МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ВОПРОСАМ РАЗРАБОТКИ ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ С ИСПОЛЬЗОВАНИЕМ ПЛАТФОРМЫ «ГОСТЕХ» И ОПРЕДЕЛЕНИЯ ОБЯЗАТЕЛЬНОСТИ ПОВТОРНОГО ИСПОЛЬЗОВАНИЯ ЦИФРОВЫХ ПРОДУКТОВ ПЛАТФОРМЫ «ГОСТЕХ» ПРИ ИХ СОЗДАНИИ И РАЗВИТИИ

Версия 1.7

МОСКВА 2023

ОГЛАВЛЕНИЕ

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

Таблица 1 - Перечень сокращений

Сокращение	Полное наименование
API	Application Programming Interface (с англ. «программный интерфейс приложения») — набор способов и правил, по которым различные программы общаются между собой и обмениваются данными
DTO	Data Transfer Object (англ.) - один из шаблонов проектирования, используется для передачи данных между подсистемами приложения
IAM	Identity and Access Management (англ.) - система управления идентификацией и доступом к информационным ресурсам
RAID	Redundant Array of Independent Disks (англ.) - технология виртуализации данных для объединения нескольких физических дисковых устройств в логический модуль для повышения отказоустойчивости и производительности.
REST	Representational state transfer – это стиль архитектуры программного обеспечения для распределенных систем
RPO	Recovery Point Objective (англ.) — показатели точки восстановления. Допустимое время потери данных.
RTO	Recovery Time Objective (англ.) — показатель времени восстановления. Допустимое время восстановления данных
SLA	Service Level Agreement (англ.) — договор между заказчиком услуги и ее исполнителем, содержащий описание услуги, состав участников, их права и обязанности, а также согласованный уровень надёжности, доступности и производительности предоставления данной услуги.
UI	User interface (англ.) — пользовательский интерфейс
БД	База данных
ГЕОП	Государственная единая облачная платформа
ГИС, Система	Государственная информационная система
Госмаркет, ФГИС «Госмаркет»	Федеральная государственная информационная система «Госмаркет»
ГосСОПКА	Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации
ГОСТ	Государственный стандарт
ГЧП	Государственно-частное партнёрство
ЕПГУ	Федеральная государственная информационная система «Единый портал государственных и муниципальных услуг»
ЕСИА	Федеральная государственная информационная система «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме»
ИБ	Информационная безопасность
ИС	Информационная система

Сокращение	Полное наименование
ИТ	Информационные технологии
НКЦКИ	Национальный координационный центр по компьютерным инцидентам
НПА	Нормативный правовой акт
НСУД	Единая информационная платформа «Национальная система управления данными»
НФАП	Национальный фонд алгоритмов и программ
ПО	Программное обеспечение
Президиум Комиссии	Президиум Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности
РФ	Российская Федерация
СМЭВ	Система межведомственного электронного взаимодействия – единая система межведомственного электронного взаимодействия, положение о которой утверждено постановлением Правительства Российской Федерации от 8 сентября 2010 г. № 697 «О единой системе межведомственного электронного взаимодействия».
СУБД	Система управления базами данных
ТЗ	Техническое задание
ЦОД	Центр обработки данных
КИИ	Критическая информационная инфраструктура

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Используемые в настоящем документе термины и основные понятия области автоматизированных систем определены действующим законодательством и ГОСТ Р 59853-2021 «Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения». В настоящем документе применены следующие термины и определения, перечисленные в таблице ниже (см.Таблица 2).

Таблица 2 - Термины и определения

Обозначение	Описание
API	Application Programming Interface (с англ. «программный интерфейс приложения») — набор способов и правил, по которым различные программы общаются между собой и обмениваются данными
DTO	Data Transfer Object (англ.) - один из шаблонов проектирования, используется для передачи данных между подсистемами приложения
IAM	Identity and Access Management (англ.) - система управления идентификацией и доступом к информационным ресурсам

Обозначение	Описание
RAID	Redundant Array of Independent Disks (англ.) - технология виртуализации данных для объединения нескольких физических дисковых устройств в логический модуль для повышения отказоустойчивости и производительности.
REST	Representational state transfer – это стиль архитектуры программного обеспечения для распределенных систем
RPO	Recovery Point Objective (англ.) — показатели точки восстановления. Допустимое время потери данных.
RTO	Recovery Time Objective (англ.) — показатель времени восстановления. Допустимое время восстановления данных
SLA	Service Level Agreement (англ.) — договор между заказчиком услуги и ее исполнителем, содержащий описание услуги, состав участников, их права и обязанности, а также согласованный уровень надёжности, доступности и производительности предоставления данной услуги.
UI	User interface (англ.) — пользовательский интерфейс
ГИС на платформе «ГосТех»	Государственная информационная система, создаваемая, развиваемая, эксплуатируемая с использованием программно-аппаратной среды, цифровых продуктов, включенных в каталог цифровых продуктов платформы «ГосТех», а также инструментов, информационных технологий платформы «ГосТех»
Государственные органы и внебюджетные фонды	Федеральные органы исполнительной власти, государственные внебюджетные фонды, исполнительные органы субъектов Российской Федерации и иные государственные органы, образуемые в соответствии с законодательством Российской Федерации, законодательством субъектов Российской Федерации
Группа требований	Отдельные требования к системе (очереди системы) и реализуемые системой одна или несколько функций (задач, комплексов задач), указанные в техническом задании на создание системы (очереди системы)
Домен деятельности (Домен)	Область деятельности государственных органов, принадлежащая одной отрасли экономики и социальной сферы, имеющая общие сегменты (профили) физических или юридических лиц, формируемая с учетом клиентских путей. Домен объединяет участников (ведомства (органы государственной власти всех уровней) и юридические лица), выполняющих различные функции в одной области деятельности, лежащие на клиентских путях общего сегмента клиентов, обеспечивающие предоставление ценности для клиента с использованием набора сервисов и данных, присущих домену.
Дополнительный сервис платформы «ГосТех»	Цифровой продукт, реализующий дополнительные функциональные потребности, поставляемый в виде дистрибутива ПО, в виде прикладных сервисов, работающих в инфраструктуре облачных вычислений, и в виде исходного кода, включенного в государственную библиотеку типовых программных компонентов информационных систем, созданную в соответствии с постановлением Правительства Российской Федерации от 30 января 2013 г. № 62 «О национальном фонде алгоритмов и программ для электронных вычислительных машин»

Обозначение	Описание
ИТ-архитектура домена	Набор архитектурных представлений, включающий: • архитектуру информационных систем (программных средств) домена - архитектурное представление, описывающее набор информационных систем, их компонентов и сервисов в рамках одного домена деятельности, их взаимосвязи между собой, с внешней средой домена деятельности, с элементами архитектуры деятельности домена, а также принципы проектирования и развития домена деятельности; • информационную архитектуру домена – архитектурное представление, описывающее данные; • техническую архитектуру домена – архитектурное представление, описывающее сервисы обработки, хранения и коммуникаций ГИС (технические сервисы), которые необходимы для запуска функциональности ГИС, а также компоненты информационно-телекоммуникационной инфраструктуры, которые реализуют эти сервисы вычислительные ресурсы и средства защиты информации домена, их взаимосвязи между собой, с внешней средой домена, а также связи с элементами архитектуры информационных систем (программных средств) домена и архитектуры деятельности домена
Итерационный подход к разработке ГИС	Подход, основанный на выполнении необходимого числа итераций для поиска и реализации наиболее эффективных технических, эргономических и (или) технико-экономических решений по созданию системы (очереди системы)
Итерация	Совокупность работ, направленных на реализацию конкретной группы требований, предусмотренных этапами создания системы (очереди системы), начиная с этапа разработки или адаптации программного обеспечения и завершая этапом проведения опытной эксплуатации системы
Канал взаимодействия	Совокупность средств, методов и правил, обеспечивающих взаимодействие пользователя с ГИС
Кластер	Группа серверов, объединённых логически, способных обрабатывать идентичные запросы и использующихся как единый ресурс. Объединение серверов в один ресурс происходит на уровне программных протоколов
Компонент	Программа, рассматриваемая как единое целое, выполняющая законченную функцию и применяемая самостоятельно или в составе комплекса (ГОСТ 19.101-77 «Единая система программной документации. Виды программ и программных документов»)
Компонент Платформы	Структурный элемент Платформы, обеспечивающий реализацию части функционала для разработки цифровых продуктов на Платформе
Компонент программного обеспечения	Составная часть (программный модуль) программного обеспечения, выполняющая определенную функцию.
Конечный пользователь	Физические и юридические лица, а также иные лица, получающие государственные (муниципальные) услуги и (или) государственные (муниципальные) функции с использованием ГИС на платформе «ГосТех» или готовых облачных Сервисов на платформе «ГосТех»

Обозначение	Описание
Модель автоматизируемых процессов деятельности	Модель, представленная в виде совокупности графических объектов (их свойств, атрибутов) и отношений между ними или иных принятых условных обозначений, которая адекватно описывает процессы деятельности, подлежащие реализации с использованием информационной системы (информационных систем)
Модель архитектуры информационной системы	Модель, содержащая описание в виде совокупности принятых условных обозначений основных понятий или свойств информационной системы, воплощенной в ее элементах, отношениях и конкретных принципах ее проектирования и развития, и предназначенная для абстрактного (понятийного) отображения указанных свойств, элементов, отношений и принципов информационной системы.
Мультитенантность,	англ. Multi-Tenancy – «множественная аренда» – распределение физических или виртуальных ресурсов таким образом, что несколько арендаторов и их вычисления, и данные изолированы друг от друга и недоступны друг другу (ГОСТ ISO/IEC 17788-2016 «Информационные технологии. Облачные вычисления. Общие положения и терминология»).
Объект информатизации	Совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров.
Оператор ИС (ГИС)	Гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных
Оператор платформы «ГосТех»	Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации или подведомственное ему казенное учреждение
Очередь системы	Целевое состояние ГИС, для которого определен набор реализуемых системой функций и (или) задач
Платформа «ГосТех», Платформа	Цифровая экосистема создания, развития и эксплуатации государственных информационных систем, включающая в себя единую программно-аппаратную среду, цифровые продукты, информацию, информационные технологии, государственные информационные системы, необходимые для реализации функций платформы «ГосТех», а также совокупность нормативных правовых, организационных, методологических правил и процедур, обеспечивающих деятельность участников отношений, возникающих в связи с созданием и функционированием платформы «ГосТех»
Пользователи платформы «ГосТех»	Обеспечивающие создание, развитие, эксплуатацию государственных информационных систем на платформе «ГосТех» и (или) использование цифровых продуктов платформы «ГосТех» государственные органы и внебюджетные фонды, иные лица, уполномоченные в соответствии с нормативными правовыми актами Российской Федерации на осуществление мероприятий по созданию, развитию, эксплуатации государственных информационных систем

Обозначение	Описание
Пользовательский (клиентский) сегмент ГИС	Не входящие в состав платформы «ГосТех» объекты информатизации, принадлежащие на праве собственности или на ином законном основании пользователям платформы и применяемые ими для взаимодействия с ГИС на платформе «ГосТех». Пользовательский (клиентский) сегмент ГИС может включать в себя автоматизированные рабочие места пользователей, информационные системы, серверное оборудование, каналы связи, в том числе средства их обеспечения, а также помещения или объекты (здания, сооружения, технические средства), в которых эти средства и системы установлены.
Поставщики платформы «ГосТех»	Юридические или физические лица, в том числе зарегистрированные в качестве индивидуальных предпринимателей, предоставляющие цифровые продукты на платформе «ГосТех»
Программное обеспечение (ПО)	Совокупность программ для обработки информации и программных документов, необходимых для их эксплуатации
Программный сервис	Программное обеспечение, реализующее функциональные потребности, предназначенное для функционирования в отдельном процессе и взаимодействующее с другими программными сервисами и сторонними приложениями с использованием стандартизированных интерфейсов. Программные сервисы могут быть написаны на разных языках программирования и использовать разные технологии хранения данных.
Рабочий экземпляр программного обеспечения ГИС	Экземпляр программного обеспечения ГИС, подлежащий испытаниям.
Типовое решение	Предварительно сконфигурированный повторно используемый (переиспользуемый) цифровой продукт, доступный для использования при создании (развитии) ГИС с возможностью адаптации под прикладные задачи и функции, реализуемые ГИС.
Участники команды разработки	Представители пользователя платформы «ГосТех», а также представители поставщика (подрядчика, исполнителя), привлеченного пользователем платформы «ГосТех» к созданию, развитию, эксплуатации государственных информационных систем на платформе «ГосТех»
Цифровой продукт	Товары, работы, услуги, произведенные с использованием информационных технологий и доступные только в цифровом виде, в том числе средства защиты информации, инфраструктура облачных вычислений, программное обеспечение
Экземпляр	Установленный экземпляр ПО, обладающий собственным идентификатором и набором данных

1 Общие положения

1.1 Назначение и область применения документа

Настоящий документ содержит методические рекомендации по созданию (развитию) государственных информационных систем (далее – ГИС, системы(-а)) на платформе «ГосТех» с использованием цифровых продуктов платформы «ГосТех» (далее – методические рекомендации).

Положения методических рекомендаций распространяются на деятельность государственных органов и внебюджетных фондов, а также иных лиц, уполномоченных в соответствии с нормативными правовыми актами Российской Федерации на осуществление мероприятий по созданию, развитию, эксплуатации государственных информационных систем (далее – иные лица) на платформе «ГосТех».

Методические рекомендации могут использоваться органами местного самоуправления, государственными (муниципальными) предприятиями и учреждениями, государственными корпорациями, государственными компаниями, публично-правовыми компаниями, а также иными юридическими лицами, принимающими решения об использовании платформы «ГосТех» для реализации процессов жизненного цикла информационных систем.

Решение о реализации мероприятий по созданию (развитию) ГИС на платформе «ГосТех» осуществляется в соответствии с подпунктами б) и в) пункта 2 Указа Президента Российской Федерации от 31 марта 2023 года № 231 «О создании развитии и эксплуатации государственных информационных систем с использованием единой цифровой платформы Российской Федерации «ГосТех».

В случае принятия совместного решения публичного партнера и частного партнера, либо совместного решения концессионера и концедента о создании, развитии и эксплуатации государственных информационных систем, являющихся объектами соглашений о государственно-частном партнерстве, либо концессионных соглашений на платформе «ГосТех», также следует руководствоваться настоящими методическими рекомендациями.

Методические рекомендации не распространяются на государственные информационные системы, содержащие сведения, составляющие государственную тайну, служебную тайну в области обороны, тайну следствия и судопроизводства, сведения о лицах, в отношении которых в соответствии с федеральными законами от 20 апреля 1995 г. № 45-ФЗ «О государственной защите судей, должностных лиц правоохранительных и контролирующих органов», от 20 августа 2004 г. № 119-ФЗ «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства» и иными нормативными правовыми актами Российской Федерации принято

решение о применении мер государственной защиты, сведения о применяемых в отношении таких лиц мерах государственной защиты.

Создание, развитие, ввод в эксплуатацию, эксплуатация и вывод из эксплуатации государственных информационных систем на платформе «ГосТех» осуществляются в соответствии с требованиями к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации, утвержденными постановлением Правительства Российской Федерации от 6 июля 2015 г. № 676, с учетом особенностей, установленных Положением о платформе «ГосТех», утвержденным Постановлением Правительства Российской Федерации от 16 декабря 2022 г. № 2338.

Методические рекомендации предназначены, в том числе, для использования участниками платформы «ГосТех»:

а) регуляторами и координаторами процессов создания и функционирования платформы «ГосТех»;

б) участниками процессов функционирования платформы «ГосТех».

1.2 Цели разработки документа

Целями разработки методических рекомендаций являются:

а) обеспечение единства принципов создания, развития и эксплуатации ГИС на платформе «ГосТех» и определение обязательности использования (повторного использования) цифровых продуктов платформы «ГосТех»;

б) обеспечение взаимосвязанности и целостности методического обеспечения процессов проектирования, создания (развития), эксплуатации ГИС на платформе «ГосТех».

1.3 Нормативные ссылки

Методические рекомендации разработаны на основании документов, перечисленных в подразделах 1.3.1, 1.3.2, 1.3.3 настоящего документа:

1.3.1 Перечень ключевых нормативных правовых актов

Федеральный закон от 27 июня 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее – Федеральный закон № 149-ФЗ).

Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

Указ Президента Российской Федерации от 31 марта 2023 г. № 231 «О создании развитии и эксплуатации государственных информационных систем

с использованием единой цифровой платформы Российской Федерации «ГосТех».

Указ Президента Российской Федерации от 30 марта 2022 г. № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации», в частности в сфере импортозамещения, технологической независимости Российской Федерации и информационной безопасности.

Постановление Правительства Российской Федерации от 16 декабря 2022 г. № 2338 «Об утверждении Положения о единой цифровой платформе Российской Федерации «ГосТех», о внесении изменений в постановление Правительства Российской Федерации от 6 июля 2015 г. № 676 и признании утратившим силу пункта 6 изменений, которые вносятся в требования к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации, утвержденных постановлением Правительства Российской Федерации от 11 мая 2017 г. № 555» (далее – Положение).

Постановление Правительства Российской Федерации от 06 июля 2015 г. № 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» (далее — Постановление № 676).

Постановление Правительства Российской Федерации от 16 ноября 2015 г. № 1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд (с изменениями и дополнениями)».

Постановление Правительства Российской Федерации от 30 января 2013 г. № 62 «О национальном фонде алгоритмов и программ для электронных вычислительных машин» (далее – Постановление № 62).

Распоряжение Правительства Российской Федерации от 21 октября 2022 г. № 3102-р «Об утверждении Концепции создания и функционирования единой цифровой платформы Российской Федерации «ГосТех», плана мероприятий («дорожной карты») по созданию единой цифровой платформы Российской Федерации «ГосТех».

