ПРОЕКТ

Стратегия создания российского репозитория программных пакетов и библиотек, находящегося в юрисдикции и на территории Российской Федерации

I. Общие положения

1.1. Настоящая Стратегия создания российского репозитория программных пакетов и библиотек, находящегося в юрисдикции и на территории Российской Федерации (далее, соответственно - Стратегия и Российский репозиторий) определяет цели и основные задачи по его созданию, принципы и механизмы реализации, а также меры, направленные на его поддержку при создании, использовании и развитии программного обеспечения, используемого во всех сферах деятельности государства, бизнеса и общества и реализуемого на отечественных аппаратных платформах.

1.2. Правовую основу настоящей Стратегии составляют:

– Конституция Российской Федерации;

– Федеральный закон от 28 июня 2014 г. № 172-ФЗ "О стратегическом планировании в Российской Федерации";

– Федеральный закон от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;

– Указ Президента Российской Федерации от 21 июля 2020 г. № 474 "О национальных целях развития Российской Федерации на период до 2030 года";

– Указ Президента Российской Федерации от 9 мая 2017 г. № 203 "О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы";

– Указ Президента Российской Федерации от 1 декабря 2016 г. № 642 "О Стратегии научно-технологического развития Российской Федерации";

– План мероприятий «Создание дополнительных условий для развития отрасли информационных технологий» («Второй пакет мер поддержки») от 9 сентября 2021 г.;

– иные нормативные правовые акты Российской Федерации, определяющие направления применения информационных технологий в Российской Федерации.

1.3. Настоящая Стратегия является основой для разработки (корректировки):

– государственных программ Российской Федерации;

– государственных программ субъектов Российской Федерации;

– федеральных и региональных проектов;

– плановых и программно-целевых документов государственных корпораций, государственных компаний, акционерных обществ с государственным участием;

– стратегических документов иных организаций в части вопросов, связанных с разработкой и использованием операционных систем и других программных продуктов, используемых во всех сферах деятельности государства, бизнеса и общества.

1.4. Положения настоящей Стратегии должны учитываться при реализации следующих документов:

– Стратегия национальной безопасности Российской Федерации, утвержденная Указом Президента РФ от 2 июля 2021 г. № 400;

– Доктрина информационной безопасности Российской Федерации, утвержденная Указом Президента от 05 декабря 2016 года № 646;

– Стратегия развития информационного общества в Российской Федерации на 2017 - 2030 годы;

– Стратегии развития отрасли информационных технологий в Российской Федерации на 2014–2020 годы и на перспективу до 2025 года;

– Стратегия развития электронной промышленности Российской Федерации на период до 2030 года;

– национальная программа «Цифровая экономика Российской Федерации» и иные национальные проекты (программы), федеральные и региональные проекты;

– план мероприятий «Создание дополнительных условий для развития отрасли информационных технологий» («Второй пакет мер поддержки») от 9 сентября 2021 г.;

– Планы мероприятий («дорожные карты») Национальной технологической инициативы;

– государственные программы, программно-целевые документы;

– проекты, обеспечивающие достижение целей и показателей деятельности федеральных и региональных органов исполнительной власти.

II. Основные понятия и их определения

Для целей настоящей Стратегии используются следующие основные понятия и их определения:

безопасное программное обеспечение - программное обеспечение, разработанное с использованием совокупности мер, направленных на предотвращение появления и устранение уязвимостей программы (ГОСТ Р 56939—2016).

программное обеспечение - совокупность программ системы обработки информации и программных документов, необходимых для эксплуатации этих программ (ГОСТ 19781—90).

система защиты информации - совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации (ГОСТ Р 50922-2006);

средство защиты информации - техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации (ГОСТ Р 50922-2006);

исходный текст (исходный код) – компьютерная программа в текстовом виде на каком-либо языке программирования;

открытый исходный код – исходный код (текст) программного обеспечения, распространяемый правообладателем на условиях открытой лицензии, удовлетворяющей 10 принципам открытости, предложенным некоммерческой организацией Open Source Initiative (OSI);

проприетарное программное обеспечение – программное обеспечение, согласно определению ГОСТ Р 54593-2011, не являющееся свободным.

