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

Основные термины, определения и сокращения

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 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»
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), которой 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 от 26.12.2008 № 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 №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 Правительства Российской Федерации от 21.04.2018 № 482.
Токен	Уникальный код с ограниченным сроком жизни, выдается после аутентификации и используется при взаимодействии с остальными участниками системы

Под плагинами, динамически подключаемыми к ТОР КНД, понимаются независимо-компилируемые модули, дополняющие функциональность 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 ТОР КНД. Это должно быть выполнено при проведении согласования тематики доработки и функционала плагина с Минкомсвязью России на предмет дублирования и переиспользования функционала.

Руководство разработчика ТОР КНД размещено на портале knd.minsvyaz.ru в разделе «Документы / Субсидия из федерального бюджета». Общие требования приведены ниже.

1.1.1. 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.

1.1.2. 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 (утв. приказом Министерства связи и массовых коммуникаций Российской Федерации от 16.09.2013 № 248).

Так же 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 объёме.

1.1.3. 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 Правительства Российской Федерации от 6.07.2015 № 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 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.

1.1.4. 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) расчёта 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 отчётов, 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 отчётности 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 удалённой 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 приёму, 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.

1.1.5. 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.

1.1.6. 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, утверждёнными Приказом Минкомсвязи России от 16.10.2015 № 405 и Методическими рекомендациями по информированию граждан о преимуществах получения государственных и муниципальных услуг в электронной форме, утверждёнными 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.