Приказ ФСБ России от 24 октября 2022 № 524 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, с использованием шифровальных (криптографических) средств».

Приказ ФСБ России от 10 июля 2014 г. № 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 ФСБ России от 13 февраля 2023 г. № 77 «Об утверждении порядка взаимодействия операторов с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, включая информирование ФСБ России о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных».

Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (далее – Приказ ФСТЭК России №17).

Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

Приказ ФСТЭК России от 29 апреля 2021 г. № 77 «Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну».

Приказ ФСТЭК России от 21 декабря 2017 года № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования».

Приказ ФСТЭК России от 25 декабря 2017 года № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

Приказ ФСТЭК России от 3 апреля 2018 г. № 55 «Об утверждении Положения о системе сертификации средств защиты информации».

Приказ Минцифры России от 23 июля 2021 г. № 761 «О формировании и ведении единого реестра российских программ для электронных вычислительных машин и баз данных и единого реестра программ для электронных вычислительных машин и баз данных из государств - членов Евразийского экономического союза, за исключением Российской Федерации».

1.3.2 Технические стандарты

ГОСТ-Р 56939-2016 Государственный стандарт Российской Федерации, Защита информации. Разработка безопасного программного обеспечения. Общие требования.

ГОСТ-Р 58412-2019 Государственный стандарт Российской Федерации, Защита информации. Разработка безопасного программного обеспечения. Угрозы безопасности информации при разработке программного обеспечения.

ГОСТ РВ 51987-2002 Информационная технология. Комплекс стандартов на АС. Типовые требования и показатели качества функционирования информационных систем.

ГОСТ 70186-2022 Интернет-ресурсы и другая информация, представленная в электронно-цифровой форме. Инструменты разработки цифрового контента. Требования доступности для людей с инвалидностью и иных лиц с ограничениями жизнедеятельности.

1.3.3 Методические рекомендации

Методические рекомендации по проектированию целевой архитектуры домена в рамках перехода государства на единую цифровую платформу Российской Федерации «ГосТех», утверждённые Протоколом заочного голосования членов президиума Комиссии от 13 июля 2022 г. №26.

Методические рекомендации по организации производственного процесса разработки государственных информационных систем с учётом применения итерационного подхода к разработке, утвержденные Протоколом заочного голосования членов президиума Комиссии от 13 июля 2022 г. №26.

Методические рекомендации по проектированию интерфейсов систем управления для государственных сервисов, утверждённые Протоколом заочного голосования членов президиума Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности от 17 августа 2022г. № 31.

Методические рекомендации по проектированию интерфейсов государственной услуги или государственной функции на едином портале государственных услуг, утверждённые Протоколом заочного голосования членов президиума Комиссии от 17 августа 2022 г. № 31.

Методические рекомендации «Базовые сервисы Единой цифровой платформы Российской Федерации «ГосТех». Основные требования к составу и функциям», утверждённые Протоколом заочного голосования членов президиума Комиссии от 5 августа 2022 г. № 30.

Методические рекомендации по включению сервисов в единую цифровую платформу Российской Федерации «ГосТех», утверждённые Протоколом заочного голосования членов президиума Комиссии от 5 августа 2022 г. №30.

Методические рекомендации по эксплуатации государственных информационных систем на единой цифровой платформе Российской Федерации «ГосТех», утверждённые Протоколом заочного голосования членов президиума Комиссии от 8 декабря 2022 г. №54.

Методические рекомендации по оценке целесообразности создания и развития государственных информационных систем на единой цифровой платформе Российской Федерации «ГосТех», утверждённые Протоколом заочного голосования членов президиума Комиссии от 4 мая 2023 г. №20.

Методика оценки угроз безопасности информации, утвержденная ФСТЭК России от 5 февраля 2021 года.

Меры защиты информации в государственных информационных системах, утвержденные ФСТЭК России 11 февраля 2014 года.

Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности», утвержденные ФСБ России от 31 марта 2015 г. (№ 149/7/2/6-432).

1.4 Основные понятия

В целях обеспечения комплексного подхода к реализации мероприятий, связанных с созданием, развитием и функционированием ГИС на платформе «ГосТех», определен состав участников отношений, возникающих в связи с созданием (развитием) и функционированием ГИС на платформе «ГосТех»:

а) регуляторы и координаторы процессов создания и функционирования платформы «ГосТех»;

б) участники процессов функционирования платформы «ГосТех».

Регуляторами и координаторами процессов создания и функционирования платформы «ГосТех» являются:

а) президиум Комиссии;

б) межведомственная рабочая группа по архитектуре базовых информационных ресурсов и принципам обработки данных;

в) Минцифры России;

г) федеральный орган исполнительной власти в области обеспечения безопасности;

д) федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации.

В рамках реализации мероприятий, необходимых для создания и развития ГИС на платформе «ГосТех», в случае утверждения регламентов взаимодействия Минцифры России с государственными органами и внебюджетными фондами, выступающими в качестве функциональных заказчиков (далее - функциональные заказчики) Минцифры России может выступать в качестве технического заказчика (далее – технических заказчик).

Участниками процессов функционирования платформы «ГосТех» являются:

а) оператор платформы «ГосТех»;

б) оператор ФГИС «Управление платформой «ГосТех»;

в) оператор ФГИС «Госмаркет»;

г) пользователи платформы «ГосТех»;

д) участники команд разработки;

е) поставщики цифровых продуктов платформы «ГосТех».

Состав мероприятий, реализуемых в ходе создания, развития, эксплуатации ГИС на платформе «ГосТех» представлен в виде типовой модели. Типовая модель определяет порядок стадий, особенности решаемых задач в рамках стадии, их обязательность. Каждая стадия, в свою очередь включает в себя типовые мероприятия, имеющие специфические характеристики и задачи, раскрытые в соответствующих пунктах раздела 2 настоящих методических рекомендаций, приведенные в таблице ниже (см. Таблица 3).

Таблица 3 – Типовые мероприятия модели создания, развития и эксплуатации ГИС на платформе «ГосТех»

№	Наименование стадии	Пункт МР	Пункт постановления 676
1	2	3	4
1. Подготовка к созданию			
1.1	Определение необходимости и целесообразности создания (развития) ГИС на платформе «ГосТех»	2.1.1	II 2[1]
1.2	Определение связи ГИС с архитектурой домена деятельности	2.1.2	
1.3	Концептуальное проектирование создания (развития) ГИС на платформе «ГосТех»	2.1.3	
2. Разработка требований			
2.1	Разработка требований к созданию (развитию) ГИС	2.2	II 3
3. Техническое проектирование			
3.1	Архитектура деятельности	2.3.1	II а)
3.2	Проектирование ИТ-архитектуры ГИС	2.3.2	
4. Разработка или адаптация ПО и документации на систему			
4.1	Разработка и (или) адаптация программного обеспечения	2.4	II б)
5. Ввод в эксплуатацию			
5.1	Проведение предварительных испытаний системы	2.5.1	II д)
5.2	Опытная эксплуатация	2.5.1	II е)

№	Наименование стадии	Пункт МР	Пункт постановления 676
1	2	3	4
5.3	Проведение приемочных испытаний	2.5.1	II ж)
5.4	Аттестация ГИС по требованиям защиты информации	2.5	III
6. Эксплуатация			
6.1	Ввод в эксплуатацию	2.5	III
6.2	Эксплуатация	2.6	V
6.3	Вывод из эксплуатации	2.7	VI

П р и м е ч а н и е – в таблице выше приводятся:

в графе 3 – пункт настоящих рекомендаций, в котором раскрывается содержание соответствующего мероприятия;

в графе 4 – соответствующий мероприятию этап реализации, предусмотренный Постановлением № 676:

II 2^1 – разработка Концепции системы

II 3 – разработка технического задания на создание системы (очереди системы)

II а) – создание системы, этап «Разработка документации на систему и ее части»;

II б) – создание системы, этап «Разработка или адаптация программного обеспечения, разработка рабочей документации»;

II г) – создание системы, этап «Пусконаладочные работы»;

II д) – создание системы, этап «Проведение предварительных испытаний системы»;

II е) – создание системы, этап «Проведение опытной эксплуатации системы»;

II ж) – создание системы, этап «Проведение приемочных испытаний системы»;

III – ввод системы в эксплуатацию;

IV – развитие системы;

V – эксплуатации системы.

В зависимости от выбранного способа создания системы мероприятия, соответствующие этапам II б) - II е) указанные в строках 4.1-5.2 таблицы 3 для очереди системы осуществляются:

– при последовательном подходе к разработке – только последовательно;

– при итерационном подходе к разработке – последовательно или последовательно-параллельно.

В соответствии с подпунктом б) пункта 19 Положения обеспечение реализации мероприятий, необходимых для создания (развития) ГИС на платформе «ГосТех» в качестве технического заказчика может осуществлять Минцифры России, в качестве функционального заказчика может выступать государственный орган или внебюджетных фонд. Описание действий, выполняемых участниками отношений, возникающих в связи с созданием и функционированием ГИС на платформе «ГосТех», в случае когда техническим заказчиком выступает Минцифры России, а функциональным заказчиком государственный орган или внебюджетный фонд, приведено в Приложении 1.

Описание действий, выполняемых участниками отношений, возникающих в связи с обеспечением реализации мероприятий, необходимых для создания и функционирования ГИС на платформе «ГосТех», в случае, когда

государственный орган или внебюджетный фонд обеспечивает создание (развитие) ГИС самостоятельно, приведено в Приложении 2.

1.5 Цифровые продукты платформы «ГосТех»

Цифровые продукты платформы «ГосТех» предназначены для создания, развития и эксплуатации ГИС на платформе «ГосТех». К цифровым продуктам платформы «ГосТех» относятся:

– цифровые продукты, предоставляющие инфраструктурные вычислительные ресурсы и сервисы, и обеспечивающие информационно-технологическое взаимодействие с инфраструктурой электронного правительства (далее - инфраструктурные технологические сервисы), в том числе предоставляемые посредством государственной единой облачной платформы;

– цифровые продукты, предоставляющие базовый набор сервисов платформы «ГосТех», включающие в себя в том числе сервисы конфигурирования, аудита событий безопасности, журналирования, сбора метрик, управления учетными записями пользователей, управления базами данных различных типов, интеграционного взаимодействия и управления очередями сообщений, сервисы управления микросервисами и процессами, сервисы интеграции с инфраструктурой электронного правительства (далее - базовые сервисы платформы «ГосТех»);

– цифровые продукты, реализующие дополнительные функциональные потребности, поставляемые в виде дистрибутивов программного обеспечения, прикладных сервисов, работающих в инфраструктуре облачных вычислений, и в виде исходного кода, включенного в государственную библиотеку типовых программных компонентов информационных систем, созданную в соответствии с Постановлением №62 (далее - дополнительные сервисы платформы «ГосТех»);

– цифровые продукты и программно-аппаратные комплексы, обеспечивающие функции защиты информации, включающие в том числе сервисы обнаружения и блокирования сетевых атак.

2 Описание требований к реализации стадий создания (развития) ГИС на платформе «ГосТех»

Состав основных стадий типовой модели создания (развития) ГИС на платформе «ГосТех» включает:

- подготовку к созданию;
- разработку требований;
- проектирование;
- разработку или адаптацию ПО и документации на систему;

– ввод в эксплуатацию;
– эксплуатацию;
– вывод из эксплуатации.

2.1 Подготовка к созданию ГИС

На этапе подготовки к созданию ГИС необходимо заключить соглашение о распределении ответственности при создании, развитии, эксплуатации ГИС на ЕЦП «ГосТех».

2.1.1 Определение необходимости и целесообразности создания (развития), эксплуатации ГИС на платформе

В соответствии с п. 7 Положения целесообразность и обязательность создания и развития ГИС на платформе «ГосТех» определяются по результатам оценки экономической и (или) технологической целесообразности их создания и развития на платформе «ГосТех» для соответствующей государственной информационной системы. На этапе подготовки к созданию ГИС государственный орган или внебюджетный фонд выполняет оценку целесообразности создания (развития) и эксплуатации ГИС на платформе «ГосТех» в соответствии с методическими рекомендации по оценке целесообразности создания и развития государственных информационных систем на единой цифровой платформе Российской Федерации «ГосТех», утверждаемыми президиумом Комиссии.

2.1.2 Определение связи ГИС с архитектурой домена деятельности

В случае наличия описания домена деятельности (или нескольких), связанных с деятельностью, автоматизируемой создаваемой (развиваемой) ГИС, необходимо определить связь создаваемой (развиваемой) ГИС с доменом (или несколькими доменами) деятельности. Связь ГИС с доменом определяется и описывается в части основных категорий:

– участники домена;
– функциональные области домена;
– клиенты домена;
– жизненные ситуации;
– потребности клиентов;
– клиентский путь;
– связь с ИТ-архитектурой домена.

Должны быть определены участники домена (или нескольких доменов): органы власти на различных уровнях управления и юридические лица, участвующие в предоставлении соответствующих услуг (функций) в домене.

Функциональные области - группа функций, направленных на обеспечение различных этапов/стадий одного процесса, в результате которого предоставляется конечная ценность для пользователя. Для создаваемой

(развиваемой) ГИС должны быть указаны функциональные области домена, цифровизацию которых будет обеспечивать ГИС.

Для создаваемой (развиваемой) ГИС должны быть определены пользователи домена, для которых предоставляются сервисы ГИС, указаны их жизненные ситуации и соответствующие потребности, обеспечиваемые сервисами ГИС.

Клиентские пути домена (при их наличии) должны быть учтены при проработке клиентских путей пользователя, создаваемой ГИС.

Необходимо обеспечить совместимость и соответствие архитектуры создаваемой (развиваемой) ГИС ИТ-архитектуре домена, в части: верхнеуровневой функциональной архитектуры домена, концептуальной модели данных домена, профилей ключевых клиентов домена, архитектуры данных, интеграционной архитектуры домена.

Основные понятия домена и описание его структуры приведены в документе «Методические рекомендации по проектированию и утверждению целевой архитектуры домена с использованием единой цифровой платформы «ГосТех», утверждаемых президиумом Комиссии.

2.1.3 Концептуальное проектирование создания (развития) ГИС на платформе «ГосТех»

Концептуальное проектирование создания (развития) ГИС включает исследование современных информационно-коммуникационных технологий построения информационных систем аналогичного назначения, используемых архитектурных, системных и технических решений, разработку мероприятий необходимых для создания (развития) ГИС, а также технико-экономическое обоснование предельных лимитов стоимости мероприятий по созданию (развитию) ГИС.

Результатом концептуального проектирования является документ концепция создания (развития) ГИС на платформе «ГосТех» (далее – Концепция), разрабатываемая в соответствии с п.2[1] Постановления № 676. Концепция должна описывать роль и место создаваемой (развиваемой) ГИС, обосновывает необходимость создания (развития) ГИС, определяет цели, задачи и принципы ее создания, дает общее представление об ожидаемых результатах, которые достигаются в результате создания (развития) ГИС.

Концепция создания ГИС является обязательным документом технической документации на систему. Необходимость разработки концепции развития ГИС, определяется оператором ГИС или иным лицом, на которое возложены полномочия по развитию системы.

Основные положения, которые следует отразить в Концепции:

а) основания создания (развития) ГИС;

б) цели, задачи и показатели результативности создания ГИС;

в) описание и обоснование варианта построения ГИС;

г) описание подсистемы защиты информации;

д) условия и мероприятия по созданию системы;

е) оценка финансовых, материальных и трудовых ресурсов.

Цели создания (развития) ГИС рекомендуется формулировать в соответствии с направлениями деятельности государственного органа в рамках осуществляемых им полномочий по выполнению государственных функций, услуг, контрольно-надзорной деятельности, иных услуг и функций, предоставляемых конечным пользователям в цифровом виде. Рекомендуется установить значения для всех целевых показателей, имеющих количественное измерение.

При формировании Концепции следует выделить группы показателей, отражающих различные аспекты влияния на функционирование ГИС, государственного органа и (или) конечных пользователей системы.

В Концепции следует привести описание варианта построения ГИС с использованием возможностей, предоставляемые цифровыми продуктами и типовыми решениями платформы «ГосТех». Для описания варианта построения ГИС рекомендуется сформировать контекстное представление, которое содержит высокоуровневое описание взаимодействий системы с внешними системами и группами пользователей.

Контекстное представление описывает контекстная диаграмма, которая дает представление границ взаимодействия ГИС. На диаграмме указываются:

а) пользователи с разделением категорий на внутренних и внешних по отношению к рассматриваемой системе;

б) интеграционные связи (в особенности в части средств межведомственного взаимодействия, способы идентификации и авторизации), в том числе с другими ГИС;

в) наличие публичного API, публичных витрин данных, сайта с неограниченным кругом пользователей;

г) компоненты, обеспечивающие аутентификацию и авторизацию;

д) указаны функциональные блоки ГИС;

е) определены ЦОД, в которых размещается ГИС, или требования к вычислительной инфраструктуре.

В Концепции необходимо привести результаты предварительной классификации системы в соответствии с требованиями о защите информации и указать: предполагаемые класс защищенности ГИС в соответствии с Приказом ФСТЭК России № 17, уровень защищенности персональных данных в соответствии с Постановлением Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в

информационных системах персональных данных», категорию значимости объекта КИИ соответствии с Постановлением № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений», класс информационной системы общего пользования в соответствии с приказами ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489 «Об утверждении Требований о защите информации, содержащейся в информационных системах общего пользования».

В Концепции следует определить способ создания системы: последовательный или с применением итерационного подхода к разработке системы, а также привести описание всех очередей создания (развития) системы (в случае ввода ГИС в эксплуатацию очередями).

Оценку финансовых, материальных и трудовых ресурсов следует предоставлять в виде технико-экономического обоснования выполнения работ по созданию (развитию) ГИС (далее - технико-экономическое обоснование, ТЭО). ТЭО является обязательным приложением к Концепции в соответствии с пунктом 2^1 Постановления № 676. ТЭО предназначено для обоснования технико-экономической целесообразности создания (развития) ГИС, а также содержит оценку финансовых, трудовых и материальных ресурсов, необходимых для реализации требований к системе, включая требования к информационной системе (подсистеме) защиты информации, с учетом сценария создания (развития) и эксплуатации ГИС на платформе «ГосТех».

