

**МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И
МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**ЕДИНАЯ ЦИФРОВАЯ ПЛАТФОРМА РОССИЙСКОЙ ФЕДЕРАЦИИ
«ГОСТЕХ» ДЛЯ СОЗДАНИЯ, РАЗВИТИЯ И ЭКСПЛУАТАЦИИ
ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ**

**МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ «БАЗОВЫЕ СЕРВИСЫ ЕДИНОЙ
ЦИФРОВОЙ ПЛАТФОРМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ «ГОСТЕХ».
ОСНОВНЫЕ ТРЕБОВАНИЯ К СОСТАВУ И ФУНКЦИЯМ»**

версия 1.0

**Москва
2022**

Содержание

1. Термины и определения	1
2. Общие положения	8
3. Состав базового набора сервисов	9
3.1 Состав сервисов работы с данными	10
3.2 Состав интеграционных сервисов	10
3.3 Состав сервисов управления	11
3.4 Состав служебных технологических сервисов	11
3.5 Состав сервисов интеграции с инфраструктурой электронного правительства	11
4. Требования к базовым сервисам	12
4.1 Общие требования к сервисам	12
4.1.1 Требования к защите информации	12
4.1.2 Требования к надежности	14
4.1.3 Требования к доступности	15
4.1.4 Требования по диагностируемости	16
4.1.5 Требования по управлению доступом и учетными записями	16
4.1.6 Требования к API	17
4.1.7 Обеспечение технической поддержки	17
4.1.8 Требования к документации	18
4.1.9 Требования к мультитенантности	18
4.2 Основные требования к сервисам работы с данными	19
4.2.1 Требования к сервису транзакционной СУБД	20
4.2.2 Требования к сервису ширококолоночной СУБД	21
4.2.3 Требования к сервису Key-value СУБД (in-memory)	22
4.2.4 Требования к сервису СУБД полнотекстового индекса	23
4.2.5 Требования к сервису СУБД аналитического хранилища данных	24
4.2.6 Требования к сервису СУБД аналитических витрин хранилища данных ..	25
4.2.7 Требования к сервису СУБД хранения неструктурированных данных	27
4.2.8 Требования к сервису объектного хранилища	27
4.3 Основные требования к интеграционным сервисам	29
4.3.1 Требования к сервисам интеграционного взаимодействия	29

4.3.2 Требования к сервису управления очередями сообщений	30
4.4 Основные требования к сервисам управления	31
4.4.1 Требования к сервису управления микросервисами	31
4.4.2 Требования к сервису управления процессами	31
4.5 Основные требования к служебным технологическим сервисам.....	32
4.5.1 Требования к сервисам IAM	32
4.5.2 Требования к сервису журналирования.....	32
4.5.3 Требования к сервису аудита.....	34
4.5.4 Требования к сервису мониторинга	35
4.6 Основные требования к сервисам интеграции с инфраструктурой электронного правительства	37
4.6.1 Требования к сервису «Типовое тиражируемое программное обеспечение витрин данных» («Витрина НСУД»)	37
4.6.2 Требования к сервису «Шлюз Единой системы идентификации и аутентификации»	37
4.6.3 Требования к сервису «Платформа государственных сервисов»	38
5. Требования к поставщику	39
6. Требования к юридическому оформлению	41
7. Требования к биллингу	41
8. Требования к порталу самообслуживания	41
9. Требования о подключении к ФГИС «Управление ГосТех»	42
Приложение А (справочное) Пример целевых показателей по обработке обращений, классифицированных как инциденты.....	43

1. Термины и определения

В настоящих методических рекомендациях применены следующие термины и сокращения с соответствующими определениями:

Термин, сокращение	Определение
Сервис	Программное обеспечение, реализующее дополнительные функциональные потребности, предназначенное для функционирования в отдельном процессе и взаимодействующее с другими сервисами и сторонними приложениями с использованием стандартизированных интерфейсов. Сервисы могут быть написаны на разных языках программирования и использовать разные технологии хранения данных.
Пользователь ЕЦП «ГосТех»	Обеспечивающие создание, развитие, эксплуатацию ГИС на ЕЦП «ГосТех» и (или) использование цифровых продуктов на ЕЦП «ГосТех» государственные органы, государственные внебюджетные фонды, иные организации, уполномоченные на осуществление мероприятий по созданию, развитию, эксплуатации государственных информационных систем в соответствии с нормативными правовыми актами Российской Федерации
Поставщик	Юридическое лицо, предоставляющее Сервис
ЕЦП «ГосТех»	Цифровая экосистема создания, развития и эксплуатации государственных информационных систем, включающая в себя единую программно-аппаратную среду, цифровые продукты, информацию, информационные технологии, государственные информационные системы