программное обеспечение с открытым кодом (также – «открытое программное обеспечение») – программное обеспечение, доступ к которому предоставлен в соответствии с открытой лицензией;

репозиторий - распределенная инфраструктура разработки программного кода, включая библиотеки программ, с возможностью контроля версионности, дополненная функциями совместной работы над кодом, багтрекинга,

автоматической проверки и тестирования, а также другими инструментами разработки и обеспечения целостности;

Российский репозиторий – репозиторий, соответствующий требованиям, определенным в данной Стратегии;

свободное программное обеспечение – программное обеспечение, согласно определению ГОСТ Р 54593-2011;

Центр компетенций по поддержке деятельности Российского репозитория – организация, уполномоченная осуществлять функции Центра компетенций по поддержке деятельности Российского репозитория, отвечающая установленным Правительством Российской Федерации базовым требованиям.

III. Предпосылки и условия создания Российского репозитория

3.1. Краткая характеристика зарубежных и отечественных репозиториев

Основными зарубежными и отечественными репозиториями являются:

– Debian. Правовая принадлежность - Ассоциация разработчиков СПО. Финансирование и юридическая поддержка - фонд Software in the Public Interest (SPI) (зарегистрирован в штате Нью-Йорк, США). Согласно Конституции Debian, SPI – единственная организация, которой доверено хранить собственность и деньги Проекта Debian.

– Red Hat. Собственник - компания IBM (США). Программные продукты на основе Red Hat регулируются правилами экспортного управления США и другими законами США и не могут быть экспортированы в страну, охваченную запретительными санкциями.

– SuSE. Собственник - EQT, консультационный фонд по частным инвестициям, основанный Swedish industrial holding (Швеция) и AEA Investors (США). (Штаб-квартира SUSE располагается в Нюрнберге (Германия).

– Сизиф «Sisyphus». Правовая принадлежность – «Базальт СПО», 100% управление и контроль над развитием из российской юрисдикции, регистрация Российская Федерация.

Российские разработчики не имеют возможности влиять на политику использования зарубежных репозиториев.

Правительства ряда иностранных государств и межгосударственные объединения поддерживают грантами и госзаказами развитие открытого

программного обеспечения. Китай также работает над созданием экосистемы свободного программного обеспечения, создавая свои варианты открытых операционных систем (HarmonyOS, OpenEuler), Java (BishengJDK), PostgreSQL (GaussDB) на базе зарубежных репозиториев.

Российские разработчики принимают активное участие в разработке открытого программного обеспечения. Россия входит в десятку крупнейших контрибьютеров международных проектов с открытым кодом.

3.2. Риски производства операционных систем и программных продуктов, в репозиториях, расположенных за рубежом и находящихся в иностранной юрисдикции

Большинство некоммерческих организаций, управляющих проектами открытого кода, а также его онлайновых репозиториев, сосредоточены в юрисдикции США. Это делает проекты открытого кода уязвимыми к односторонним решениям государственных органов США, особенно в таких критически важных областях, как КИИ и обороноспособность страны.

В настоящее время санкционное давление на Российскую Федерацию продолжает усиливаться, в том числе, на жизненно важные отрасли народного хозяйства и оборонного комплекса Российской Федерации. В этой связи, наиболее серьезными рисками при производстве программного обеспечения, созданного на базе зарубежных репозиториев, являются:

– возможность встраивания недекларируемых возможностей (закладки для сбора информации либо совершения какого-либо вредоносного действия), а также библиотек, отдельных файлов, модификация существующих файлов в разрабатываемых данным репозиторием дистрибутивах;

– отсутствие контроля и определения жизненного цикла программного продукта, созданного на базе репозитория (важно отметить, что жизненный цикл любого инфраструктурного технологического программного продукта определяется жизненным циклом операционной системы, для которой он написан);

– отсутствие гарантированной возможности вносить в проекты свободного программного обеспечения разработки российских программистов для повышения конкурентоспособности отечественных программных продуктов на мировом рынке;

– отсутствие механизмов, обеспечивающих и гарантирующих совместимость с отечественными аппаратно-программными платформами и в целом с российскими микропроцессорами;

– наличие проблем обратной совместимости произведенных ранее программно-аппаратных средств и отсутствие современных драйверов для их запуска;

– отсутствие влияния на техническую политику разработки программного обеспечения, включённого в зарубежные репозитории.

Таким образом, с учетом рассмотренных выше условий, предпосылок и связанных с ними рисков, создание Российского репозитория является актуальной задачей.