Предварительную оценку предоставления базовых сервисов платформы «ГосТех» с учетом стоимости инфраструктуры, необходимой для разработки, тестирования и эксплуатации ГИС возможно выполнить с пользованием калькулятора, размещенного на официальном сайте ФКУ «ГосТех»: https://market.platform.gov.ru/. Для получения доступа к калькулятору необходимо отправить запрос официальным письмом включающий следующую информацию: название организации, ИНН, ОГРН, ФИО, должность, контактный телефон и адрес электронной почты, на который будут высланы учётные данные для доступа.

На основе результатов концептуального проектирования формируются требования к ГИС, а также обеспечиваются единый контекст и взаимосвязь результатов реализации требований к ГИС на последующих стадиях ее жизненного цикла, в том числе при разработке технического задания на создание (развитие) ГИС.

2.2 Разработка требований к созданию (развитию) ГИС

На этапе разработки требований к создаваемой (развиваемой) ГИС выполняется проработка требований к функциям, выполняемым ГИС, которые фиксируются в техническом задании на создание (развитие) ГИС (далее - ТЗ).

ТЗ на систему разрабатывается согласно Концепции создания (развития) системы (в случае ее наличия) и в соответствии с классификацией системы в соответствии с требованиями о защите информации.

В дополнение к техническому заданию на создание (развитие) системы может быть разработано частное техническое задание на систему в целом или на отдельные ее части, детализирующее требования, утвержденные ранее в техническом задании. Кроме того, требования к системе могут быть уточнены в функционально-технических требованиях на отдельные компоненты системы или создаваемые сервисы ГИС.

2.3 Техническое проектирование

В соответствии с п.6 Постановления № 676 этап разработки документации на систему и ее части включает разработку, согласование и утверждение технической документации в объеме, необходимом для описания полной совокупности проектных решений (в том числе по защите информации) и достаточном для дальнейшего выполнения работ по созданию системы, в том числе описания проектных решений по процессам деятельности, реализуемым посредством системы, решений по архитектуре системы, решений по содержанию, структуре и ограничениям целостности, используемых для создания базы данных системы.

В соответствии с п 5^1 Постановления № 676 техническая документация должна содержать описание автоматизируемых процессов деятельности, архитектуры системы и базы данных системы, которое создается по результатам моделирования.

На этапе технического проектирования рекомендуется разработать модель архитектуры информационной системы. Модель архитектуры системы проектируется с использованием архитектурных представлений.

Архитектурное представление определяет основные решения по построению ГИС, отображает декомпозицию архитектуры ГИС на составляющие ее компоненты в соответствии с установленными шаблонами описания элементов и взаимосвязей. Рекомендуемый состав представлений модели архитектуры системы включает:

а) архитектуру деятельности;

б) программную архитектуру;

в) интеграционную архитектуру;

е) технологическую архитектуру.

д) архитектуру информационной безопасности;

Техническое проектирование ГИС на платформе «ГосТех» должно учитывать положения следующих документов, утверждаемых президиумом Комиссии:

– «Методические рекомендации по проектированию интерфейсов государственной услуги или государственной функции на едином портале государственных услуг»;

– «Методические рекомендации по проектированию интерфейсов систем управления для государственных сервисов».

2.3.1 Архитектура деятельности

Архитектура деятельности – описывает процессную обработку элементов и последовательную организацию отдельных этапов процессов в структуры, изображающие комплексные процессы, отражающие их логическую связь и взаимозависимость. Архитектура деятельности строится на описании вариантов использования системы и реализуемых ею процессов деятельности.

Вариант использования системы описывает функциональность, реализуемую системой, в виде сценария взаимодействия пользователя с системой. Вариант использования описывается моделью (или несколькими моделями), визуализируемой диаграммой. Для варианта использования может быть разработана диаграмма последовательности, детализирующая поток событий варианта использования с точки зрения пользователей системы. В описании диаграммы последовательности указываются связанные варианты использования.

Описание проектных решений по процессам деятельности рекомендуется выполнять с помощью модели(-ей) автоматизируемых процессов деятельности. В модели автоматизируемого процесса деятельности рекомендуется определить его окружение: организационно-штатные и/или ролевые элементы, подпроцессы/функции, информационные/документарные сущности (артефакты). Модель(-и) автоматизируемого процесса деятельности, как правило, являются детализацией и логическим продолжением вариантов использования ГИС. Модели автоматизируемого процесса рекомендуется разрабатывать в нотации BPMN 2.0 или Archimate.

Для систематизации моделей автоматизируемых процессов деятельности может быть сформировано представление процессов, которое детализирует происходящие в системе процессы и связи между ними.

При описании архитектуры деятельности рекомендуется провести обследование процессов и процедур, автоматизированная поддержка которых будет обеспечиваться в рамках создания (развития) системы,

а также сформированы предложения по оптимизации процессов и процедур с учетом спроектированных клиентских путей домена деятельности (при наличии).

2.3.2 Проектирование ИТ-архитектуры ГИС

2.3.2.1 Программная архитектура

Программная архитектура включает описание основной организации программного обеспечения системы, воплощенную в ее компонентах, их взаимоотношениях друг с другом и со средой окружения.

Проектирование программной архитектуры необходимо осуществлять с учетом положений методических рекомендаций по обеспечению безопасности при разработке программного обеспечения с использованием компонентов Единой цифровой платформы «ГосТех», утвержденных президиумом Комиссии.

Проектирование архитектуры должно строиться с использованием микросервисного подхода к проектированию программной архитектуры.

В ходе проектирования программной архитектуры необходимо использовать возможности, предоставляемые цифровыми продуктами платформы «ГосТех», а также типовые решения платформы «ГосТех».

Программная архитектура ГИС должна учитывать:

– поддержку технологий виртуализации и контейнеризации, используемых в составе платформы «ГосТех»;

– совместимость не менее чем с одной из операционных систем (ОС), систем управления базами данных (СУБД), используемых в составе платформы «ГосТех».

Техническое проектирование должно ориентироваться на реализацию показателей назначения ГИС, определенных в Концепции, ТЗ на создание (развитие) ГИС, а также показатели мероприятия по информатизации, определенные в ведомственной программе цифровой трансформации (при наличии).

Описание программной архитектуры может включать несколько представлений:

а) логическое представление – сфокусировано на функциональности, предоставляемой системой для конечных пользователей. В этом представлении используются компонентные диаграммы, диаграммы классов, связей и последовательностей.

б) физическое представление – показывает распределение компонентов программного обеспечения по физическим уровням и физические каналы связи между уровнями. Представление физической структуры системы может быть описано с помощью диаграммы развёртывания.

в) представление данных – включает описание состава сведений, подлежащих размещению в системе, информационные потоки (как внутри системы, так и связи с внешними источниками).

Описание решений, построенных с использованием базовых сервисов приведено в разделе 3 настоящего документа. Решения следует применять в соответствии с условиями и задачами, решаемыми путем создания (развития) ГИС.

2.3.2.2 Интеграционная архитектура

Интеграционная архитектура системы – комплекс программных компонентов, обеспечивающих информационный обмен между различными компонентами системы, а также унификацию, стандартизацию и безопасность этого обмена, в том числе реализующие взаимодействие ГИС с внешними и смежными системами. Описание интеграционной архитектуры может включать описание решений по использованию:

а) компонентов инфраструктуры электронного правительства;

б) программных сервисов, обеспечивающих взаимодействие внутренних компонентов системы между собой;

в) программных сервисов, обеспечивающих взаимодействие с внешними системами.

Приоритетным решением по построению асинхронной коммуникации между программными компонентами ГИС и внешних систем должно быть использование подходов событийно-ориентированной архитектуры.

Обеспечение снижения связности между компонентами ПО при их взаимодействии может быть достигнуто путем использования брокеров сообщений. Рекомендуется применять решение по созданию высокодоступной и высоконадежной системы обмена сообщениями с использованием базового сервиса платформы «ГосТех» «Сервис управления очередями сообщений». Для обеспечения доступности и надежности брокеры организуются в кластеры.

Интеграционное решение, позволяющее системам обмениваться большим количеством событий в режиме реального времени с высокой доступностью и пропускной способностью, может обеспечиваться с помощью сервиса интеграционного взаимодействия.

Интеграцию системы с Единой системой идентификации и аутентификации рекомендуется выполнять с использованием сервиса IAM.

Описание решений с использованием интеграционных сервисов платформы «ГосТех» приведено в разделе 3.

2.3.2.3 Технологическая архитектура

Технологическая архитектура содержит описание структуры и логики построения системного, платформенного программного обеспечения и

аппаратной среды, обеспечивающих работу системы. Построение технологической архитектуры осуществляется с использованием инфраструктурных технологических сервисов платформы «ГосТех».

В случае обоснованного использования ЦОД, не относящегося к платформе «ГосТех», параметры ЦОД, в котором размещается ГИС, должны соответствовать:

а) требованиям ГОСТ Р 70139-2022 для ЦОД класса ГИС-3;
б) параметрам отказоустойчивости и катастрофоустойчивости с учетом требований Приказа Минцифры России от 1 июня 2023 г. № 500 «Об утверждении критериев оценки отказоустойчивости и катастрофоустойчивости инфраструктуры платформы «ГосТех»;
в) требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах (утв. приказом ФСТЭК России от 11 февраля 2013 г. №17) по классу защищенности не ниже класса защищенности размещаемых на нем информационных систем.

Для описания технологической архитектуры должна быть разработана диаграмма развертывания или набор архитектурных представлений, включающих указание:

– используемых сервисы платформы «ГосТех»;
– функциональных блоков (компонентов) ГИС,
– функциональности/назначения контейнеров и используемые технологии,
– используемых программных продуктов и их версии (например, ClickHouse X.XX.XXX) для единиц развертывания ПО;
– интеграционные связи и протоколы для интеграционного взаимодействия;
– режимов развертывания контейнеров - в среде управления микросервисами (Kubernetes) или на виртуальных машинах;
– инфраструктуры (ЦОД, в которых размещается ГИС), в том числе количество узлов кластера (Server Node), если используется.

Описание решений по обеспечению доступности, отказоустойчивости, масштабируемости системы с использованием инфраструктурных технологических сервисов платформы «ГосТех» приведено в разделе 3.

2.3.2.4 Архитектура информационной безопасности

Проектирование архитектуры информационной безопасности ГИС осуществляется с использованием следующих документов:

– Концепция обеспечения информационной безопасности единой цифровой платформы Российской Федерации «ГосТех» (утв. приказом Минцифры России от 12 января 2023 г. № 7);

– Концепция разработки безопасного программного обеспечения на единой цифровой платформе Российской Федерации "ГосТех", утвержденная Протоколом заочного голосования членов президиума Комиссии от 4 мая 2023 г. №20;

– Методические рекомендации по обеспечению безопасности при разработке программного обеспечения с использованием компонентов Единой цифровой платформы «ГосТех», утверждаемые президиумом Комиссии;

– Концепция обнаружения, предупреждения, ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, связанные с информационными ресурсами платформы «ГосТех», а также порядка, определяющего зону ответственности и взаимодействие НКЦКИ, Минцифры России, центров ГосСОПКА, владельцев ГИС, утверждаемая президиумом Комиссии;

– Методические рекомендации по предъявлению требований к поставщикам вычислительной инфраструктуры и облачных платформ, утверждаемые президиумом Комиссии;

– Политика информационной безопасности Единой цифровой платформы «ГосТех», утверждаемые президиумом Комиссии;

– Типовая модель угроз и нарушителя безопасности информации для доменов и ГИС при развертывании на платформе «ГосТех» в мультитенантном исполнении (предоставляется оператором платформы по запросу);

– Модель угроз и нарушителя безопасности информации платформы «ГосТех» в мультитенантном исполнении (предоставляется оператором платформы по запросу);

– Методические рекомендации по организации и проведению работ по аттестации государственных информационных систем на единой цифровой платформе Российской Федерации «ГосТех» на соответствие требованиям по защите информации, утверждаемые президиумом Комиссии.

Проектирование архитектуры информационной безопасности должно осуществляться с учетом архитектуры комплексной системы защиты информации платформы «ГосТех» и предоставляемых платформой средств защиты информации.

При проектировании также необходимо учитывать, что автоматизированные рабочие места пользователей (далее – АРМ) ГИС на платформе «ГосТех» (включая привилегированных), размещённые на пользовательских площадках

(пользовательский (клиентский) сегмент ГИС), по умолчанию рассматриваются как внешние информационные системы. Таким образом, в отношении указанных АРМ должна быть реализована мера защиты информации УПД.16 (управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы) с учетом требований к усилению, приведённых в Методическом документе «Меры защиты информации в государственных информационных системах» (утв. ФСТЭК России 11 февраля 2014 г.).

Требования к защите пользовательского (клиентского) сегмента ГИС и порядок оценки эффективности принимаемых мер по защите информации в пользовательских сегментах ГИС определены в документе «Требования по защите пользовательского сегмента ГИС, размещаемых на платформе «ГосТех».

Механизмы идентификации и аутентификации, применяемые в ГИС на платформе «ГосТех», должны быть реализованы в том числе с применением Сервиса IAM (Identity and Access Management) единой цифровой платформы Российской Федерации «ГосТех» с использованием учетных записей ЕСИА.

Мандатный метод управления доступом при использовании Сервиса IAM платформы «ГосТех» недоступен, поскольку платформа «ГосТех» не предназначена для обработки информации, составляющей государственную тайну.

В рамках этапа проектирования архитектуры информационной безопасности осуществляется, в том числе, определение угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в ГИС на платформе «ГосТех», и разработка на их основе модели угроз безопасности информации, а также модели нарушителя информационной безопасности, подлежащие согласованию с федеральным органом исполнительной власти в области обеспечения безопасности и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий в части, касающейся выполнения установленных требований о защите информации. На этапе проектирования разрабатывается проектная документация, включая технический проект на систему защиты информации ГИС на платформе «ГосТех».

Определение класса средств криптографической защиты информации осуществляется на основании данных, содержащихся в согласованных с ФСБ и ФСТЭК России модели угроз безопасности информации, а также модели нарушителя информационной безопасности, рассматриваемых в совокупности.

2.4 Разработка или адаптация программного обеспечения ГИС, разработка документации

Разработка или адаптация программного обеспечения ГИС, создаваемой (развиваемой) на платформе «ГосТех» выполняется с использованием платформы для создания, развития и эксплуатации прикладного программного обеспечения для единой цифровой платформы Российской Федерации «ГосТех» (далее - платформа разработки) с применением методических рекомендаций по организации производственного процесса разработки государственных информационных систем с учетом применения итерационного подхода к разработке, утверждаемых президиумом Комиссии.

Платформа разработки предназначена для организации производственного и технологического процесса разработки программного обеспечения при создании (развитии) ГИС и их компонентов на платформе «ГосТех», в том числе для разработки и подключения новых каналов обслуживания граждан, организаций и органов власти с использованием облачных технологий и обеспечением безопасности информации и масштабируемости.

Основным назначением платформы разработки является автоматизация технологических аспектов жизненного цикла приложений, разработанных на платформе, а именно: непрерывное внедрение изменений без приостановки обслуживания, защита от сбоев вследствие влияния человеческого фактора; мониторинг состояния системы, локализация корневых причин проблем и инцидентов; корректная работа и целостность данных при отказе инфраструктурных элементов, отказе интеграций, аномальных всплесках нагрузки; линейное масштабирование приложений; изоляция разных потребителей по взаимовлиянию; централизованное управление поведением приложений; набор инструментов, автоматизирующих штатные операции разработчиков приложений на платформе; моделирование и выполнение пользовательских сценариев и бизнес-процессов.

Разработка ПО ГИС производится с использованием высокоуровневых языков программирования, указанных в методических рекомендациях, по включению сервисов в платформу «ГосТех» утверждаемых президиумом Комиссии, а также использованием производственного конвейера платформы «ГосТех» при сборке и развертывании ГИС.

2.4.1 Применение цифровых продуктов платформы «ГосТех»

Разработка или адаптация программного обеспечения ГИС, создаваемой (развиваемой) на платформе «ГосТех» выполняется с использованием цифровых продуктов платформы «ГосТех» и типовых решений, предназначенных для создания, развития и эксплуатации государственных информационных систем на платформе «ГосТех».

Описание состава и выполняемых функций цифровыми продуктами платформы «ГосТех» приведены в размещаемых на сайте платформы «ГосТех» соответствующих методических рекомендациях, утверждаемых президиумом Комиссии.

Функции платформы «ГосТех» реализуются через специально созданные для обеспечения функционирования платформы «ГосТех», входящие в ее состав федеральную государственную информационную систему «Управление единой цифровой платформой Российской Федерации «ГосТех» (далее - система «Управление платформой «ГосТех») и федеральную государственную информационную систему «Госмаркет» (далее – ФГИС «Госмаркет»), а также через функции цифровых продуктов платформы «ГосТех».

Цифровые продукты платформы «ГосТех», доступные для использования при создании (развитии) ГИС, размещаются в каталоге цифровых продуктов платформы «ГосТех» (далее – каталог цифровых продуктов), порядок ведения которого определяется Минцифры России.

Ведение каталога обеспечивается в ФГИС «Госмаркет» после завершения мероприятий по ее созданию.

При создании (развитии) ГИС на платформе «ГосТех» следует использовать типовые решения платформы «ГосТех», размещаемые в НФАП.

При создании (развитии) ГИС могут быть определены требования к созданию новых типовых решений платформы «ГосТех».

2.4.2 Разработка безопасного программного обеспечения

Разработка или адаптация программного обеспечения ГИС должна осуществляться с учетом положений методических рекомендации по обеспечению безопасности при разработке программного обеспечения с использованием компонентов единой цифровой платформы Российской Федерации «ГосТех» (утвержденных президиумом Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности).