	ЕЦП «ГосТех», необходимые для реализации функций ЕЦП «ГосТех», а также совокупность нормативных правовых, организационных, методологических правил и процедур, обеспечивающих деятельность участников ЕЦП «ГосТех»
ГИС на ЕЦП «ГосТех»	Государственные информационные системы, создаваемые, развиваемые, эксплуатируемые с использованием программно-аппаратной среды, цифровых продуктов, инструментов, информационных технологий ЕЦП «ГосТех» для реализации полномочий государственных органов и обеспечения обмена информацией между ними, а также в иных установленных федеральными законами целях
SIEM-система	Системы управление информацией о безопасности и управлением событиями безопасности
Конечный пользователь	Физические и юридические лица, а также иные лица, получающие государственные (муниципальные) услуги и (или) государственные (муниципальные) функции с использованием ГИС на ЕЦП «ГосТех» или готовых облачных Сервисов на ЕЦП «ГосТех»
Мультитенантность	Элемент архитектуры программного обеспечения, где единый экземпляр приложения, сервиса платформы или инфраструктура (далее – мультитенантные объекты), изолированно обслуживает множество клиентов-организаций (Tenancy – аренда, Multitenancy – множественная аренда)
Оператор ЕЦП «ГосТех»	Министерство цифрового развития, связи и массовых коммуникаций Российской

	Федерации или подведомственное ему казенное учреждение
Государственные органы	Федеральные органы исполнительной власти, органы исполнительной власти субъектов Российской Федерации и иные органы государственной власти, образуемые в соответствии с законодательством Российской Федерации, законодательством субъектов Российской Федерации
ГОСТ-TLS	Реализация протокола TLS средствами криптографической защиты информации, использующими российские криптографические алгоритмы и соответствующими требованиям ФСБ России к средствам криптографической защиты информации.
VPN с ГОСТ-шифрованием	Реализация технологии VPN средствами криптографической защиты информации, использующими российские криптографические алгоритмы и соответствующими требованиям ФСБ России к средствам криптографической защиты информации.

В настоящем стандарте применены следующие сокращения:

Сокращение	Определение
ACID	Atomicity, Consistency, Isolation, Durability (Атомарность, Согласованность, Изолированность, Прочность)
ACL	Access Control List (список управления доступом)
ANSI	American national standards institute (Американский национальный институт стандартов — объединение американских промышленных и деловых групп, разрабатывающее торговые и коммуникационные стандарты)

Сокращение	Определение
API	Application Programming Interface (набор классов, процедур, функций, структур или констант, которыми одна компьютерная программа может взаимодействовать с другой программой)
BITSET	Индекс по битовой маске
BPM	Business Process Management (система управления бизнес-процессами)
CLI	Command Line Interface (интерфейс командной строки)
CPU	Central Processing Unit (центральный процессор)
CSV	Comma-Separated Values (текстовый формат, предназначенный для представления табличных данных)
DLQ	Dead Letter Queue (очереди, куда могут перенаправляться сообщения, которые не смогли обработать получатели в обычных очередях)
EDIFACT	Electronic Data Interchange for Administration, Commerce and Transport
EQL	Event Query Language (язык запросов ко временным рядам)
FHIR	Fast Healthcare Interoperability Resources (ресурсы быстрого взаимодействия в сфере здравоохранения)
FIFO	First In — First Out (последовательный способ организации обработки сообщений в очередях)
FIX	Financial Information eXchange (протокол обмена финансовой информацией)
GSSAPI	Generic Security Services API (общий программный интерфейс сервисов безопасности)
HASH	Индекс, требует уникальности полей
HDD	Hard Disk Drive (накопитель на жёстких магнитных дисках)
HDFS	Hadoop File System (файловая система Hadoop)

Сокращение	Определение
HTTP/ HTTPS	HyperText Transfer Protocol (Secure)
IAM	Identity and Access Management (система управления идентификацией и доступом к информационным ресурсам)
IMAP	Internet Message Access Protocol (протокол прикладного уровня для доступа к электронной почте)
IP	Internet Protocol (маршрутизируемый протокол сетевого уровня стека TCP/IP)
ISO	International Organization for Standardization (Международная организация по стандартизации, ИСО)
JDBC	Java DataBase Connectivity (платформенно независимый промышленный стандарт взаимодействия Java-приложений с различными СУБД)
JSON	JavaScript Object Notation (текстовый формат обмена данными, основанный на JavaScript)
LDAP	Lightweight Directory Access Protocol (протокол прикладного уровня для доступа к службе каталогов X.500)
ODBC	Open Database Connectivity (программный интерфейс доступа к базам данных)
ODS	Operational Data Store (оперативное хранилище данных)
PaaS	Platform as a Service (Платформа как услуга)
PAM	Privileged Access Management (Системы контроля действий привилегированных пользователей)
POP	Post Office Protocol (Протокол почтового офиса)
POST	Метод запроса, поддерживаемых HTTP протоколом
RADIUS	Remote Authentication in Dial-In User Service (протокол для реализации аутентификации, авторизации и сбора сведений об использованных ресурсах)
RAM	Random Access Memory (оперативная память)