IV. Цели и задачи создания Российского репозитория

4.1. Целями создания Российского репозитория являются:

– обеспечение условий устойчивого развития отечественной отрасли информационных и телекоммуникационных технологий;

– обеспечение необходимого уровня конкурентоспособности отечественных компаний на международном рынке;

– содействие созданию инфраструктуры разработки отечественного программного обеспечения, реализуемого на отечественных аппаратных платформах;

– обеспечение целостности, безопасности и устойчивости функционирования объектов критической информационной инфраструктуры Российской Федерации, включая объекты военного и государственного управления (далее – КИИ).

4.2. Для достижения указанных в п. 4.1. целей необходимо решить следующие задачи:

а) создание экосистемы системного программного обеспечения для отечественного микропроцессорного оборудования;

б) создание единой цифровой среды на отечественных технологиях, программных и аппаратных средствах, включающей, в том числе российские

операционные системы, Российский репозиторий и оборудование с российскими архитектурно независимыми от зарубежных решений процессорами;

в) создание служб технической поддержки единой цифровой среды, построенной на российской технологической платформе;

г) поддержка системы обучения специалистов и пользователей в сферах развития информационных технологий и телекоммуникаций, а также обеспечения доверия и безопасности их использования;

д) актуализация и совершенствование системы нормативного правового и технического регулирования в вопросах создания и развития российского программного обеспечения и оборудования с российскими архитектурно независимыми от зарубежных решений процессорами, в том числе для использования в КИИ.

V. Основные принципы создания, функционирования и развития Российского репозитория

5.1. Участие государства в поддержке создания и осуществлении контроля за соблюдением основных требований к Российскому репозиторию.

5.2. Технологический суверенитет: обеспечение необходимого уровня самостоятельности Российской Федерации в области разработки и использования программного обеспечения посредством гарантированного доступа к необходимым компонентам и участия в разработке открытых стандартов и спецификаций, в том числе международных.

5.3. Недискриминационный доступ разработчиков к информации о применяемых в программных продуктах алгоритмах работы и их исходному коду при создании программных продуктов.

5.4. Для разработчиков, разместивших программное обеспечение в Российском репозитории, создаются преференции на российском рынке.

5.5. Целостность инновационного цикла: обеспечение тесного взаимодействия научных исследований и разработки программного обеспечения с реальным сектором экономики.

5.6. Экономическая эффективность: обеспечение доступности под открытой лицензией исходного кода, разработанного на средства федерального и регионального бюджетов, в том числе, используемого в

государственных информационных системах (далее – ГИС) для его доработки и повторного использования.

5.7. Внедрение инноваций, основанных на обмене знаниями и навыками, в качестве базы для создания современных эффективных бизнес-моделей цифровой трансформации, построения массовых онлайновых сервисов, развития цифровых экосистем.

5.8. Участие в международных разработках: увеличение доли разработок, осуществляемых в Российской Федерации, участие в международных проектах, участие в разработке открытых стандартов и спецификаций, увеличение количества российских проектов с открытым кодом.

5.9. В библиотеке Российского репозитория может размещаться проверенное в соответствии с уровнем доверия российское, иностранное и «открытое» программное обеспечение.

5.10. К программному обеспечению предъявляются требования или рекомендации по уровню доверия в соответствии с уровнем безопасности объекта, на котором оно используется.

5.11. Высокие уровни доверия к программному обеспечению устанавливаются только для объектов КИИ с высоким уровнем ущерба при нарушении функционирования. Для иных объектов защиты требования или рекомендации определяются с учетом создания благоприятных условий для развития рынка российского программного обеспечения.

5.12. Российский репозиторий в обязательном порядке используется при создании программного обеспечения для объектов КИИ и ГИС, а также может использоваться для разработки иного российского программного обеспечения.

5.13. Объекты защиты с высокими рисками должны иметь «закрытую» архитектуру, выделенные каналы взаимодействия (если они требуются) и высокие уровни доверия программного обеспечения.

5.14. ГИС с высоким уровнем рисков должны быть категорированы как объекты КИИ. Для иных ГИС, в том числе взаимодействующих с объектами массового рынка, должны быть установлены менее жесткие требования к уровню доверия программного обеспечения.

5.15. К объектам защиты с «открытой» архитектурой, в том числе объектам массового рынка, использующим сети связи общего пользования, не предъявляются требования с высоким уровнем доверия к программному обеспечению.