Разработка программного безопасного программного обеспечения должна выполняться в соответствии с требованиями ГОСТ Р 56939 «Защита информации. Разработка безопасного программного обеспечения. Общие требования» и ГОСТ Р 58412 «Защита информации. Разработка безопасного программного обеспечения. Угрозы безопасности информации при разработке программного обеспечения».

Необходимо обеспечить использование средств организации автоматизированного производственного конвейера в составе платформы «ГосТех» при разработке программного обеспечения с учетом ФГИС

«Управление платформой «ГосТех» по результатам ее технологической готовности.

Для организации процесса разработки (или адаптации ПО), проведения испытаний и эксплуатации ГИС на платформе «ГосТех» используются стенды:

Стенд разработки (DEV-стенд платформы, от англ. Development, разработка, создание) - комплекс программных и технических средств, размещенный в облачной инфраструктуре, являющейся частью платформы «ГосТех», предназначенный для разработки ПО с использованием установленных на стенде компонентов платформы (включая разработку, отладку, сборку и предварительное тестирование).

Стенд тестирования (TEST-стенд платформы, от англ. Testing, Тестирование) - комплекс программных и технических средств, размещенный в облачной инфраструктуре, являющейся частью платформы «ГосТех», предназначенный для интеграционно-функционального тестирования разработанного ПО и(или) его компонент. Характеризуется наличием настроенных адаптеров со смежными системами интеграционного ландшафта (или их эмуляторов).

Стенд нагрузочного тестирования (НТ-стенд платформы) - комплекс программных и технических средств, размещенный в облачной инфраструктуре, являющейся частью платформы «ГосТех», предназначенный для сбора определения показателей производительности, оценки времени отклика в ответ на сформированные запросы разработанного ПО и(или) его компонент с целью установления соответствия требованиям по нагрузке, предъявляемым для разработанного программного обеспечения.

Стенд приемо-сдаточных испытаний (ПСИ-стенд платформы) - комплекс программных и технических средств, размещенный в облачной инфраструктуре, являющейся частью платформы «ГосТех», предназначенный для проведения испытаний разработанного на платформе ПО и(или) непосредственно перед его установкой на PROD-стенд.

Продуктивный стенд (PROD-стенд платформы, от англ. Production, производство) - комплекс программных и технических средств, размещенный в облачной инфраструктуре, являющейся частью платформы «ГосТех», предназначенный для промышленной эксплуатации разработанного ПО и(или) его компонент.

Для предоставления доступа к стендам платформы «ГосТех» должна быть подготовлена заявка на предоставление стендов с прилагаемой к ней компонентной диаграммой, а для предоставления стендов нагрузочного тестирования, приемо-сдаточных испытаний и продуктивного - заявка на

предоставление стендов с прилагаемой к ней диаграммой развертывания ГИС на платформе «ГосТех» (требования к диаграммам приведены в п.2.3.2.).

2.4.3 Сборка рабочего экземпляра программного обеспечения ГИС посредством автоматизированного сборочного конвейера платформы «ГосТех»

Сборка рабочего экземпляра программного обеспечения ГИС, в ходе которой реализуется набор проверок разрабатываемого ПО на соответствие определенным критериям, необходимым для перехода к следующей стадии жизненного цикла ГИС осуществляется посредством инструмента ФГИС «Управление платформой «ГосТех» - автоматизированного сборочного конвейера платформы «ГосТех».

Использование автоматизированного сборочного конвейера платформы «ГосТех» позволяет сократить трудовые и временные затраты на осуществление сборки рабочего экземпляра программного обеспечения ГИС, а также обеспечить автоматизацию прохождения разрабатываемым ПО необходимых проверок.

Автоматизированные проверки в процессе сборки рабочего экземпляра программного обеспечения ГИС на конвейере платформы «ГосТех» реализованы про помощи шлюзов качества (Quality Gates), под которыми понимаются определенные этапы, во время которых ПО проверяется на соответствие требованиям качества, безопасности и работоспособности, предъявляемым платформой «ГосТех». Проведение данных проверок позволяет выявить имеющиеся в разрабатываемом ПО несоответствия и устранить их на этапе разработки, тем самым сократив сроки создания ГИС и предотвратив ряд рисков.

Использование шлюзов качества обеспечивает следующие преимущества:

– обеспечение единообразия процессов разработки ПО ГИС;

– соответствие разрабатываемого ПО ГИС определенным критериям качества и безопасности, единым для ГИС на платформе «ГосТех»;

– раннее выявление дефектов разрабатываемого ПО ГИС и их оперативное устранение;

– проведение комплексной проверки разрабатываемого ПО ГИС, которое обеспечивает высокое конечное качество создаваемых ГИС.

Сборка рабочего решения посредством автоматизированного сборочного конвейера платформы «ГосТех» включает следующие мероприятия:

а) загрузка измененной ветки исходного кода ПО в репозиторий исходного года;

б) формирование запроса на слияние с основной веткой исходного кода ПО;

в) проведение первичной проверки исходного кода, комментариев и документации;

г) слияние измененной ветки исходного кода с основной веткой кода ПО;

д) проведение полный цикл проверок шлюзов качества;

е) сборка рабочего экземпляра ПО;

ж) перемещение артефакта сборки (готового образа) в хранилище артефактов;

з) развёртывание рабочего экземпляра ПО на стенды для проведения испытаний.

Подробное описание сборки рабочего решения посредством автоматизированного сборочного конвейера платформы «ГосТех» представлено в Методических рекомендациях по организации производственного процесса разработки государственных информационных систем с учетом применения итерационного подхода к разработке, утверждаемых президиумом Комиссии.

2.5 Ввод в эксплуатацию

Порядок ввода ГИС в эксплуатацию осуществляется в соответствии с требованиями, определенными Постановлением № 676.

2.5.1 Проведение испытаний

Целью проведения этапа является проверка создаваемой ГИС на платформе «ГосТех» на соответствие требованиям технического задания на создание (развитие) ГИС на платформе «ГосТех», а также частных технических заданий и(или) функционально-технических требований (при наличии).

Испытания должны проводиться на стендах платформы «ГосТех».

Этап проведения испытаний представляет собой процесс проверки выполнения заданных функций ГИС, определения и проверки соответствия количественных и (или) качественных характеристик ГИС установленным требования.

Для ГИС, создаваемой (развиваемой) на платформе «ГосТех» устанавливаются следующие основные виды испытаний:

а) предварительные;

б) опытная эксплуатация;

в) приемочные.

Дополнительно допускается проведение других видов испытаний ГИС и их частей. Перечень проводимых испытаний и статус приемочной комиссии устанавливаются в государственном контракте и (или) техническом задании на ГИС.

Для планирования и проведения всех видов испытаний разрабатываются соответствующие программы и методики испытаний, которые должны устанавливать необходимый и достаточный объем испытаний, обеспечивающий заданную достоверность получаемых результатов.

В случае применения последовательного способа создания ГИС на платформе «ГосТех» все виды испытаний осуществляются последовательно.

В случае применения итерационного подхода к разработке системы в отношении групп требований технического задания на создание системы в рамках итерации могут проводиться предварительные испытания и опытная эксплуатация. Допускается начинать выполнение отдельных этапов испытаний до завершения выполнения предшествующих этапов работ по созданию ГИС, а также параллельное во времени выполнение этапов работ.

В ходе этапа «Ввод в эксплуатацию» проводятся следующие мероприятия по обеспечению ввода системы (очереди системы) в эксплуатацию:

а) оформление прав на использование компонентов ГИС, являющихся объектами интеллектуальной собственности;

б) разработка и утверждение организационно-распорядительных документов, определяющих мероприятия по защите информации в ходе эксплуатации системы;

в) аттестация системы по требованиям защиты информации;

г) подготовка государственного органа к эксплуатации системы;

д) подготовка должностных лиц государственного органа к эксплуатации системы, включая лиц, ответственных за обеспечение защиты информации;

е) размещение в реестре территориального объектов контроля сведений о размещении технических средств информационной системы на территории Российской Федерации;

ж) размещение и публикация в НФАП исходного кода прикладных программных компонентов (разрабатываемых специально для данной ГИС) и документации на ГИС.

Размещение в НФАП исходного кода прикладных программных компонентов, разрабатываемых специально для данной ГИС, осуществляется посредством инструментов ФГИС «Управление платформы «ГосТех» по итогу ее технологической готовности. Состав сведений, размещаемых в НФАП, устанавливается Постановлением № 62.

Приведенный выше состав мероприятий является обязательным, но не исчерпывающим (может быть расширен по усмотрению государственного органа власти или внебюджетным фондом или иным лицом, реализующим мероприятия по созданию (развитию) ГИС).

Конкретный перечень мероприятий по обеспечению ввода системы (очереди системы) в эксплуатацию, а также срок начала эксплуатации устанавливается правовым актом государственного органа, определенного в соответствии с нормативным правовым актом, регламентирующим функционирование ГИС.

Особенности аттестации ГИС по требованиям защиты информации определяются:

а) Концепцией обеспечения информационной безопасности единой цифровой платформы Российской Федерации «ГосТех» (утв. приказом Минцифры России от 12 января 2023 № 7);

б) Порядком организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну (утв. приказом ФСТЭК России от 29 апреля 2021 г. №77);

в) Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах (утв. приказом ФСТЭК России от 11 февраля 2013 г. № 17);

г) Методическими рекомендациями по организации и проведению работ по аттестации государственных информационных систем на единой цифровой платформе Российской Федерации «ГосТех» на соответствие требованиям по защите информации, утверждаемые президиумом Комиссии.

2.6 Эксплуатация

Эксплуатация ГИС на платформе «ГосТех» осуществляется в соответствии положениями Постановления № 676, а также следующими документами:

– методические рекомендации по эксплуатации государственных информационных систем на Единой цифровой платформе «ГосТех», утверждаемые президиумом Комиссии;

– методические рекомендации «Стандарт по управлению динамической инфраструктурой Единой цифровой платформы «ГосТех» утверждаемые президиумом Комиссии;

– методические рекомендации по предъявлению требований к поставщикам вычислительной инфраструктуры и облачных платформ в части используемых ими информационных технологий и технологий обеспечения информационной безопасности на единой цифровой платформе Российской Федерации «ГосТех», утверждаемые президиумом Комиссии;

– регламент по эксплуатации (согласуется с оператором платформы «ГосТех»);

– регламент по информационной безопасности (согласуется с оператором платформы «ГосТех»).

2.7 Вывод из эксплуатации

Совокупность процессов (работ) определения невозможности и (или) нецелесообразности дальнейшей эксплуатации системы и реализации

соответствующих мероприятий, в том числе деинсталляцию программного обеспечения, реализацию прав на программное обеспечение, демонтаж и списание технических средств, обеспечение хранения и дальнейшее использование информационных ресурсов осуществляется в соответствии с Постановлением №676.

3 Подходы к решению прикладных архитектурных и технологических задач при создании ГИС на платформе «ГосТех»

Решения прикладных архитектурных и технологических задач, описание которых приведено в настоящем разделе, спроектированы с использованием функциональности, предоставляемой базовыми сервисами платформы «ГосТех». Описанные решения и их возможности обеспечиваются платформой «ГосТех».

В рамках настоящих методических рекомендаций базовые сервисы платформы «ГосТех» предоставляются пользователям платформы «ГосТех» по модели «Platform as a Service» (PaaS, «платформа как услуга»). Данная модель предполагает, что пользователь платформы «ГосТех» получает удаленный доступ посредством облачных вычислений к набору базовых сервисов платформы «ГосТех». Данных подход обеспечивает возможность использования и переиспользования цифровых продуктов платформы «ГосТех».

Порядок развертывания, алгоритмах работы и последующей эксплуатации цифровых продуктовплатформы «ГосТех», а также технологические карты будут размещаться на технологическом портале на сайте платформы «ГосТех».

3.1 Сервисы работы с данными

3.1.1 Сервис транзакционной СУБД

Сервис транзакционной СУБД - объектно-реляционная система управления базами данных, основанная на свободно распространяемой версии PostgreSQL. Она содержит ряд доработок, позволяющих обеспечить требования к безопасности хранимых данных, доступности, надежности и производительности:

- гибкое управление парольными политиками;
- прозрачное шифрование хранимой информации;
- защита от привилегированных пользователей;
- аудит действий пользователей;
- автоматическое развертывание и конфигурирование кластера высокой доступности;
- инкрементальное резервное копирование;
- соответствие четвертому уровню доверия по ФСТЭК.

Доступность и надежность хранения данных обеспечивается за счет использования кластера высокой доступности на основе patroni.

Сервис рекомендуется к использованию для хранения и обработки структурированных данных в системах, требующих гарантий целостности: финансовые системы, приложения электронной коммерции, медицинские системы, учетные системы, системы управления предприятием.

3.1.2 Сервис Key-value СУБД (in-memory)

Сервис in-memory СУБД – горизонтально масштабируемая, отказоустойчивая платформа для хранения и обработки больших объемов данных в оперативной памяти кластера на основе Apache Ignite. Функционал свободно распространяемого решения дополнен плагином безопасности Ignite SE:

– аутентификация пользователей по логину и паролю;
– второй фактор аутентификации – по сертификату;
– утилиты управления пользователями и разрешениями (web UI, command line), не требующие перезапуска кластера для применения изменений.

Сервис рекомендуется к использованию для ускорения обработки больших объемов данных:

– выполнение распределённых вычислений (map reduce);
– использование Ignite как кэширующего слоя к реляционным и NoSQL СУБД;
– хранение веб-сессий при использовании микросервисной архитектуры;
– аналитические системы (OLAP).

3.1.3 Сервис управления очередями сообщений

Сервис управления очередями сообщений - программный брокер сообщений на основе Apache Kafka, представляющий собой распределенную, реплицированную и масштабируемую систему передачи сообщений, работающую по принципу «публикация-доставка».

Ключевые особенности сервиса:

– поддержка ACID-транзакций;
– обновление продукта без остановки сервиса;
– TLS шифрование с контролем срока действия сертификатов;
– schema registry.

Сервис рекомендуется к использованию:

– в качестве брокера сообщений приложений с микросервисной архитектурой;
– для передачи событий между слабосвязанными компонентами и службами (архитектура, управляемая событиями);
– для вычислений с сохранением состояния по потокам данных (потоковая и пакетная обработка);
– для реализации распределённой репликации данных.

3.1.4 Сервис ширококолоночной СУБД

Сервис ширококолоночной СУБД основан на дистрибутиве Hortonworks Data Platform (HDP) open source решения Apache Hadoop. Сервис предназначен для работы с большими (до десятков петабайт) объемами данных.

Основные возможности сервиса:

– хранение структурированных и неструктурированных данных;

– обработка данных с применением модели распределенных вычислений;

– управление кластером компонентов, необходимых для работы с данными.

Сервис рекомендуется использовать в следующих целях:

– хранение больших объемов данных в HDFS;

– распределенная обработка больших объемов данных с использованием MapReduce и Spark;

– анализ и управление данными с использованием Hive.

3.1.5 Сервис СУБД полнотекстового индекса

Сервис СУБД полнотекстового индекса основан на open source решении OpenSearch и предназначен для реализации функционала полнотекстового и структурированного поиска, визуализации и анализа текстовых данных. В качестве поискового движка используется Apache Lucene, в качестве инструмента визуализации – OpenSearch Dashboards.

Сервис предоставляет REST API, а также поддерживает дополнительные возможности через расширения (plugins):

– детектирование аномалий в данных в реальном времени;

– анализ с использованием алгоритмов машинного обучения;

– асинхронные запросы.

Сервис интегрирован с платформенными сервисами: IAM, сервисы журналирования и мониторинга. Сервис поддерживает мультитенантность.

Сервис рекомендуется к использованию для реализации:

– функционала полнотекстового поиска в приложениях заказчика;

– систем мониторинга приложений и инфраструктуры;

– систем мониторинга событий и расследования инцидентов информационной безопасности.

3.1.6 Сервис СУБД аналитического хранилища данных

Сервис СУБД аналитического хранилища данных представляет собой аналитическую колоночную массивно-параллельную СУБД, основанный на open source решении Greenplum. Кластер Greenplum состоит из экземпляров PostgreSQL, каждый из которых обрабатывает часть данных, к которым

предоставляется единый интерфейс для работы, доступный через узел-координатор.

Сервис предоставляет возможности работы с большими объемами данных с поддержкой SQL-запросов и транзакций.

Сервис рекомендуется к использованию для построения:

– аналитических хранилищ данных;
– аналитических витрин данных.

3.1.7 Сервис СУБД аналитических витрин хранилища данных

Сервис СУБД аналитических витрин хранилища данных представляет собой колоночную СУБД с возможностью построения аналитики в реальном времени и основан на open source решении ClickHouse.

Сервис предназначен для хранения и обработки больших объем (до петабайт) структурированных данных с поддержкой расширенного синтаксиса SQL-запросов, но без поддержки транзакций.

Сервис рекомендуется к использованию для построения аналитических витрин данных с возможность интерактивной аналитики в реальном времени.

3.2 Интеграционные сервисы

3.2.1 Сервис интеграционного взаимодействия

Сервис интеграционного взаимодействия - интеграционная платформа, построенная на базе open source продукта Istio. Продукт отвечает за контроль и управление взаимодействием между сервисами, работающими в среде контейнеризации.

В сервисе реализованы следующие возможности:

– валидатор запросов с поддержкой JSON/XML схем;
– панель управления на основе доработанного open source решения Kiali;
– валидаторы новых и существующих конфигураций service mesh;
– сервис трассировки, возможна отправка событий трассировки в формате Jaeger либо Zipkin.

Сервис рекомендуется к использованию при построении систем с микросервисной архитектурой, работающих в среде контейнеризации.