Сокращение	Определение
RDBMS	Relational Database Management System (Реляционная СУБД)
REST	Representational State Transfer (архитектурный стиль взаимодействия компонентов распределённого приложения в сети)
RTREE	Многомерный индекс
SAML	Security Assertion Markup Language (язык разметки, основанный на языке XML)
SAS HDD	Serial Attached SCSI (последовательный компьютерный интерфейс)
SATA HDD	Serial Advanced Technology Attachment (последовательный интерфейс обмена данными с накопителями информации)
SDK	Software Development Kit (комплект для разработки программного обеспечения)
SE	SE-Linux (реализация системы принудительного контроля доступа)
SIEM	Security Information and Event Management (управление информацией о безопасности и управление событиями безопасности)
SLA	Service Level Agreement (Соглашение об уровне услуг)
SMTP	Simple Mail Transfer Protocol (сетевой протокол, предназначенный для передачи электронной почты в сетях TCP/IP)
SOAP	Simple Object Access Protocol (протокол обмена структурированными сообщениями в распределённой вычислительной среде)
SQL	Structured Query Language (декларативный язык программирования, применяемый для создания, модификации и управления данными в реляционной базе данных)
SQS	Simple Queue Service (сервис очередей сообщений)

Сокращение	Определение
SSD	Solid-State Drive (твердотельный накопитель)
SSL	Secure Sockets Layer (уровень защищённых сокетов)
SSPI	Security Support Provider Interface (интерфейс поставщика поддержки безопасности)
TLS	Transport Layer Security (криптографический протокол, обеспечивающий защищенную передачу данных в компьютерной сети)
TPC	Transaction Processing Performance Council (совет по производительности обработки транзакций)
TREE	Индекс для пространственных данных
TTL	Time to Live (время жизни пакета данных в протоколе IP)
VPN	Virtual private network (англ. «виртуальная частная сеть», технология защищенного соединения)
XLS	Файл в формате Microsoft Excel 97-2003
XML	eXtensible Markup Language (расширяемый язык разметки)
YAML	YAML для управления кластером
YARN	Yet Another Resource Negotiator (система планирования заданий и управления кластером)
YCSB	Yahoo! Cloud Serving Benchmark (сравнительный анализ облачного обслуживания)
БД	База данных
ВН	Время недоступности сервиса
ГБ	Гигабайт
ГИС	Государственная информационная система
ГОСТ	Государственный стандарт
ЕСИА	Единая система идентификации и аутентификации

Сокращение	Определение
ИТ	Информационная технология
ОГВ	Орган государственной власти
ОМСУ	Орган местного самоуправления
ОС	Операционная система
ПО	Программное обеспечение
ПОДД	Подсистема обеспечения доступа к данным
ПБ	Петабайт
РСУБД	Реляционная система управления базами данных
СВД	Согласованное время доступности сервиса
СМЭВ	Система межведомственного электронного взаимодействия
СПО	Специальное программное обеспечение
СУБД	Система управления базами данных
ТБ	Терабайт
ФЛ	Физическое лицо
ФСТЭК	Федеральная служба по техническому и экспортному контролю
ЦОД	Центр обработки данных
ЮЛ	Юридическое лицо

2. Общие положения

Цифровые продукты ЕЦП «ГосТех» предназначены для создания, развития и эксплуатации ГИС на ЕЦП «ГосТех». К цифровыми продуктам ЕЦП «ГосТех» относятся в том числе:

- цифровые продукты, предоставляющие инфраструктурные вычислительные ресурсы и сервисы, обеспечивающие информационно-технологическое взаимодействие информационных систем, используемых для

предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме;

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

- цифровые продукты, реализующие дополнительные функциональные потребности, поставляемые в виде дистрибутивов программного обеспечения, в виде прикладных сервисов, работающих в облачной инфраструктуре, и в виде исходного кода, включенного в государственную библиотеку типовых программных компонентов информационных систем;

- цифровые продукты, обеспечивающие функции защиты информации, включающие в том числе обнаружения и блокирования сетевых атак.

В рамках настоящих методических рекомендаций определяются требования к базовым сервисам ЕЦП «ГосТех», которые предоставляются Пользователям ЕЦП «ГосТех» по модели Platform as a Service (PaaS, «платформа как услуга»). Данная модель предполагает, что Пользователь ЕЦП «ГосТех» получает удаленный доступ посредством облачных вычислений к набору базовых сервисов ЕЦП «ГосТех», размещенному у Поставщика.

Требования к цифровым продуктам, предоставляющим инфраструктурные вычислительные ресурсы и сервисы определены в методических рекомендациях по управлению динамической инфраструктурой.

Требования к цифровым продуктам, реализующим дополнительные функциональные потребности определены в методических рекомендациях по включению сервисов в ЕЦП «ГосТех».

3. Состав базового набора сервисов

Сервисы в базового набора подразделяются на следующие типы:

- 1) сервисы работы с данными;
- 2) интеграционные сервисы;
- 3) сервисы управления;
- 4) служебные технологические сервисы;

5) сервисы интеграции с инфраструктурой электронного правительства.