5.16. Уровни доверия программного обеспечения должны формироваться с учетом рисков для каждой его категории. В объектах КИИ определенной категории значимости должно использоваться программное обеспечение с установленным уровнем доверия.

5.17. Должна быть обеспечена технологическая независимость от зарубежных дистрибутивов и репозиториев.

5.18. Российский репозиторий, как объект защиты, должен включать систему защиты информации со встроенными и (или) дополнительными средствами защиты информации, обеспечивающими уровень безопасности разработки и хранения, достаточный для соответствующей категории программного обеспечения, а также:

а) идентификацию и аутентификацию пользователей (разработчиков программного обеспечения);

б) управление доступом в среде виртуализации с выделением временных сегментов с ресурсами разработки для каждого разработчика;

в) изоляцию среды разработки и тестирования для каждого разработчика программного обеспечения;

г) динамическое разграничение доступа к библиотекам исходного кода и объектным файлам для разных разработчиков программного обеспечения с обеспечением защиты прав на интеллектуальную собственность в соответствии с правовым статусом программного обеспечения;

д) контроль целостности эталонных файлов программного обеспечения, компиляторов и интерпретаторов, в том числе при использовании их на оборудовании разработчиков;

е) защиту каналов связи при удаленном взаимодействии разработчиков с Российским репозиторием с использованием российских или иностранных средств криптографической защиты информации в зависимости от сегмента Российского репозитория;

ж) антивирусную проверку файлов, размещаемых в библиотеке эталонного программного обеспечения;

з) сетевую защиту (межсетевое экранирование, обнаружение и защиту от вторжений.

VI. Требования к программному обеспечению по уровням доверия

С учетом принципов, изложенных в разделе V, требования к различным сегментам программного обеспечения, формируемого в Российском репозитории, могут быть представлены следующим образом:

6.1. Уровень доверия к программному обеспечению определяет возможность его использования в установленных классах или категориях объектов защиты.

6.2. К программному обеспечению, используемому на объектах КИИ или в ГИС, устанавливаются более высокие уровни доверия, чем к программному обеспечению для иных информационных систем.

6.3. К программному обеспечению, используемому на объектах защиты с «открытой» архитектурой, по определению не требуются высокие уровни доверия.

6.4. Иерархия уровня доверия к программному обеспечению по уровню контроля недокументированных возможностей: контроль исходного кода; контроль интерпретируемого кода; контроль объектного файла.

6.5. Иерархия уровня доверия к программному обеспечению по разработчику: российский; независимый («открытое» программное обеспечение), иностранный.

6.6. Иерархия уровня доверия к программному обеспечению по архитектуре объекта защиты: «закрытая»; «открытая» (т.е. с неопределенным кругом пользователей, программного или аппаратного обеспечения, трансграничными каналами связи, например, объекты массового рынка).

6.7. Иерархия уровня доверия к программному обеспечению по производителю и разработчику архитектуры аппаратного обеспечения: российские разработчик архитектуры и производитель; российский разработчик архитектуры, но иностранный производитель; иностранный разработчик архитектуры, но российский производитель; иностранный разработчик архитектуры и производитель.

6.8. Иерархия уровня доверия к программному обеспечению по разработчику системного и прикладного программному обеспечению: российский разработчик СПО и ППО; российский разработчик СПО, но иностранный разработчик ППО; иностранный разработчик СПО, но российский разработчик ППО; иностранный разработчик СПО и ППО.

6.9. Иерархия по категории значимости объекта КИИ: 1; 2; 3 (применимо к КИИ).

6.10. Иерархия по классу защищенности ГИС: 1; 2; 3 (применимо к ГИС).

6.11.Уровни доверия к программному обеспечению должны быть установлены нормативным правовым актом.

VII. Базовые требования к Российскому репозиторию

7.1. Наличие у отечественных производителей системного и прикладного программного обеспечения собственной инфраструктуры разработки, находящейся на территории и в юрисдикции Российской Федерации, соответствующей ГОСТ Р 54593-2011 «Информационные технологии. Свободное программное обеспечение. Общие положения», в том числе наличие:

а) собственного открытого репозитория программного обеспечения (rpm-/src.rpm/deb-пакеты);

б) инструментария для подготовки и тестирования программных пакетов;

в) инструментария обеспечения целостности репозитория;

г) инструментария для разработки конечных решений: дистрибутивов, образов виртуальных машин, контейнеров, Live-образов.