3.2.2 Сервис управления микросервисами

Сервис управления микросервисами – среда управления контейнеризацией на основе open source решения Kubernetes. Продукт отвечает за автоматизацию развертывания и масштабирования контейнеризированных приложений, а также за управление ими.

Сервис рекомендуется к использованию:

– при построении систем с микросервисной архитектурой;
– для ускорения внедрения DevOps практик за счет ускорения прототипирования и развертывания приложений;

– для масштабирования и распределения нагрузки в высоконагруженных системах, например, в системах искусственного интеллекта и машинного обучения.

3.3 Сервисы управления

3.3.1 Сервис управления процессами

Сервис управления процессами – инструмент, позволяющий автоматизировать бизнес-процессы, включая оркестрацию сервисов и пользовательских задач. Включает в себя среду разработки процессов в нотации BPMN2, ядро исполнения процессов, панель управления, позволяющую контролировать исполнение процессов, а также портал для работы пользователя с назначенными задачами.

Сервис интегрирован с другими сервисами платформы: IAM, журналирование, аудит, мониторинг.

Сервис рекомендуется к использованию для автоматизации процессов, отвечающих следующим критериям:

– процесс носит достаточно массовый характер, чтобы затраты на автоматизацию окупились;

– процесс достаточно сложен, включает много этапов и/или участников;

– процесс относительно часто изменяется, что делаем классическую автоматизацию через разработку/доработку ПО неэффективной;

– заказчику требуется автоматизированный контроль и учет исполнения бизнес-процессов.

Типовыми примерами применения сервиса управления процессами выступают:

– процессы управления взаимоотношениями с клиентами;
– процессы продаж;
– процессы обработки заявок, кредитный скоринг;
– процессы управления персоналом;
– процессы юридических подразделений;
– производственные процессы контроля качества и логистики.

3.4 Служебные технологические сервисы

3.4.1 Сервис журналирования

Сервис журналирования предназначен для сбора журналов приложений и компонентов инфраструктуры, а также последующей работы с данными журналов – поиском и визуализацией в виде графиков. Сервис построен на основе open source решений Logstash, OpenSearch и OpenSearch Dashboards.

Сервис включает доработки для поддержки мультитенантности и интеграции с другими платформенными сервисами:

– IAM (аутентификация и авторизация с поддержкой мультитенантности);

– с сервисом аудита в части отправки событий аудита;

– с сервисом мониторинга в части отправки метрик сервиса журналирования.

Сервис рекомендуется к использованию в качестве готового решения для сбора и визуализации журналов приложений заказчика.

3.4.2 Сервис мониторинга

Сервис мониторинга предназначен для сбора, хранения и визуализации метрик приложений и компонентов инфраструктуры.

Сервис включает доработки для поддержки мультитенантности и интегрирован с IAM, который выступает внешним поставщиком аутентификации и авторизации.

Сбор метрик осуществляется по протоколу Prometheus.

Сервис рекомендуется к использованию в качестве готового решения для сбора метрик с приложений.

3.4.1 Сервис предоставления кворумного ЦОД

Сервис предоставления кворумного ЦОД размещается в отдельном физическом ЦОД и включает в себя компоненты, обеспечивающие кворум при выборе лидера кластера в географически распределенных системах:

– кворумные узлы etcd для кластеров сервиса транзакционной СУБД;

– кворумные узлы zookeeper для кластеров kafka;

– при необходимости – другие типы кворумных узлов.

Сервис необходимо использовать при построении катастрофоустойчивых (географически распределенных) решений.

3.5 Сервисы безопасности

3.5.1 Сервис IAM

Сервис IAM (Identity and Access Management) включает сервисы аутентификации и авторизации на основе open source решения KeyCloak. IAM также включает в себя:

– компонент «IAM Proxy», представляющий собой реверсивный прокси на основе nginx с поддержкой аутентификации и авторизации через IAM;

– компонент «Авторизация IAM», позволяющий создать ролевую модель и проводить динамический расчет полномочий пользователя.

– плагин для аутентификации пользователя через ЕСИА.

Сервис IAM сертифицирован ФСТЭК. Сервис рекомендуется к использованию в качестве внешнего средства аутентификации и авторизации для приложений заказчика, в том числе для организации единой точки входа (SSO).

3.5.2 Сервис аудита

Сервис аудита предназначен для регистрации и протоколирования действий пользователей при работе в автоматизированных системах. Сервис предоставляет

единый пользовательский интерфейс (UI) для просмотра и работы с зарегистрированными событиями безопасности при расследовании инцидентов. Сервис интегрирован с IAM как провайдером аутентификации и авторизации.

Функциональные возможности:

- сбор событий безопасности из приложений;
- хранение событий безопасности;
- просмотр событий безопасности;
- управление метамоделью событий аудита;
- подготовка отчетов по событиям;
- просмотр статистики событий.

Сервис рекомендуется к использованию в качестве готового решения для аудита событий информационной безопасности.

3.6 Сервисы интеграции с инфраструктурой электронного правительств

3.6.1 Обеспечение предоставления государственных данных посредством витрин данных НСУД

Витрина данных – комплекс программных и технических средств в составе информационно-телекоммуникационной инфраструктуры участника взаимодействия, обеспечивающий хранение и предоставление данных другим Участникам взаимодействия с использованием подсистемы обеспечения доступа к данным (ПОДД СМЭВ).

Подсистема обеспечения доступа к данным федеральной государственной информационной системы «Единая система межведомственного электронного взаимодействия» – часть транспортной подсистемы СМЭВ, обеспечивающая доступ к данным, размещённым на Витринах данных.

Поставщик данных – участник взаимодействия, владелец сведений, направляемых в ПОДД СМЭВ. Потребитель данных – участник взаимодействия, получающий данные от Поставщиков данных с использованием ПОДД СМЭВ.

Для подключения к ПОДД СМЭВ используется Агент ПОДД СМЭВ, не входящий в состав витрины данных НСУД. Агент ПОДД СМЭВ – Типовое программное обеспечение, устанавливаемое в контуре участника взаимодействия и обеспечивающее сопряжение экземпляров витрин данных с ПОДД СМЭВ.

Поставщику данных для обеспечения информационного взаимодействия посредством витрин данных НСУД необходимо:

– установить ПО витрин данных НСУД (предоставляется в качестве сервиса «Типовое тиражируемое программное обеспечение витрин данных» на платформе «ГосТех» на платформе «ГосТех»);

– установить ПО Агент ПОДД (предоставляется в качестве сервиса взаимодействия с ядром подсистемы обеспечения доступа к данным СМЭВ на платформе «ГосТех») и обеспечить подключение к СМЭВ;

– сформировать модель данных и регламентированные запросы (РЗ);

– зарегистрировать модель данных и регламентированные запросы в ЕИП НСУД (в соответствии с Регламентом подключения к ЕИП НСУД и СМЭВ).

Порядок описания моделей витрин данных и регламентированных запросов регламентирован Минцифры России:

https://info.gosuslugi.ru/articles/Коротко_о_ЕИП_НСУД/

Регламентированный запрос (РЗ) – SQL-запрос, выраженный в терминах Модели данных, загруженной в ПОДД, и зарегистрированный в Ядре ПОДД СМЭВ под символической мнемоникой, используемой ИС Потребителя ПОДД СМЭВ для выполнения регламентированного запроса. Может иметь параметры, значения которых задаются Потребителем данных ПОДД СМЭВ при выполнении регламентированного запроса. После регистрации витрин данных в СМЭВ витрины Поставщиков могут использоваться для предоставления сведений.

Общая схема построения сервиса Витрины данных НСУД на платформе «ГосТех» показана на рисунке 1.

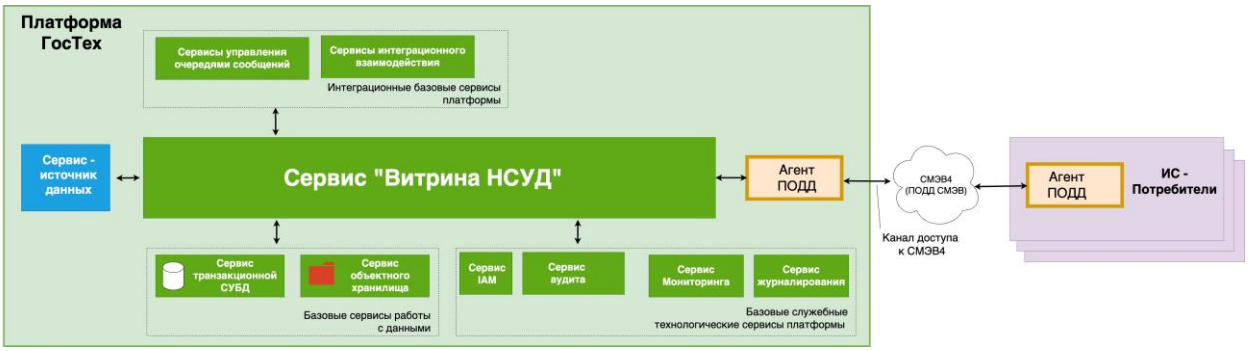

Рисунок 1 - Схема построения витрины данных НСУД на платформе «ГосТех»

Для обеспечения развертывания и функционирования сервиса витрина данных НСУД используются также следующие базовые сервисы платформы «ГосТех»:

г) Сервисы работы с данными:

1) сервис транзакционной СУБД (или иной базовый сервис работы с данными);

2) сервис объектного хранилища (опционально);

д) Интеграционный сервис:

1) сервис управления очередями сообщений;

е) Служебные технологические сервисы:

1) сервис мониторинга;

2) сервис журналирования;

3) сервис аудита;
4) сервис IAM.

Загрузка данных в витрину осуществляется от источника данных (ГИС или сервиса, реализованного на платформе «ГосТех») по следующим:

- JDBC – драйвер:
- REST – адаптер;
- Сервис извлечения данных.

Источник данных, ГИС (сервис) поставщика данных, передающий данные в витрину данных НСУД, размещенную на платформе «ГосТех» может располагаться не на платформе «ГосТех». При этом должна быть обеспечена сетевая связанность между источником данных и витриной данных НСУД, размещенной на платформе «ГосТех».

На рисунке ниже представлены варианты размещения витрин данных НСУД, в то числе на платформе «ГосТех».

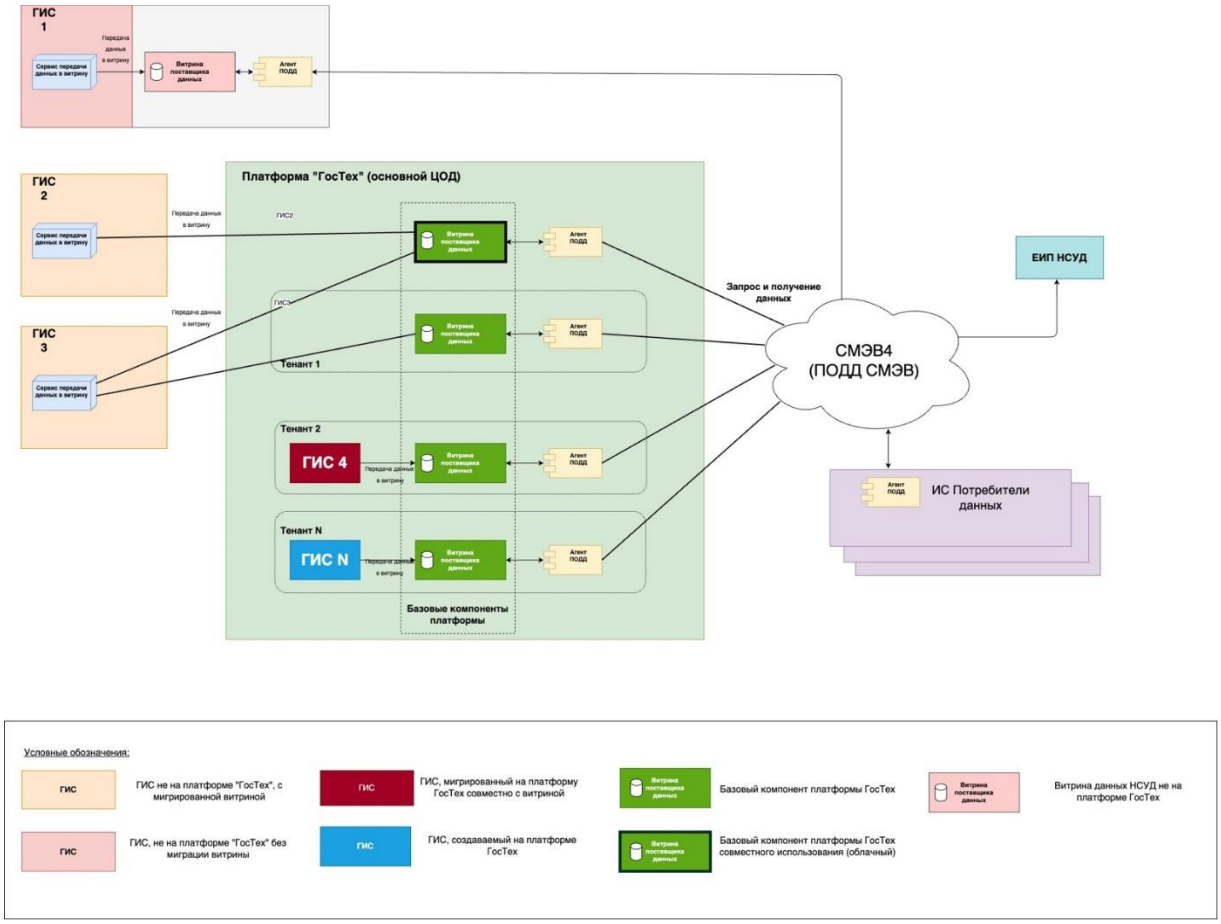

Рисунок 2 - Варианты размещения витрин данных НСУД

Все вновь разрабатываемые ГИС (ИС) на платформе смогут использовать витрину НСУД как базовый сервис в виде независимой витрины и в виде «облачного» сервиса.

В случае, если ГИС (ИС) мигрирует на платформу «ГосТех» и уже использует витрину НСУД, то она так же мигрирует на платформу «ГосТех».

Также витрина НСУД может быть мигрирована на платформу «ГосТех» (или создана на платформе) отдельно от ГИС (ИС).

Общие сведения о Типовом тиражируемое программном обеспечении витрин данных, их возможностях, порядке подключения и настройке опубликовано на ресурсе Минцифры России: https://info.gosuslugi.ru/sections/%D0%A1%D0%9C%D0%AD%D0%92_4_(%D0%9F%D0%9E%D0%94%D0%94)/# .

3.6.2 Платформа государственных сервисов

Платформа государственных сервисов (далее – ПГС) предназначена для обеспечения возможности конструирования и исполнения процессов предоставления услуг (функций) (в том числе при взаимодействии с ЕПГУ посредством СМЭВ), включая:

– обеспечение ведения в электронном виде реестров данных;

– автоматизацию предоставления государственных (муниципальных) услуг в электронной форме заявителям в соответствии с утвержденными административными, с момента поступления заявления из федеральной государственной информационной системы «Единый портал государственных и муниципальных услуг (функций)» (ЕПГУ), либо при приеме заявления при личном приеме заявителя в органе власти, органе государственного внебюджетного фонда или многофункциональном центре предоставления государственных (муниципальных) услуг, до выдачи заявителям результатов предоставления услуг в личном кабинете заявителя на ЕПГУ;

– автоматический контроль как сроков исполнения каждой административной процедуры предоставления услуги в отдельности, так и срока предоставления услуги в целом на основании административного регламента, а также сведений о государственной (муниципальной) услуге (функции);

– обеспечение возможности регистрации заявлений физических лиц, пришедших на личный прием в органы государственной власти, органы местного самоуправления, органы государственных внебюджетных фондов и многофункциональные центры предоставления государственных (муниципальных) услуг (функций);

– обеспечение получения наглядной информации по предоставлению государственных и муниципальных услуг (функций) в электронной форме, в т. ч. сводной отчетности.

Общая концептуальная схема применения ПГС приведена на рисунке ниже (см. Рисунок 3).

Пользователями ПГС, предоставляемого в качестве сервиса на платформе «ГосТех», являются руководители и сотрудники органов исполнительной власти субъектов Российской Федерации и органов местного самоуправления.

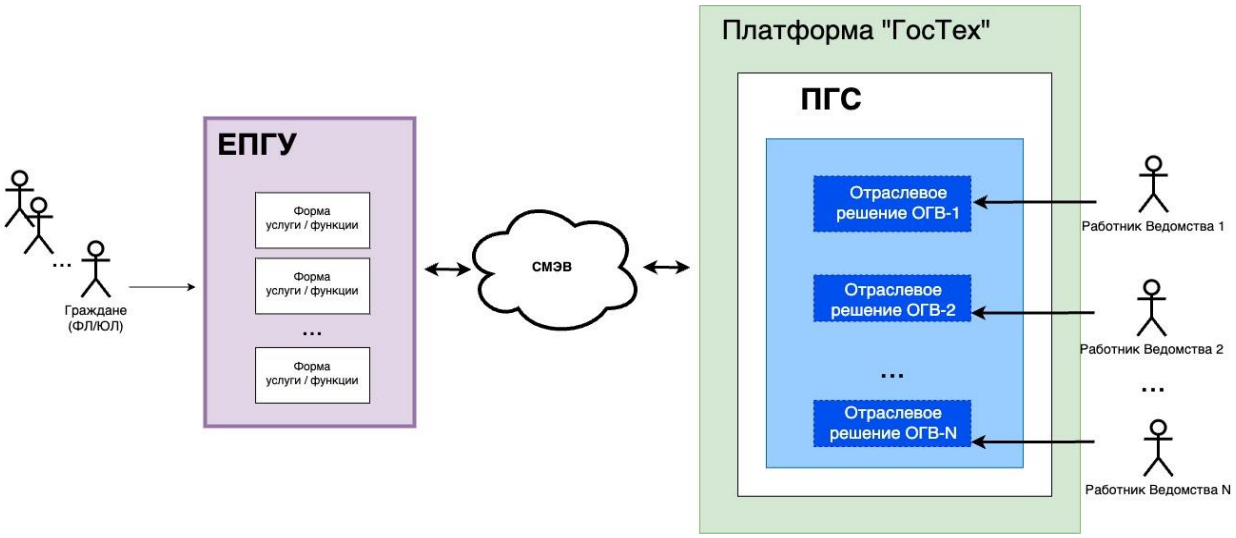

Рисунок 3 - Общая концептуальная схема применения ПГС

4 Проектные решения с учётом определения обязательности повторного использования цифровых продуктов Платформы «ГосТех» при создании и развитии ГИС

4.1 Обеспечение доступности

Решения по применению подхода геораспределенному георезервированию не носит обязательный характер и применяется для высконагруженных систем.

