрические датчики, датчики PIR, LiDAR и активные датчики, датчики MEMS);

- интеллектуальные оконечные точки IIоТ;

- исполнительные устройства и устройства вывода информации;

- устройства ввода информации (извещатели);

- источники энергии и устройства управления электропитанием.

Итоговые требования к датчикам устанавливаются уполномоченными лицами субъекта Российской Федерации исходя из целей автоматизации КНД.

# 3.6.1. 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:

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

- организация семинаров по порядку и методологии сбора данных для настройки процессов КНД в 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 knd.minsvyaz.ru в разделе "Документы/Субсидия из федерального бюджета";

- анализу процессов контрольно-надзорной деятельности КНО для настройки реестров и справочников в 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

- работа с данными, включающая 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 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 ТОР КНД.

# 3.6.2. 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 ТОР КНД в КНО, и иных уполномоченных лиц настройке процессов контроля и надзора в 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 ТОР КНД;

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

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

- настройки подсистемы безопасности;

- настройка печатных форм документов;

- импорт/экспорт данных из внешних систем посредством файловых выгрузок, средствами универсальных механизмов настройки форматов загрузки -.xls, -.dbf, -.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 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, сведения которых необходимы для региональных видов контроля (надзора);

- настройка интеграции 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 ТОР КНД.

# 3.6.3. 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 ТОР КНД и включать в себя одну или несколько работ по настройке ТОР КНД из перечисленных ниже:

- разработка новых и (или) корректировка в 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 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 ТОР КНД.