7.1. Инфраструктура разработки обеспечивает полный жизненный цикл разработки и эксплуатации системного и прикладного программного обеспечения, в том числе используемого для оснащения программно-аппаратных комплексов КИИ Российской Федерации.

7.2. Жизненный цикл продуктов (дистрибутивов) на аппаратно-программной платформе не зависит от выпуска каких-либо зарубежных дистрибутивов операционных систем.

7.3. Обеспечивается единая кодовая база для всех поддерживаемых аппаратных архитектур.

7.4. Обеспечивается поддержка отечественных аппаратных платформ, в том числе архитектура отечественных процессоров, разработанная в Российской Федерации и находящейся в ее юрисдикции.

7.5. Обеспечивается участие разработчиков в ключевых международных проектах, наличие значимого числа патчей кода, принятых международными проектами и включенными в международные версии продуктов, либо полностью самостоятельная разработка.

7.6. Жизненный цикл операционных систем и инфраструктурных программных продуктов, используемых в КИИ, не зависит от зарубежных репозиториев.

7.7. Оценка соответствия требованиям, указанным в пунктах 7.1.-7.6. настоящего раздела, осуществляется уполномоченным органом государственной власти в порядке, определенном Правительством Российской Федерации, на основе прилагаемой к настоящей Стратегии методики проверки.

VIII. Механизмы реализации Стратегии

8.1. Реализация настоящей Стратегии обеспечивается согласованными действиями федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления, государственных академий наук, научных и образовательных организаций, государственных корпораций, государственных компаний и акционерных обществ с государственным участием.

8.2. Для координации деятельности сообществ разработчиков, образовательных и научных организаций по реализации настоящей Стратегии создается центр компетенций по содействию деятельности Российского репозитория на базе организации, отвечающей базовым требованиям настоящей Стратегии. Такая организация выполняет следующие функции:

а) обеспечивает взаимодействие с операторами Российских репозиториев по вопросам организационного, технологического, экономического и правового характера, а также другим вопросам, связанным с функционированием и развитием Российских репозиториев;

б) оказывает участникам рынка разработки программного обеспечения организационно-техническую и методическую поддержку;

в) содействует сотрудничеству между потенциальными заказчиками и разработчиками программного обеспечения;

г) оказывает просветительскую и образовательную поддержку заказчиками и разработчикам отечественного программного обеспечения, включая проведение мероприятий и размещение соответствующих материалов в медиа;

д) оказывает юридическую поддержку, включая консультирование разработчиков и заказчиков по вопросам использования Российских репозиториев, проверке юридической корректности использования программного обеспечения.

8.3. Финансовое обеспечение реализации настоящей Стратегии осуществляется за счет средств Государственного бюджета, средств государственных внебюджетных фондов и внебюджетных источников, включая средства институтов развития, государственных корпораций, государственных компаний, акционерных обществ с государственным участием и частные инвестиции.

8.4. Результаты мониторинга реализации настоящей Стратегии и предложения по ее корректировке отражаются в совместном экспертно-аналитическом докладе Правительства Российской Федерации и Центра компетенций.

IX. Меры по созданию и развитию Российского репозитория

9.1. Меры организационного и технологического характера.

9.1.1. Разработка по тематике, связанной с созданием и применением репозиториев, национальных стандартов и спецификаций и их продвижение при участии в разработке соответствующих международных стандартов.

9.1.2. Формирование технической политики разработки программного обеспечения, развертывание на базе Российского репозитория современных средств анализа кода и тестирования приложений с использованием разработок отечественных компаний в области информационной безопасности.

9.1.3. Формирование механизмов проверки и обеспечения совместимости с российскими микропроцессорами и российскими аппаратно-программными платформами.

9.1.4. Формирование единого российского реестра российских технических средств с включением в него как российских программных, так и российских аппаратных средств.

9.1.5. Обеспечение процесса безопасной разработки, тестирования и исследований безопасности программного обеспечения для использования в КИИ. Тестирование, включающее статический и динамический анализ кода, должно проводиться на всех доступных аппаратных архитектурах, включая российские.

9.1.6. Разработка комплекса требований, рекомендаций и стандартов по использованию программного обеспечения с открытым кодом для целей КИИ. Создание системы контроля за соблюдением установленных требований.