4.1.1 Георасределённое резервирование

Для обеспечения доступности все элементы ГИС должны быть дублированы с использованием георасределённого резервирования. При проектировании ГИС необходимо закладывать дублирование компонент на каждом уровне архитектуры. Дублирование компонент преследует единственную цель - исключение единых точек отказа (single point of failure, SPOF) в системе. Минимальный рекомендуемый фактор резервирования для всех компонент – 2, но существуют исключения для компонент использующих алгоритмы решений задачи консенсуса (например, Raft), где необходимо использовать нечетное число экземпляров с фактором резервирования 3+.

Георезервирование прикладных ГИС

Схема георезервирования прикладных ГИС приведена на рисунке ниже.

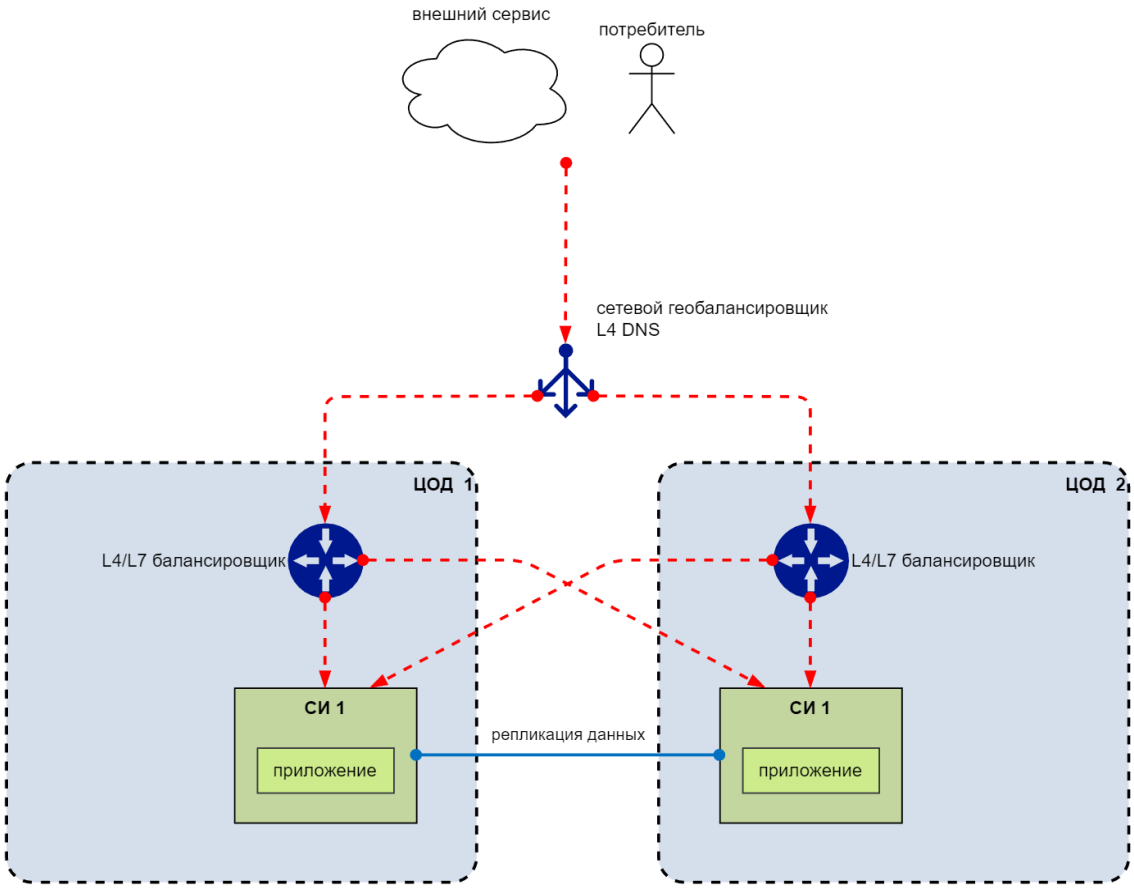

Рисунок 4 - Схема георезервирования прикладных ГИС

Первичную балансировку между ЦОД, прозрачную для потребителя, рекомендуется делать на уровне DNS серверов - при запросе IP адреса сервиса со стороны потребителя ему предоставляются IP адреса либо из ЦОД 1, либо из ЦОД 2, в зависимости от алгоритма балансировки - как циклично, т.е. каждый следующий запрос направляется в другой ЦОД, либо через хэш функцию пары IP и порта вызывающей стороны

В каждом ЦОД рекомендуется иметь дополнительный L4/L7 балансировщик, который может определять недоступность сервисов внутри ЦОД и перенаправлять запросы в другой ЦОД

Необходимо обеспечить прикладную репликацию данных между хранилищами данных в разных ЦОД, например, с использованием сервиса управления очередями сообщений.

Георезервирование с кворумом на примере серверов ссервиса управления очередями сообщений

Схема георезервирования с кворумом на примере серверов сервиса управления очередями сообщений приведена на рисунке ниже.

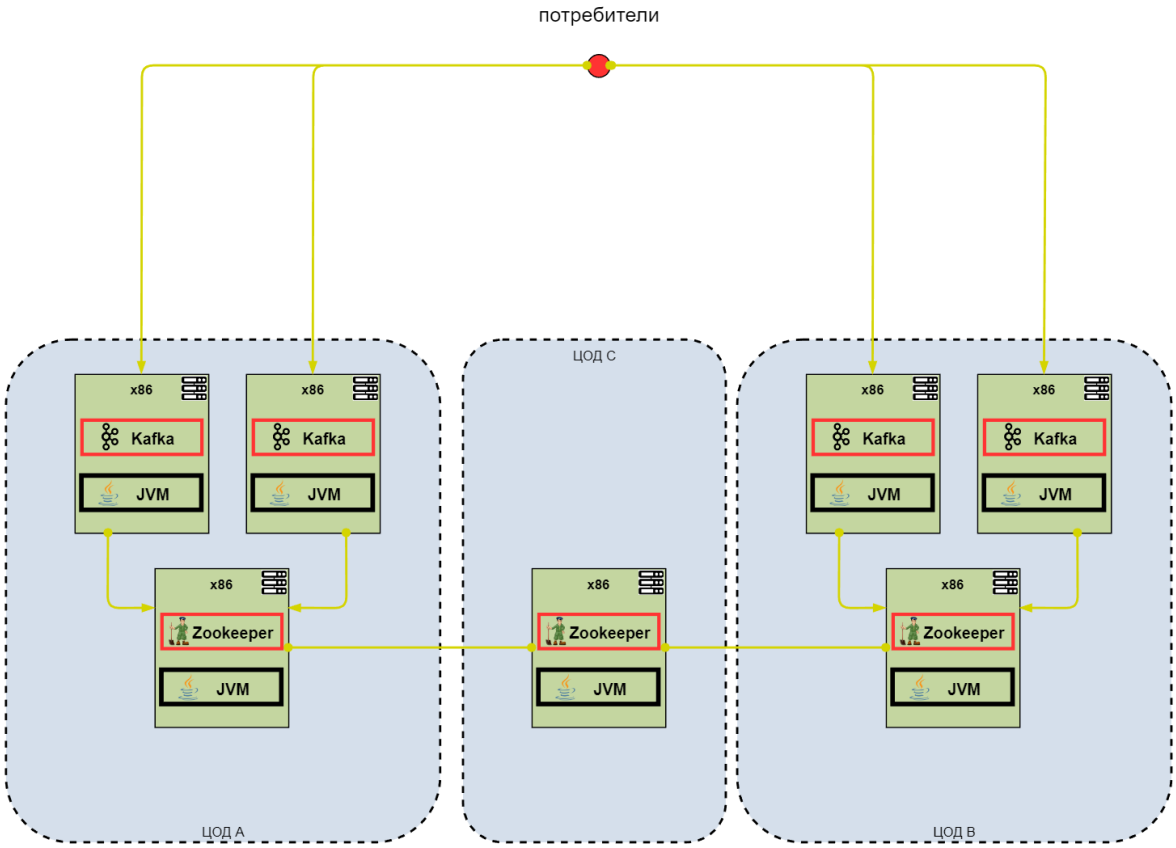

Рисунок 5 - Схема георезервирования с кворумом на примере серверов сервиса управления очередями сообщений

Сервис управления очередями сообщений (Kafka) использует компоненты Zookeeper, для которого используется кворумное резервирование, т.е. узлов должно быть нечётное количество. Для георезервирования нечётные узлы рекомендуется размещать в отдельных ЦОД.

Рекомендуется брокеры сообщений размещать на виртуальных серверах разных физических машин в случае наличия требований высокой отказоустойчивости.

Для повышения надёжности рекомендуется настроить фактор репликации равным количеству брокеров в кластере и параметр acks = all.

4.2 Обеспечение отказоустойчивости

4.2.1 Управление репликами баз данных и приложений

В схеме Stand-In реализуется отказоустойчивое приложение путём создания дублирующего контура приложения, которое в штатном режиме не задействовано и принимает реплики данных от основного контура в объёме, предусмотренном моделью реализации дублирования. В случае возникновения нештатной ситуации происходит переключение на маршрутизаторе дублирования и вся работа потребителей идёт с приложением на резервном контуре.

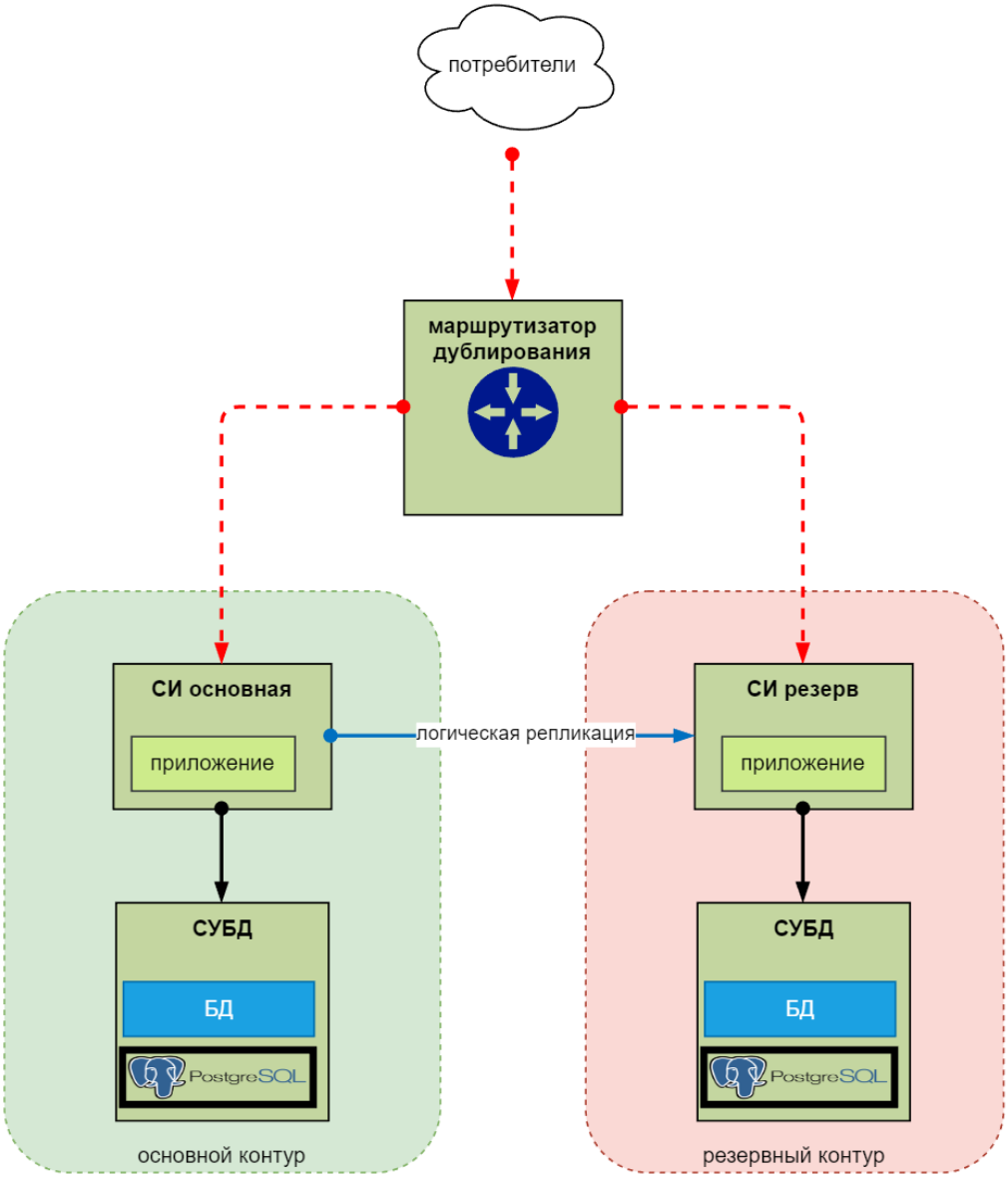

Рисунок 6 - управление репликами баз данных и приложений схемы Stan-dIn

Отказоустойчивый кластер

Отказоустойчивый кластер применяется для защиты от инфраструктурных сбоев – таких как:

- отказ сервера;
- отказ системы хранения данных;
- потеря соединения с сервером БД;
- потеря ЦОД;
- неустранимая внутренняя ошибка СУБД.

Использование отказоустойчивого кластера рекомендуется для всех промышленных сред сервиса транзакционной СУБД.

При развёртывании кластера в соответствии с рекомендациями (3 ЦОД с расстоянием между любой парой не более 50 км) гарантируется автоматическое восстановление после любой одиночной ошибки.

При развёртывании кластера в двух ЦОД возможны ситуации, требующие ручного вмешательства администратора БД.

При развёртывании кластера в единственном ЦОД гарантируется автоматическое восстановление после любой одиночной ошибки кроме полной потери ЦОД – в этом случае БД станет недоступна.

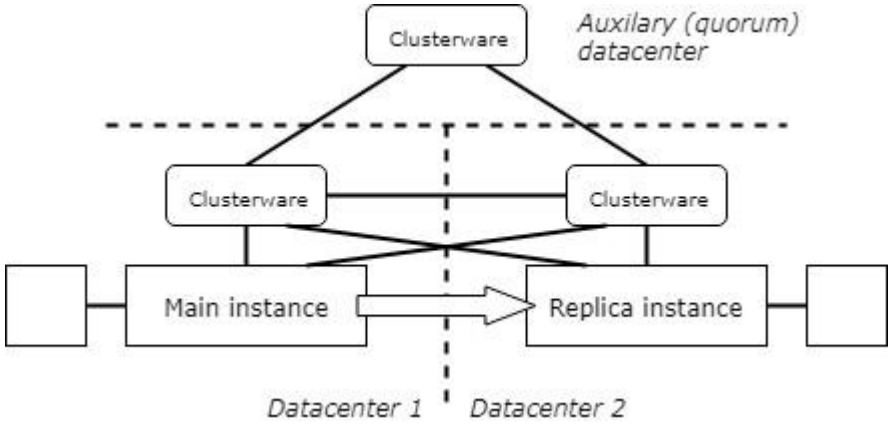

Рисунок 7 - Схема отказоустойчивого кластера

Развёртывание кластера сервиса транзакционной СУБД осуществляется «из коробки» штатным инсталлятором. В установку входят следующие продукты, перечисленные в таблице ниже.

Таблица 4 – Состав продуктов

Продукт	**Назначение**
PostgreSQL	СУБД
Patroni, etcd	средство автоматизации переключения кластера при сбоях
pgBouncer	мультиплексор соединений
HAProxy	единая точка входа в кластер, обеспечивающая соединение клиента с активным узлом БД

Отказоустойчивый кластер состоит из следующих компонентов:

а) подсистема физической репликации;

б) средство автоматизации переключения.

Подсистема физической репликации (streaming replication) является частью сервиса транзакционной СУБД. Принцип её действия основан на передаче журналов БД с основной базы данных и повторении изменений, записанных в журнале, на базе-реплике (standby).

Сервис транзакционной СУБД позволяет сконфигурировать синхронную репликацию, т. е. завершение операции «commit» на основном сервере означает, что информация о транзакции уже передана на standby-сервер. Такая конфигурация обеспечивает нулевую потерю данных при сбое, но снижает производительность БД за счёт увеличения времени commit. Чтобы снижение

производительности не выходило за приемлемые рамки, рекомендуется, чтобы сетевая задержка между серверами не превышала 5 мс. Это соответствует расположению серверов в ЦОД, находящихся друг от друга на расстоянии до 50 км (т. н. metropolitan area).

Демон Patroni следит за состоянием обоих экземпляров сервиса транзакционной СУБД (основного и standby) и при необходимости выполняет операции над кластером. Перечень возможных состояний приведен в таблице ниже (см. Таблица 5).

Таблица 5- События

Событие	Реакция
Остановка основной БД вследствие любой причины (отказ сервера, отказ СХД, потеря ЦОД и т. д.)	активация standby-базы; изменение маршрута в HAProxy; отключение репликации.
Остановка резервной БД вследствие любой причины (отказ сервера, отказ СХД, потеря ЦОД и т. д.)	отключение репликации.
Обрыв связи между ЦОД	отключение репликации.
Восстановление после аварии	включение репликации, восстановление кластера

ПО etcd необходимо для исключения ситуации «split brain», когда нарушена связь между ЦОД, оба сервера БД считают, что остались в одиночестве, и доступны для чтения и записи.