3.1 Состав сервисов работы с данными

В состав сервисов работы с данными ЕЦП «ГосТех» входят:

1) Сервис транзакционной СУБД – СУБД общего назначения, которая поддерживает таблично ориентированную модель данных;

2) Сервис ширококолоночной СУБД – СУБД специального назначения, которая ориентирована на большое количество операций согласованного чтения с элементами простой аналитической обработки над максимальными объемами данных не менее 300 ТБ;

3) Сервис Key-value СУБД (in-memory) – горизонтально масштабируемая СУБД с доступом по ключу, которая применяется для ускоренной работы с данными и использует оперативную память для их хранения и обработки;

4) Сервис СУБД полнотекстового индекса – горизонтально масштабируемая СУБД, которая предназначена для быстрого поиска информации в больших объемах (массивах) текста;

5) Сервис СУБД аналитического хранилища данных – СУБД специального назначения, которая используется для построения корпоративных хранилищ данных со сложносоединенными запросами при максимальных размерах баз не менее 200 ТБ;

6) Сервис СУБД аналитических витрин хранилища данных – СУБД специального назначения, которая используется для однотоабличных аналитических запросов с максимальными размерами баз не менее 500 ТБ;

7) Сервис СУБД хранения неструктурированных данных – СУБД специального назначения, которая используется для обработки данных в форматах NoSQL и предназначена для обслуживания не менее 1 ПБ на одну аренду;

8) Сервис объектного хранилища – объектное хранилище для извлечения данных любых объемов из любого места.

3.2 Состав интеграционных сервисов

В состав интеграционных сервисов ЕЦП «ГосТех» входят:

1) Сервисы интеграционного взаимодействия – сервисы для создания и управления API, а также для настройки интеграции приложений и сервисов;

2) Сервис управления очередями сообщений – распределенный программный брокер сообщений для обмена сообщениями между компонентами распределенных приложений и микросервисов.

3.3 Состав сервисов управления

В состав сервисов управления ЕЦП «ГосТех» входят:

- 1) Сервис управления микросервисами – инструмент управления контейнерами, обеспечивающий автоматизацию и управление жизненным циклом контейнеров и сервисов;
- 2) Сервис управления процессами – сервис для автоматизации бизнес-процессов в бессерверном режиме, включая оркестрацию микросервисов и пользовательских задач.

3.4 Состав служебных технологических сервисов

В состав служебных технологических сервисов ЕЦП «ГосТех» входят:

- 1) Сервис IAM – сервис идентификации и контроля доступа, предназначенный для централизованного управления правами доступа пользователей к ресурсам ЕЦП «ГосТех»;
- 2) Сервис журналирования – сервис для агрегации и чтения логов пользовательских приложений и ресурсов ЕЦП «ГосТех»;
- 3) Сервис аудита – сервис сбора и выгрузки аудитных записей ресурсов ЕЦП «ГосТех»;
- 4) Сервис мониторинга – сервис мониторинга состояния ресурсов и программных компонентов (сервисов) ЕЦП «ГосТех».

3.5 Состав сервисов интеграции с инфраструктурой электронного правительства

В состав сервисов интеграции с инфраструктурой электронного правительства входят:

- 1) Сервис «Типовое тиражируемое программное обеспечение витрин данных» («Витрина НСУД») – комплекс программных и технических средств, обеспечивающий загрузку, хранение и предоставление данных посредством единой системы межведомственного электронного взаимодействия (СМЭВ) с использованием регламентированных запросов;
- 2) Сервис «Шлюз Единой системы идентификации и аутентификации», предназначенный для интеграции с Единой системой идентификации и аутентификации (ЕСИА). Данный сервис обеспечивает:
 - получение данных по ФЛ;
 - получение данных по ЮЛ и ОГВ;
 - работу с несколькими мнемониками и разными наборами данных.

3) Сервис «Платформа государственных сервисов» – комплекс программных и технических средств, обеспечивающий выполнение участниками информационного взаимодействия административных процедур (действий) при предоставлении государственных, муниципальных и иных услуг, исполнении государственных, муниципальных и иных функций, содержащихся в разделах федерального реестра.

4. Требования к базовым сервисам

В настоящем разделе приведены требования к назначению, функциям и характеристикам базовых сервисов (базовому набору сервисов) ЕЦП «ГосТех».

4.1 Общие требования к сервисам

Все базовые сервисы ЕЦП «ГосТех» должны быть включены в Единый реестр российских программ для электронных вычислительных машин и баз данных. Исключение могут составлять сервисы, созданные в рамках государственных контрактов.

Базовые сервисы и их компоненты должны быть совместимы, по крайней мере, с одной из операционных систем на базе Linux, внесенных в Единый реестр российских программ для электронных вычислительных машин и баз данных.

4.1.1 Требования к защите информации

Разработка Сервиса, включаемого в состав ЕЦП «ГосТех», должна проводиться с учётом общих требований к содержанию и порядку выполнения работ, связанных с созданием безопасного (защищенного) программного обеспечения, а также формированием (поддержанием) среды обеспечения оперативного устранения выявленных ошибок программного обеспечения и уязвимостей в соответствии с требованиями ГОСТ Р 56939-2016 «Защита информации. Разработка безопасного программного обеспечения. Общие требования» (далее – ГОСТ Р 56939-2016).