9.1.7. Организация публикации под отечественной открытой лицензией исходных кодов программного обеспечения, документации к нему и описаний процесса сборки программного обеспечения, разработанного на бюджетные средства (в том числе, по государственному заказу) в Российском репозитории, кроме случаев, когда программному обеспечению присвоен гриф секретности.

9.1.8. Стимулирование участия российских разработчиков в международных проектах, продукты которых используются в России.

9.1.9. Привлечение отечественных разработчиков к доработке и развитию программного обеспечения в Российском репозитории.

9.1.10. Публикация методических материалов и содействие заказчикам в создании системного программного обеспечения, используемого в КИИ.

9.2. Меры по усилению кадрового потенциала.

9.2.1. Продвижение использования и создания программного обеспечения из отечественного Репозитория с открытым кодом в сфере науки и образования.

9.2.2. Преимущественное использование программного обеспечения с открытым кодом продуктов в учебных курсах, включая лабораторные работы, примеры и упражнения. Организация доступа к Российскому репозиторию для образовательных и научных организаций.

9.2.3. Стимулирование участия ИТ-компаний в преподавании практических аспектов программирования и технологий в образовательных организациях высшего и среднего профессионального образования и в направлении своих специалистов и экспертов для преподавания и руководства выпускными квалификационными работами и другими студенческими проектами в области разработки программных продуктов, созданных на базе Российского репозитория.

9.2.4. Формирование у выпускников ВУЗов готовности и способности применять получаемые знания для совершенствования отечественных архитектур вычислительной техники, расширения функциональности, надежности, безопасности и совместимости программного обеспечения для этих архитектур, повышения доверия и заинтересованности пользователей в применении отечественной продукции.

Для содействия решению указанных задач представляется целесообразным разработать и реализовать новую учебную дисциплину «Инфраструктура разработки отечественного программного обеспечения», включающую следующие основные разделы:

– программирование, оптимизация, отладка, портирование, отечественные и зарубежные архитектуры микропроцессоров;

– сборка и сопровождение совместимого программного продукта в отечественном репозитории;

– тестирование программного продукта в отечественной доверенной программно-аппаратной среде;

– приложения для ИКТ-инфраструктуры на отечественных программно-аппаратных средствах;

– приложения для КИИ на отечественных программно-аппаратных средствах.

Преподавание всех разделов новой учебной дисциплины должно включать лабораторные и практические занятия в оснащенных отечественными программно-аппаратными средствами учебно-исследовательских и учебно-производственных лабораториях.

Важным аспектом успешной реализации новой учебной дисциплины должны стать практико-ориентированные выпускные квалификационные работы студентов, а также трудоустройство выпускников на ведущие предприятия отрасли.

9.3. Меры нормативного регулирования.

Совершенствование нормативной базы, необходимой для реализации Стратегии, осуществляется поэтапно на основе действующего законодательства, с учетом приоритетов, установленных в доктринальных и программных документах.

На 1-м этапе (2022 год) необходима разработка следующих документов:

1) Распоряжение Правительства Российской Федерации об утверждении «Стратегии создания российского репозитория программных пакетов и библиотек, находящегося в юрисдикции и на территории Российской Федерации».

Данным Распоряжением утверждается также план мероприятий (дорожная карта) реализации Стратегии.

2) Распоряжение Правительства Российской Федерации по созданию Центра компетенций по поддержке деятельности Российского репозитория.

Данным Распоряжением утверждается статус, функции, полномочия, источники финансирования и другие вопросы, связанные с созданием и функционированием Центра компетенций.

2) приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации «Об утверждении требований к российскому репозиторию программных пакетов и библиотек, находящегося в юрисдикции и на территории Российской Федерации, и методики его проверки».

Приказ должен утвердить базовые требования к Российскому репозиторию, а также критерии и порядок проведения оценки соответствия репозиториев установленным требованиям.

3) приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации «Об установлении требований к программному обеспечению по уровням доверия».

Приказ должен утвердить уровни доверия к программному обеспечению и определить возможность его использования в установленных классах или категориях объектов защиты.

4) Перечень стандартов и методических материалов, связанных с процессами применения Российского репозитория.

В последующем (с 2022 года и далее) решение по совершенствованию нормативной правовой базы принимается в зависимости от достигнутого уровня развития и совершенствования российских репозиториев, расширения их возможностей, совершенствования механизмов применения, выбора путей дальнейшего развития системы российских репозиториев.