Демон Patroni перед тем, как переключить активный узел, записывает конфигурацию кластера в хранилище etcd. Запись считается удачной, если набран кворум, то есть её подтвердили большинство узлов – в данном случае два узла. Таким образом при сбое канала между ЦОД демон резервного попытается перевести резервный узел в статус основного, однако не сделает этого, т. к. в кластере etcd записана информация о том, что основной узел продолжает работу. Связность кластера etcd сохраняется за счёт независимых каналов связи между основными ЦОД и кворумным ЦОД.

Логическая репликация

Использование кластера серверов сервиса управления очередями сообщений позволяет делать репликацию данных между компонентами приложения, в т.ч. и в разных ЦОД. Данные, записываемые в кластер, становятся доступными на всех узлах кластера, благодаря чему несколько компонентов могут получить информацию об изменении данных по принципу подписки. Таким образом, одно изменение может быть реплицировано на произвольное количество компонентов ИС.

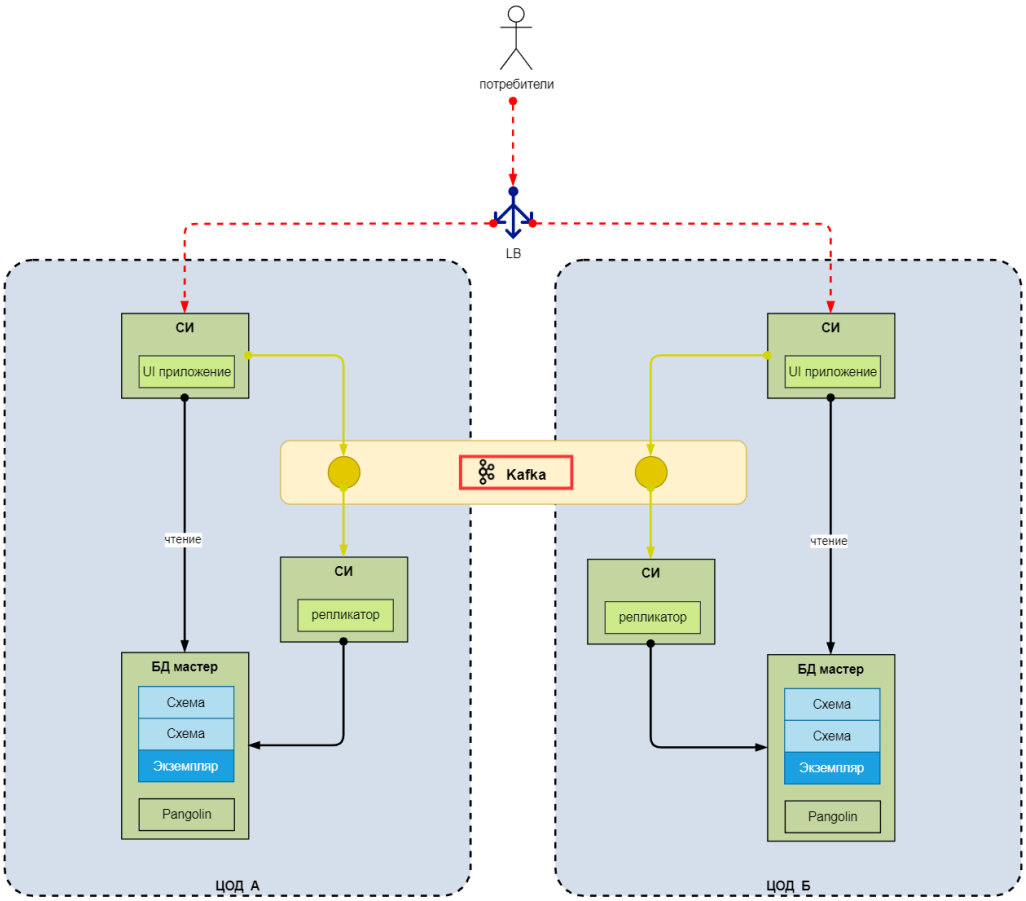

Рисунок 8 – Схема логической репликации

4.2.2 Мониторинг (снижение критичных показателей системы относительно нормы), журналирование (снижение времени разбора инцидентов)

Мониторинг и журналирование работы прикладных приложений выполняется с использованием сервисов журналирования и мониторинга.

Мониторинг: точки вызова приложения

Добавляется новая точка, через которую возможно осуществлять вызов приложения. Например, новый rest API. Необходимо добавить для новой точки вызова следующие метрики:

- имя_точки_start;
- имя_точки_finish_success;
- имя_точки_finish_failure;
- имя_точки_duration;

Такой набор метрик позволит при эксплуатации приложения мониторить работоспособность добавленной точки вызова приложения.

Мониторинг: выбор единиц измерения метрики

Добавляется новая метрика приложения. Необходимо использовать одинаковый набор единиц изменения для всех приложений.

Таблица 6 – Таблица единиц измерения

Измерение	Единица измерения
Факт	штуки
Время	секунды
Температура	градусы Цельсия
Длина	метры
Байты	байты
Биты	байты
Проценты	отношение (диапазон 0-1)
Напряжение	вольты
Сила тока	амперы
Энергия	джоули
Масса	граммы

Использование одинаковых единиц измерения снижает риск неправильной интерпретации показателей работы приложения при его эксплуатации.

Мониторинг аномальной нагрузки приложения

Необходимо настроить сравнительные графики операций приложения к аналогичному периоду в прошлом:

- текущий день к аналогичному дню неделю назад, две недели назад;
- месяц к предыдущему месяцу;
- год к предыдущему году.

Такой набор графиков позволит при эксплуатации приложения отслеживать аномальные изменения нагрузки на приложение.

Мониторинг: достаточность метрик приложения

Решение о достаточности набора метрик приложения должно приниматься инженером службы эксплуатации при приёмке приложения на эксплуатацию. При недостаточности реализованного набора метрик, приложение должно быть доработано с учётом замечаний по составу метрик до передачи его в эксплуатацию.

Мониторинг: инструкция по работе с инцидентами

Руководителем службы эксплуатации должна быть разработана инструкция по действиям инженеров в случае возникновения инцидента. Инструкция должна описывать что считается инцидентом и критерии классификации инцидентов по их уровню влияния.

Мониторинг: регистрация инцидента

Любой сбой в работе приложения должен быть зарегистрирован в специальном журнале учёта инцидентов. При регистрации инцидента он должен быть классифицирован согласно SLA по работе с инцидентами.

Мониторинг: поиск корневой причины инцидента

Каждый инцидент должен быть рассмотрен комиссией по разбору инцидентов с целью определения его корневых причин, определения способов их устранения и способов обхода последствий инцидента до внедрения исправлений корневой причины инцидента.

Мониторинг: добавление точек мониторинга в результате анализа инцидента

По итогам разбора инцидента необходимо запланировать добавление метрик в приложение, если в ходе разбора инцидента было выявлено, что данные метрики отсутствовали, а их реализация позволила бы более оперативно реагировать на инцидент.

Мониторинг: анализ корневой причины инцидента применительно к другим приложениям

При анализе инцидента необходимо проводить анализ возможности аналогичных или похожих инцидентов при работе других приложений в эксплуатации. Если в результате анализа обнаружены новые риски, комиссия по инцидентам должна запланировать их митигацию и устранение.

Мониторинг: сценарии устранения аварийных ситуаций

При подготовке приложения к эксплуатации необходимо провести анализ возможных сценариев его отказа и для каждого из сценариев составить план действий. Необходимо регулярно (не реже одного раза в квартал) производить ревизию сценариев и планов действий при их наступлении. Ревизию необходимо проводить и при подготовке к внедрению новой версии приложения.

Мониторинг: план отката на предыдущую версию приложения

При подготовке к внедрению приложения должен быть разработан план отката на предыдущую версию приложения. План будет приведён в исполнение, если при установки новой версии приложения обнаружена ошибка, которая делает невозможным эксплуатацию новой версии.

Мониторинг: аварийные учения

Необходимо на регулярной основе (не реже раза в месяц) организовывать аварийные учения по отработке действия инженеров в аварийной ситуации. Целью учений является проверка уровня подготовки инженеров, приобретение ими необходимых навыков и проверка планов действия в аварийной ситуации.

Журналирование: формирование сообщения

При добавлении нового сообщения в лог, требуется воспользоваться следующими вопросами для самопроверки:

– это сообщение необходимо?

– сообщение содержательно? Описывает какое событие произошло?

– сообщение содержит достаточно данных?

– сообщение содержит лишние данные? Можно ли его сократить без потери смысла?

– указан источник возникновения события?

– по сообщению можно понять причину возникновения события?

– по сообщению можно установить шаг процесса?

– сообщение связано с предыдущими шагом процесса и предыдущими сообщениями?

– сообщение является человекочитаемым?

– сообщение является машиночитаемым?

В случае, если вопросы самопроверки показывают необходимость исправления, необходимо внести соответствующие корректировки.

Журналирование: выбор уровня отладки для сообщения

Выбирать правильный уровень отладки нужно согласно следующим правилам (см. таблицу ниже).

Таблица 7 – Правила отладки

Уровень отладки	**Когда используется**
ERROR	Ошибки вызова сервисов платформы, кроме отправки метрик в сервис журналирования Ошибки интеграционных вызовов Runtime ошибки в ходе исполнения шага Workflow
WARNING	Проверки на null значений, которые не должны быть null Ошибки отправки метрик в сервис журналирования
INFO	Сообщения о переходе на шаг процесса (инициализация, исполнение)
	Сообщения о вызове и возврате из подпроцесса Сообщения о вызове и возврате из вызова внешней интеграции (интеграционного адаптера)
DEBUG	Факт входа и выхода в методы сервисов. Все входные и выходные параметры операций Все входные и выходные параметры вызовов интеграционных адаптеров (DTO) Все входные и выходные параметры вызова подпроцесса (DTO)
TRACE	Все остальное, что требуется залогировать для отладки приложения

Журналирование: достаточность логов приложения

Решение о достаточности набора логов приложения должно приниматься инженером службы эксплуатации при приёмке приложения на эксплуатацию. При недостаточности реализованного объема и подробности логов, приложение

должно быть доработано с учётом замечаний по составу и содержанию логов до передачи его в эксплуатацию.

Журналирование: чувствительная информация

При добавлении сообщения в лог, необходимо провести проверку того, что в результирующем сообщении отсутствуют персональные данные или чувствительная и конфиденциальная информация. Контроль отсутствия таких данных в сообщениях должен осуществляться во время тестирования приложения и при приёмке приложения в эксплуатацию.

Журналирование: ресурсоёмкие операции

Для вывода сообщения, для формирования которого требуются существенные процессорные ресурсы, требуется отдельная проверка о том, что уровень логирования соответствует данному сообщению.

Для вывода сообщений рекомендуется использовать уровень DEBUG или ниже.

Журналирование: расстановка сообщений в функции

В лог функции необходимо передавать:

– факты входа и выхода из функции с указанием аргументов и возвращаемых значений.
– факты входа и выхода в методы сервисов.
– все входные и выходные параметры операций
– все входные и выходные параметры вызовов интеграционных адаптеров
– (DTO)
– все входные и выходные параметры вызова подпроцесса (DTO)

4.2.3 Обработка сбоев при вызове сервисов в Synapse

Интеграции между сервисами внутри прикладного приложения, строятся с использованием сервиса интеграционного взаимодействия.

В сервисе интеграционного взаимодействия предусмотрены следующие механизмы обеспечения отказоустойчивости:

– Устранение сбойного звена из цепочки вызова или автоматический выключатель (circuit breaker).
– Повторные вызовы (retries).
– Ограничение времени ожидания ответа (timeouts).
– Имитация сбоев (fault injection).

Устранение сбойного звена из цепочки вызова или автоматический выключатель (circuit breaker)

При сервисных взаимодействиях может возникать ситуация, когда вызываемый сервис или его реплика (на рисунке ниже Сервис B) недоступен или работает медленно. Для того чтобы максимально быстро выявить неработающий сервис (принцип fail fast) и предпринять автоматические действия по отключению

его от потока вызовов используется механизм "автоматический выключатель" или circuit breaker (далее Выключатель). Отключение сбойного сервиса от потока вызовов обеспечивает отсутствие задержек на его вызов (и ожидание таймаута) на стороне вызывающего сервиса и сокращение затрат ресурсов, связанных с выполнением данного вызова (память, процессор, сеть). Для реализации подобного Выключателя в составе сервиса интеграционного взаимодействия используется компонент «Сервисный прокси», который реализует политики отключения неработающего сервиса от потока вызовов. Схема работы выключателя представлена на рисунке.

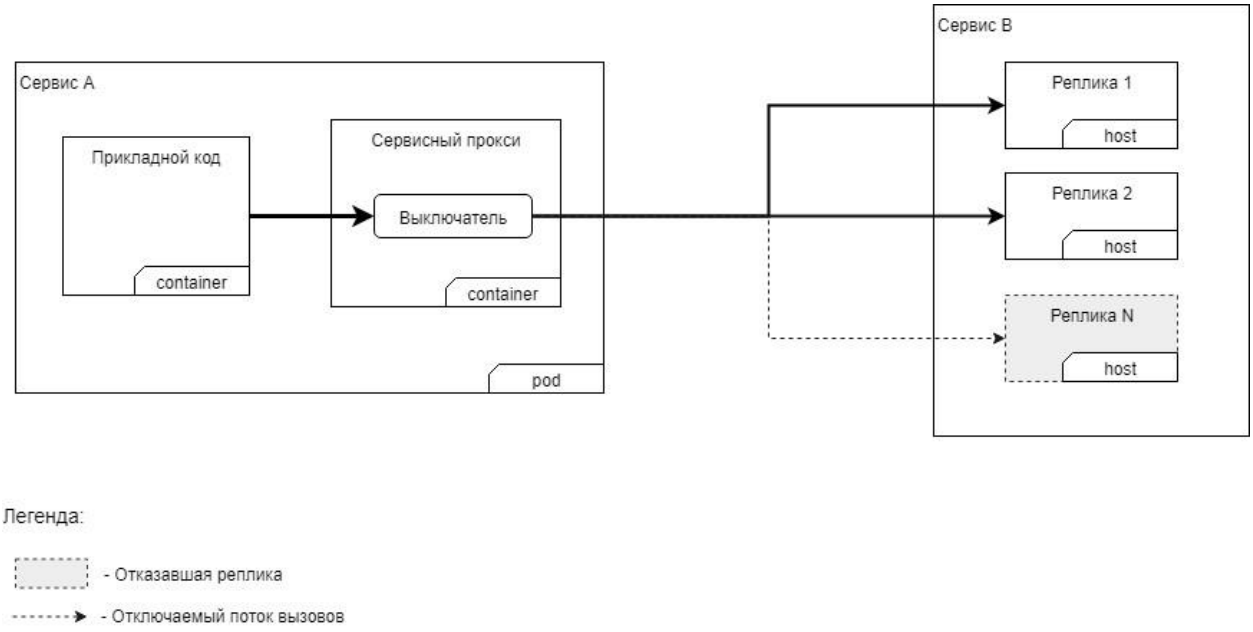

Рисунок 9– Схема механизма «circuit breaker»

Схема работает следующим образом:

В исходном состоянии все реплики сервиса B работают корректно. Сервисный прокси распределяет поток запросов равномерно по всем репликам Сервиса B.

В определенный момент времени сервисный прокси начинает получать системные ошибки (сетевые или серверные) при вызове одной из реплик Сервиса B. При получении определенного числа последовательных ошибок (настраиваемый параметр), сервисный прокси понимает, что реплика сервиса недоступна и должна быть временно отключена от потока вызовов. Для этого сервисный прокси переводит Выключатель в положение «open», исключая данную реплику из балансировки. При этом поток вызовов перераспределится по оставшимся «живым» репликам. Если сервис B имеет единственную реплику, тогда все запросы к нему будут заканчиваться мгновенной ошибкой в прикладном коде Сервиса A.

По истечении таймаута отключения потока вызовов (настраиваемый параметр) сервисный прокси переведет Выключатель в положение «closed» и включит поток вызовов на данную реплику.

Повторные вызовы (retries)

Механизм повторных вызовов позволяет выполнить несколько попыток (настраиваемый параметр) вызова сервиса до возвращения в вызывающий сервис ошибки вызова. Это позволяет скрыть от прикладного кода вызывающего сервиса кратковременную недоступность вызываемого сервиса, например, по причине "моргания" сети. Интервал вызова между повторными вызовами выбирается автоматически на основе внутреннего алгоритма. Данный механизм реализуется в компоненте «Сервисный прокси» сервиса интеграционного взаимодействия.

Ограничение времени ожидания ответа (timeouts)

Механизм ограничения времени ожидания ответа (timeouts) позволяет ограничить время ожидания ответа от вызывающего сервиса. Данный механизм позволяет избежать «подвисания» процесса получения ответа от вызывающего сервиса на непредсказуемое время. Данный механизм реализуется в компоненте «Сервисный прокси» сервиса интеграционного взаимодействия.

Имитация сбоев (fault injection)

Механизм имитации сбоев позволяет воспроизвести сбой прямо в среде исполнения в управляемом режиме (на определенном проценте вызовов) чтобы проверить что вызывающий сервис корректно обрабатывает данные сбои. Может быть использована имитация двух типов сбоев - задержки при вызове (выставляется время задержки) и ошибки при вызове (выставляется код воспроизводимой ошибки, например, HTTP 503). Механизм позволяет подключать имитацию сбоев динамически прямо в среде исполнения. Данный механизм реализуется в компоненте «Сервисный прокси» сервиса интеграционного взаимодействия.