В отношении предоставляемого поставщиком Сервиса должен быть проведен анализ уязвимостей по требованиям к оценочному уровню доверия (далее – ОУД) в соответствии с требованиями национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 15408-3-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности», утвержденного приказом Федерального агентства по техническому регулированию и метрологии от 08.11.2013 № 1340-ст.

В качестве подтверждения соответствия вышеуказанным требованиям Поставщик может предоставить заверенную в установленном порядке копию одного из следующих документов:

- сертификат соответствия по требованиям безопасности информации ФСТЭК России;
- заключение испытательной лаборатории об оценке соответствия прикладного программного обеспечения Сервиса требованиям к оценочному уровню доверия;
- оценку соответствия реализованных Поставщиком мер по разработке безопасного программного обеспечения с приложением результатов проведенных испытаний по выявлению уязвимостей в программном обеспечении Сервиса.

В соответствии с требованиями приказов ФСТЭК России от 11.02.2013 № 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах", от 03.04.2018 № 55 "Об утверждении Положения о системе сертификации средств защиты информации" Сервисы, являющиеся средствами защиты информации, должны быть сертифицированы на соответствие требованиям по безопасности информации, установленным нормативными правовыми актами ФСТЭК России, а также техническими условиями, техническим заданием, заданием по безопасности, согласованными заявителями на сертификацию с ФСТЭК России.

Все применяемые средства криптографической защиты информации должны соответствовать требованиям ФСБ России.

Вместе с этим, для усиления подсистемы защиты информации сервисы должны соответствовать следующим основным требованиям:

- резервное копирование программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры;
- многофакторная аутентификация для защиты доступа к облачным службам;
- поддержка программного или аппаратного VPN с ГОСТ-шифрованием;
- возможность доступа к веб-консоли и API управления облачными ресурсами с использованием ГОСТ-TLS;
- управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры;

- обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов.

Кроме того, Поставщик в части поддержки безопасности ПО обеспечивает реализацию:

- процедур отслеживания и исправления обнаруженных ошибок и уязвимостей программного обеспечения, входящего в состав ЕЦП «ГосТех»;
- определение способов и сроков доведения Поставщиком до Оператора ЕЦП «ГосТех» и Пользователей ЕЦП "ГосТех» информации об уязвимостях программного обеспечения, о компенсирующих мерах по защите информации или ограничениях по применению программного обеспечения, способов получения пользователями программного обеспечения его обновлений, проверки их целостности и подлинности;
- наличие процедур информирования Оператора ЕЦП «ГосТех» и Пользователей ЕЦП «ГосТех» об окончании поддержки программного обеспечения.

Сервис и его компоненты должны осуществлять отправку событий безопасности, связанных с действиями Конечных пользователей в системе в централизованный сервис аудита ЕЦП «ГосТех» (см. раздел 4.5.3 настоящих методических рекомендаций).

Состав, формат и иные требования к отслеживаемым событиям безопасности Сервиса, передаваемые в централизованный компонент аудита ЕЦП «ГосТех», определяются на этапе формирования требований по безопасности информации и разработки Модели угроз безопасности информации.

4.1.2 Требования к надежности

Должны быть определены требования к надежности Сервиса, а именно:

- состав и количественные значения показателей надежности функционирования Сервиса в целом и/или его компонентам, обеспечивающим реализацию одного или нескольких процессов предоставления Сервиса;
- перечень аварийных ситуаций, по которым должны быть регламентированы требования к надежности, и значения соответствующих показателей;
- требования к надежности технических средств на базе которых должен быть развернут (будет функционировать) Сервис;

- требования к методам оценки и контроля показателей надежности на разных этапах жизненного цикла Сервиса в соответствии с действующими нормативно-техническими документами.

Должно быть предусмотрено сохранение работоспособности Сервиса при некорректных действиях Конечных пользователей и сохранение целостности данных при нештатном завершении работы Сервиса (отказ рабочей станции, потеря сетевого доступа и т.п.).

Сервис должен предоставлять механизмы обеспечения сохранности данных через применение процедур резервного копирования и восстановления, описанных в документации Сервиса.

4.1.3 Требования к доступности

В документации Сервиса должен быть указан максимальный уровень доступности, который Сервис может обеспечить, а также необходимые для этого условия.

Совокупный показатель доступности сервиса, должен учитывать показатели доступности сервисов, от которых зависит его работоспособность.

Минимальное значение совокупного показателя доступности Сервиса устанавливается равное 99,5%, и оно не должно превышать значения показателей сервисов, от которых есть зависимость.

Для каждого сервиса показатель доступности рассчитывается отдельно.

Доступность за отчетный период рассчитывается как среднее между двумя показателями:

- общее время доступности сервиса, за указанный период (ВД);
- общее время недоступности сервиса, за указанный период (ВНД).

Формула расчёта доступности определяется следующим образом:

$$\text{Доступность} = (\text{ВД} - \text{ВНД}) / \text{ВД} * 100\%.$$

В соглашении об уровне предоставления сервиса помимо совокупного показателя доступности необходимо определить целевые значения также для следующих показателей:

- ограничение количества простоев, независимо от их длительности;
- средняя наработка на отказ – среднеарифметическое за весь период действия договора;
- среднее время подтверждения – время с момента регистрации обращения до момента подтверждения начала работ по восстановлению;
- среднее время исправления - время с момента подтверждения до момента восстановления работоспособности;

- среднее время разрешения, включающее в себя не только время, затраченное на обнаружение сбоя, диагностику проблемы и ее устранение, но и время, затраченное на предотвращение повторения проблемы.

4.1.4 Требования по диагностируемости

Сервис и его компоненты должны обеспечивать диагностику своей работоспособности путем передачи журналов и метрик в централизованную систему диагностики ЕЦП «ГосТех». Передаваемой информации должно быть достаточно для однозначной локализации уже произошедших ошибок или потенциальных проблем. Информация, поступающая от Сервиса в систему диагностики, должна позволять однозначно указать элемент или группу элементов согласно спецификации развертывания, в которой произошли ошибки или в ближайшее время прогнозируются ошибки при нарушении установленных диапазонов значений для метрик мониторинга.

Уровень логирования должен конфигурироваться и поддерживать, как минимум, следующие значения:

- DEBUG – логирование всех видов событий;
- INFO – логирование ошибок, предупреждений и сообщений;
- WARN – логирование ошибок и предупреждений;
- ERROR – логирование всех ошибок.

Для определенных уровней логирования должна быть возможность настроить передачу исчерпывающей информации обо всех действиях потребителей Сервиса (внесение, изменение, удаление и т.п.) в отношении всех объектов данных, с которыми работает Сервис.

Обязательным набором метрик является:

- метрики использования системных ресурсов (CPU, RAM, Memory);
- время исполнения входящих запросов;
- количество успешных/неуспешных выполнений входящих запросов;
- время исполнения исходящих запросов или обращений к СПО;
- количество успешных/неуспешных выполнений исходящих запросов или обращений к СПО.

4.1.5 Требования по управлению доступом и учетными записями

Сервис и его компоненты должны использовать один из протоколов:

- OpenID Connect 1.0;
- SAML 2.0;

- Kerberos;
- LDAP.

В Сервисе должна быть разработана ролевая модель, которая загружается в IAM ЕЦП «ГосТех» через интерфейс администрирования, либо при разворачивании или запуске сервиса с привилегированным доступом по одному из доступных протоколов.

Если Сервис предполагает подключение Конечных пользователей, он должен позволять осуществлять их идентификацию и аутентификацию через Сервис IAM (см. раздел 4.5.1) с использованием учетных записей единой системы идентификации и аутентификации (ЕСИА) (см. раздел 4.6.2).

4.1.6 Требования к API

Сервис должен обеспечивать обратную совместимость своих API, в том числе за счет поддержки механизмов версионирования. В случае необходимости внести в API изменения, нарушающие обратную совместимость, новая версия Сервиса рассматривается как новый Сервис и должна удовлетворять всем требованиям данных методических рекомендаций.

4.1.7 Обеспечение технической поддержки

Для оказания технической поддержки в рамках ЕЦП «ГосТех» выделяются следующие линии сопровождения:

- 1 линия – обработка обращений от Пользователей ЕЦП «ГосТех», передача обращений техническим специалистам;
- 2 линия – консультация, настройка, составление технической документации;
- 3 линия – системное сопровождение, устранение ошибок в работе сервиса.

Сервис должен предоставлять информацию относительно состава услуг и ключевых показателей технической поддержки в соответствии с Приложением А, а также способах коммуникаций при оказании технической поддержки.

Должен быть определён состав участников, зоны их ответственности, время работы с указанием графиков дежурств, способы коммуникаций при оказании технической поддержки и телефонами ответственных для эскалаций.

Должен быть представлен регламент обработки обращений, связанных со снижением или отсутствием работоспособности сервиса, в том числе с учётом взаимодействия с другими сервисами, должны быть представлены описания технологических операций, с указанием состава исполнителей, надзора,

продолжительности работ и плана действий с делением на операции, и схемы эскалаций по каждому типу обращению.

Должны быть предоставлены соглашения об уровне предоставления сервиса (SLA, OLA) которые, в том числе, должны включать описание и условия для проведения профилактических и регламентных работ, работ по резервному копированию и восстановлению данных.

Контроль предоставления согласованного уровня сервиса обеспечивается путём анализа следующих показателей:

- количество нерешенных обращений на начало периода;
- количество поступивших за период обращений;
- количество решенных за период обращений;
- количество обращений, перешедших в следующий период;
- процент обращений, решенных за период в соответствии с SLA;
- процент обращений, решенных за период с нарушением SLA;
- количество зарегистрированных проблем;
- перечень решенных проблем;
- перечень зарегистрированных запросов на изменение;
- перечень решенных запросов на изменение.