4.3 Обеспечение масштабируемости

Одним из способов обеспечения масштабируемости ГИС является механизм шардирования - способ горизонтального масштабирования, в котором прикладные приложения вместе с данными разделяются на изолированные области (шарды).»

4.3.1 Масштабирование компонентов, не хранящих состояние

Схема масштабирования компонентов, не хранящих состояние показана на рисунке ниже.

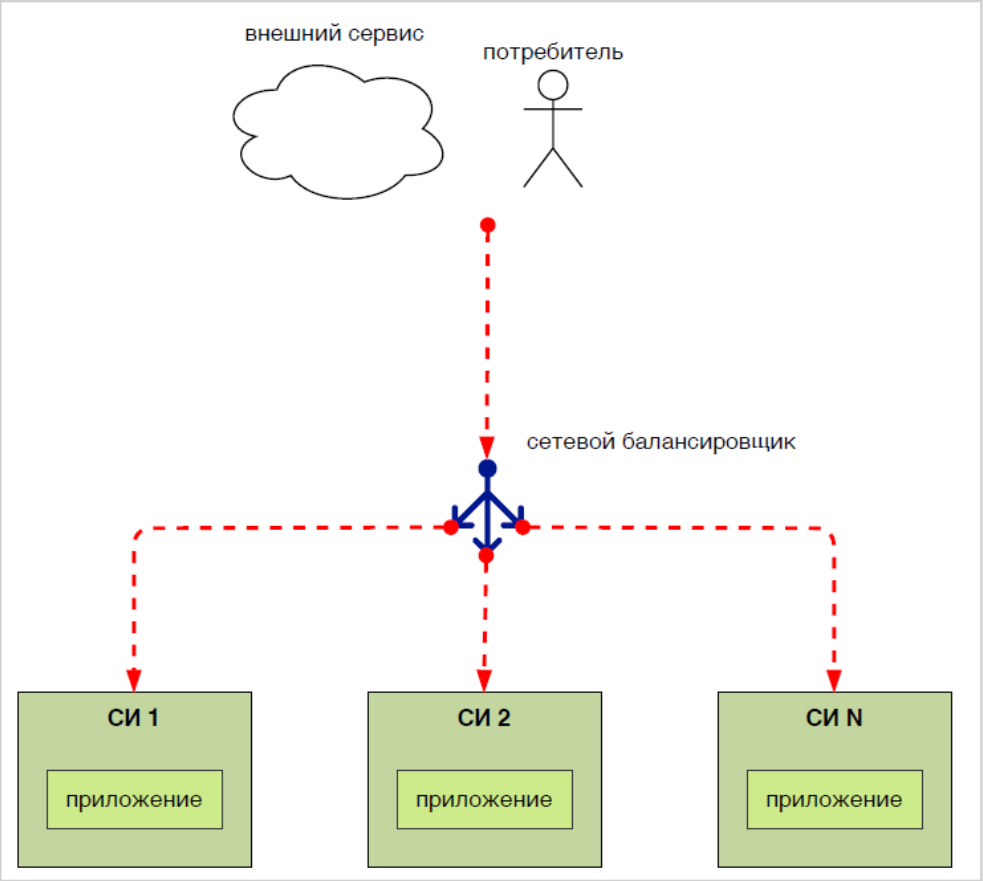

Рисунок 10 - Схема масштабирования компонентов, не хранящих состояние

Элемент	**Описание**
сетевой балансировщик	аппаратный или программный компонент, позволяющий направлять трафик на разные сетевые узлы по заранее заданным правилам
СИ 1...N	среды исполнения, на которых развёрнуто масштабируемое приложение
БД	база данных

При данной схеме горизонтальное масштабирование осуществляется путём добавления экземпляров СИ в программно-аппаратный комплекс, а входящий трафик от потребителей приложения распределяется между экземплярами СИ на балансировщике.

Данная схема предполагает, что данные не хранятся на экземплярах СИ и приложение на любом экземпляре СИ выдаст одинаковый для всех экземпляров ответ. При этом невозможно реализовать механизм хранения сессий на стороне приложения. Для обхода данного ограничения можно применить следующие дополнительные паттерны:

Прилипание сессий - при первом обращении потребителя на один из экземпляров СИ приложение выдаёт потребителю признак, идентифицирующий конкретный экземпляр СИ, и при последующих обращениях потребителя на уровне балансировщика все запросы направляются на первоначальный экземпляр СИ, т.е. сессия прилипает к экземпляру

Централизованное хранилище сессионных данных - любой экземпляр СИ сохраняет и получает данные сессии пользователя из общего хранилища

4.3.2 Шардирование баз данных

Схема шардирования баз данных приведена на рисунке ниже (см. Рисунок 11).

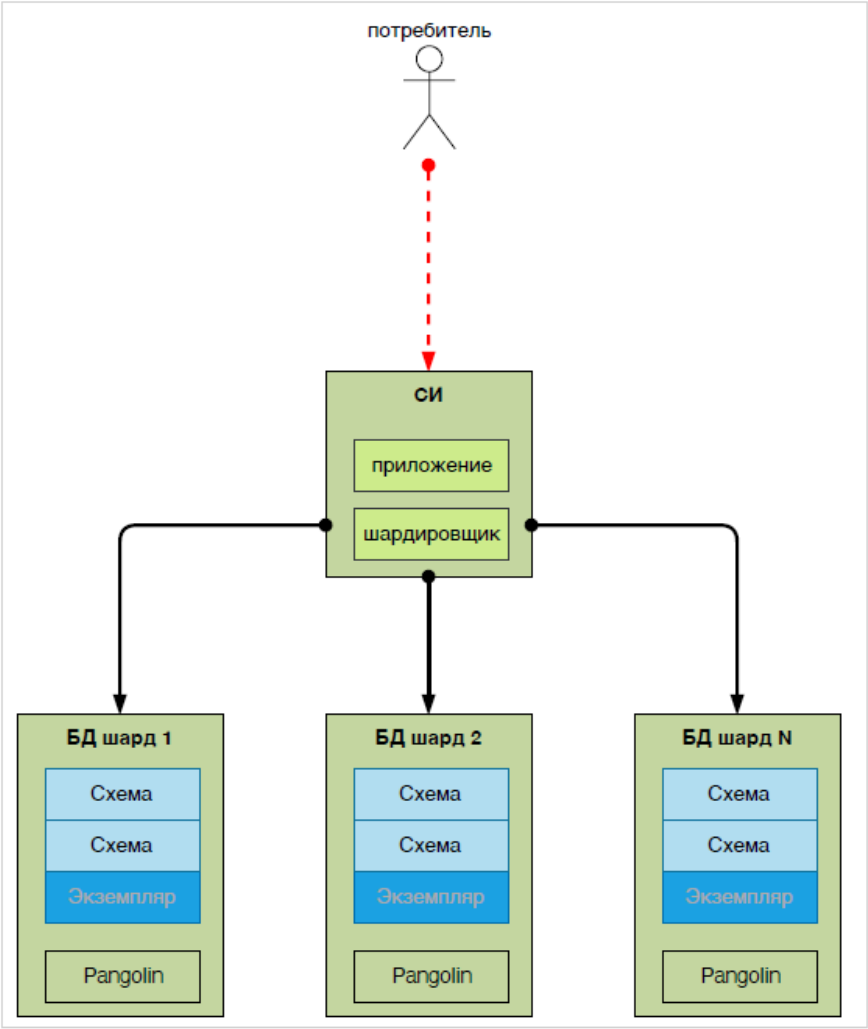

Рисунок 11 - Схема шардирования баз данных

Масштабирование осуществляется путём разнесения объема хранимых данных на несколько серверов СУБД и распределение запросов на них на стороне приложения.

Пример: предположим, что необходимо хранить данные пользователей в БД шард 1. Каждый пользователь имеет суррогатный ключ - userID. По мере добавления пользователей этот ключ увеличивается. Когда будет решено, что настало время горизонтального масштабирования, в приложении добавляется ключ шардирования - userID. Для пользователей, у которых userID < 5000, шардировщик направляет запросы в БД шард 1, а для тех, у кого больше 5000 - на БД шард 2.

4.3.3 Шардирование приложения

Схема шардирования приложения приведена на рисунке ниже (см. Рисунок 12).

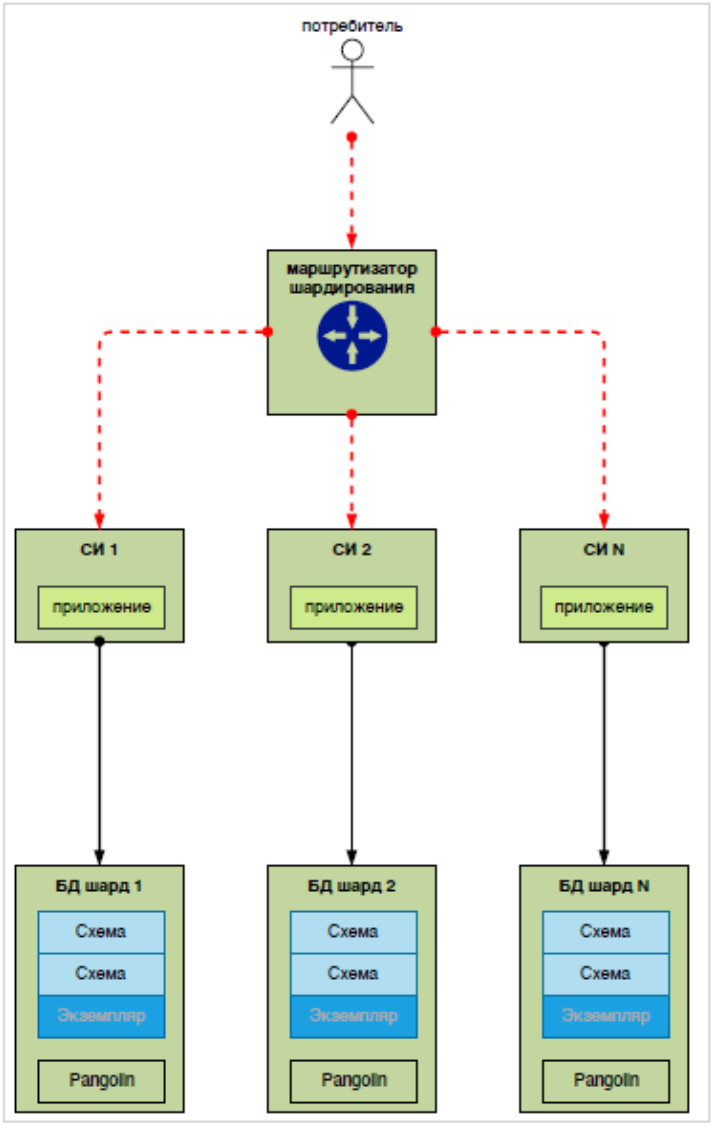

Рисунок 12 - Схема шардирования приложения

Данная схема шардирования предполагает масштабирование «стаканами» - комплекс из прикладных компонентов и систем хранения данных с выбором нужного шарда на маршрутизаторе шардирорвания.

Пользователь проходит процедуру аутентификации и создаётся сессия пользователя. В сессии пользователя есть атрибут «region», в котором содержится информация о коде региона, в котором обслуживается пользователь. Маршрутизатор nginx по параметру в cookie, приходящем в запросе от пользователя, маршрутизирует запросы на группу серверов, которые сконфигурированы для нужного региона

4.4 Обеспечение надежности

Надёжность – характеристика системы, состоящая из доступности и устойчивости. Надёжная система не только позволяет потребителям использовать свой функционал согласно заявленным метрикам, но также сохраняет это свойство при изменении профилей нагрузки, наплыву потребителей и т.д.

Один из паттернов повышения надёжности – CQRS, или разделение запросов на чтение и на запись.

Паттерн CQRS на базе сервиса управления очередями сообщений и сервиса Key-value СУБД (Ignite)

В данном паттерне приложение при необходимости изменения данных отправляет изменения в кластер сервиса управления очередями сообщений для последующей асинхронной обработки изменений. Данный звено обеспечивает сглаживание пиков нагрузки и возможность увеличения производительности за счёт увеличения количества обработчиков изменений. Запросы на изменение попадают в обработчик, который непосредственно вносит изменения в основное хранилище или отправляет заявку во внешнюю систему, после чего дублирует изменения в кэширующую базу данных Ignite SE. При необходимости чтения данных запросы идут сразу в кэш, что ускоряет процесс формирования ответа и не загружает основное хранилище ГИС.

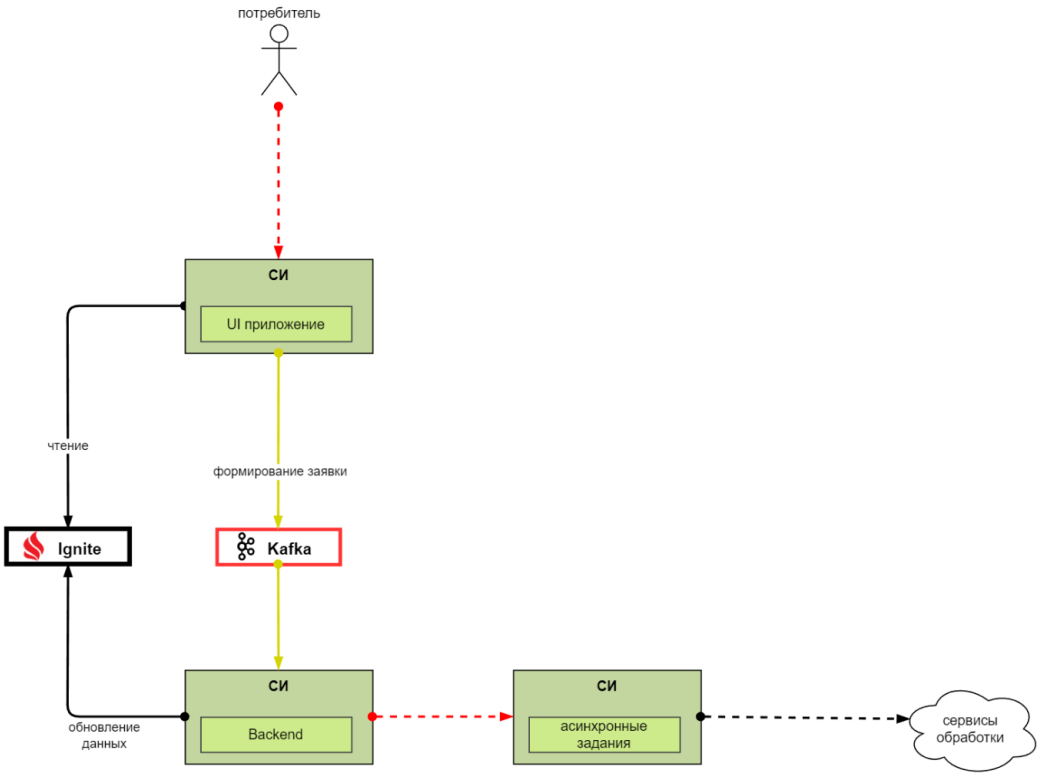

Рисунок 13 – Схема построения решения по обеспечению надежности с применением паттерна CQRS на базе сервиса управления очередями сообщений и сервиса Key-value СУБД (Ignite)

Паттерн CQRS для сервиса транзакционной СУБД

В данном решении операции чтения и записи разделены по репликам кластера БД, таким образом, операции чтения не влияют на операции записи, что позволяет ИС выдерживать изменения профиля нагрузки и даже увеличить производительность в целом за счёт добавления дополнительных реплик БД.

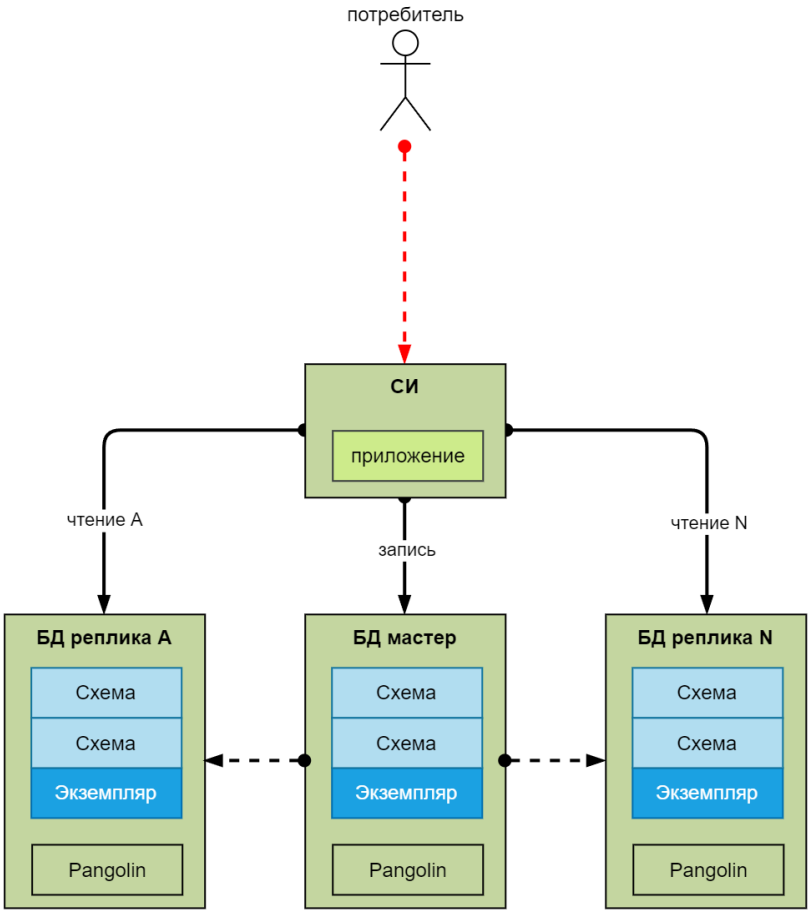

Рисунок 14 - Схема построения решения по обеспечению надежности с применением паттерна CQRS для сервиса транзакционной СУБД