4.1.8 Требования к документации

Минимальный пакет эксплуатационной документации для базовых сервисов должен включать в себя:

- описание сервиса (назначение, перечень основных функций, выполнение которых обеспечивает сервис);
- руководство пользователя;
- регламент эксплуатации;
- руководство системного администратора (приложений/баз данных);
- руководство по установке;
- регламент управления доступностью и непрерывностью;
- технологическая карта мониторинга;
- регламент резервного копирования.

4.1.9 Требования к мультитенантности

Мультитенантный режим обеспечивает изолированное обслуживание сервисов на уровне доступа к данным и на уровне квотирования объема выделенных ресурсов при одновременной работе сервиса с несколькими конфигурациями и наборами данных нескольких Пользователей ЕЦП «ГосТех».

Сервис, обеспечивающий поддержку мультитенантного режима для различных Пользователей ЕЦП «ГосТех», должен соответствовать следующим основным требованиям и обеспечивать:

- изоляцию данных;
- изоляцию рабочей области потребителя (памяти);
- изоляцию характеристик исполнения (производительность и доступность);
- изоляцию пользовательских настроек и расширений бизнес-логики;
- безопасность, мониторинг, управление, отчетность и администрирование независимо для каждого Пользователя ЕЦП «ГосТех»;
- отслеживание и запись использования ресурсов отдельно каждым Пользователем ЕЦП «ГосТех»;
- возможность распределять ресурсы отдельно для каждого Пользователя ЕЦП «ГосТех» динамически по мере необходимости и на основе политик;
- горизонтальную масштабируемость для поддержки добавления/удаления ресурсов в режиме реального времени без прерывания работающей среды.

При этом возможны два режима использования Сервисов:

- Обособленный – режим работы, при котором разные Пользователи ЕЦП «ГосТех» используют отдельные экземпляры Сервисов в рамках одного экземпляра платформы;
- Совместный - режим работы, при котором разные Пользователи ЕЦП «ГосТех» используют один и тот же экземпляр Сервиса и работают в своих выделенных проектных областях. Доступ к проектной области и данным в ней возможен в рамках выделенной квоты ресурсов при успешной авторизации вызова на транспортном уровне для межсервисных вызовов, либо в платформенном Сервисе аутентификации и авторизации для пользовательских вызовов. Механизмы авторизации доступа к проектным областям при межсервисном взаимодействии реализуются для каждого вида транспорта.

Для обоих режимов использования Сервисов требования мультитенантности должны быть обеспечены.

4.2 Основные требования к сервисам работы с данными

Средства (системы) управления базами данных (СУБД) – программы, которые должны предоставлять возможность организации и ведения баз данных, в том числе с использованием технологии распределенного реестра.

Класс программного обеспечения СУБД по Классификатору программ для электронных вычислительных машин и баз данных (приказ Минкомсвязи России от 22.09.2020 № 486) должен соответствовать коду «02.07 Средства управления

базами данных» (или «02.09 Системы управления базами данных» по классификатору, утвержденному приказом Минкомсвязи России от 31.12.2015 № 621).

Сервисы работы с данными ЕЦП «ГосТех» должны:

- обеспечивать пользователю возможность создавать новые базы данных с идентичной логической структурой данных (деление по темам);
- позволять записывать, хранить, находить, редактировать и считывать данные;
- обеспечивать модификацию базы данных;
- позволять осуществлять ввод основной массы данных посредством считывания (записи) массива данных;
- обеспечить контроль достоверности вводимых данных в каждом поле таблиц базы данных (обязательное поле, умолчание, шаблон и т.д.);
- обеспечивать нахождение слов, выделение, просмотр и редактирование таблиц базы данных с удобным графическим интерфейсом;
- обеспечивать резервное копирование всех данных кластера базы данных автоматически и с заданной регулярностью.

Основные операции, которые должны выполнять сервисы работы с данными ЕЦП «ГосТех»:

- классические операции с наборами: объединение, пересечение, различие;
- выбор подмножества записей согласно определенным критериям;
- проецирование – выбор подмножества атрибутов / колонок таблицы;
- сцепление;
- операции для создания, модификации и удаления схем таблиц;
- операции для управления транзакциями и управления пользователями;
- резервное копирование базы данных.

4.2.1 Требования к сервису транзакционной СУБД

Сервис транзакционной СУБД ЕЦП «ГосТех» должен соответствовать следующим основным требованиям:

- программное обеспечение, использованное для реализации сервиса, должно быть включено в Реестр отечественного ПО и/или иметь сертификат ФСТЭК России;
- работать на сертифицированной ОС;
- поддерживать протокол подключения PostgreSQL или JDBC;
- обеспечивать следующие лимиты на аренду:
 - отсутствие ограничений на размер базы данных;

- отсутствие ограничений на максимальное количество записей;
- отсутствие ограничений на количество индексов;
- максимальный размер таблицы – не менее 32 ТБ;
- максимальный размер строки – не менее 1,6 ТБ;
- максимальный размер значения в поле – не менее 1 ГБ;
- количество столбцов таблицы – не менее 1600;
- количество подключений – не менее 2000.
- обеспечивать производительность для одной аренды:
 - не менее 10000 tpsB (pgbench) при SF=30000 и clients=1000;
 - не более 1000 с на TPC-H Q1 при SF=3000.
- поддерживать ACID на уровне аренды;
- иметь уровень изолированности по умолчанию – чтение фиксированных данных;
 - поддерживать уровень упорядочиваемости;
 - иметь возможность установки уровня изолированности на уровне отдельной транзакции;
 - иметь поддержку секционирования для больших таблиц;
 - иметь встроенную поддержку работы с массивами на уровне SQL;
 - иметь поддержку хранимых процедур;
 - иметь поддержку табличных триггеров базы данных и триггеров событий;
 - поддерживать несколько процедурных языков Perl, Python;
 - иметь программные интерфейсы для работы с C/C++, Java, .Net, Perl, Python, Tcl, ODBC;
 - иметь встроенные средства аутентификации пользователей, поддерживающих SSL, LDAP, GSSAPI, SSPI, RADIUS, PAM;
 - обеспечивать возможность заказа аренды с асинхронной репликации в удалённый ЦОД (катастрофоустойчивость).

4.2.2 Требования к сервису ширококолоночной СУБД

Сервис ширококолоночной СУБД ЕЦП «ГосТех» должен соответствовать следующим основным требованиям:

- программное обеспечение, использованное для реализации сервиса, должно быть включено в Реестр отечественного ПО и/или иметь сертификат ФСТЭК России;
- поддерживать протокол подключения Hbase-Client или JDBC;
- поддерживать файловую систему HDFS;

- поддерживать распределенную блочную обработку больших объемов данных (например Spark);
- поддерживать от 1 000 000 столбцов и от 1 000 000 000 строк в таблицах;
- поддерживать мультикластерный режим;
- поддерживать механизм регионирования – автоматической горизонтальной группировки табличных строк;
- поддерживать использование средств загрузки, хранения и обработки объемов данных: MapReduce, Hive, Tez;
- работать в среде исполнения сертифицированной и/или включенной в Реестр отечественного ПО;
- поддерживать горизонтальную масштабируемость;
- поддерживать декомиссию числа хостов без остановки и прерывания рабочей нагрузки;
- обеспечивать автоматическое восстановление при потере любого из узлов.

4.2.3 Требования к сервису Key-value СУБД (in-memory)

Сервис Key-value СУБД (in-memory) ЕЦП «ГосТех» должен соответствовать следующим основным требованиям:

- программное обеспечение, использованное для реализации сервиса, должно быть включено в Реестр отечественного ПО и/или иметь сертификат ФСТЭК России;
- работать на сертифицированной ОС;
- поддерживать протокол подключения JDBC или REST API;
- обеспечивать не менее 20000 запросов в секунду;
- поддерживать базовый SQL (в рамках одного экземпляра);
- обеспечивать ведение синхронного журнала предзаписи;
- обеспечивать возможность организации синхронной реплики для экземпляра;
- обеспечивать возможность заказа аренды с асинхронной репликации в удаленный ЦОД (катастрофоустойчивость);
- обладать свойствами: персистентности, транзакционности ACID;
- поддерживать ANSI-99 SQL;
- использовать модель ACL для разграничения доступа;
- позволять хранение всех данных в оперативной памяти, с дисковыми снимками данных и логом транзакций;
- поддерживать индексы: TREE;

- поддерживать различные форматы хранения и протоколы передачи данных;
- поддерживать кооперативную многозадачность для одновременного выполнения кода;
- обеспечивать возможность интеграции с NoSQL СУБД, Hadoop, Kafka;
- поддерживать горизонтальную масштабируемость без остановки работы сервиса;
- иметь встроенные механизмы отказоустойчивости данных;
- иметь встроенный механизм репликации (как минимум, асинхронного типа);
- поддерживать алгоритмы шифрования при передаче данных ГОСТ 34.12-2018;
- иметь средства захвата изменений Change Data Capture (CDC);
- иметь скриптовые средства выполнения логики над данными внутри СУБД;
- иметь средства администрирования с пользовательскими интерфейсами.

4.2.4 Требования к сервису СУБД полнотекстового индекса

Сервис СУБД полнотекстового индекса ЕЦП «ГосТех» должен соответствовать следующим основным требованиям:

- программное обеспечение, использованное для реализации сервиса, должно быть включено в Реестр отечественного ПО и/или иметь сертификат ФСТЭК России;
- работать на сертифицированной ОС;
- поддерживать протокол подключения RESTful API;
- обеспечивать отсутствие ограничений на размер индекса (лимиты на аренду);
- обеспечивать горизонтальная масштабируемость;
- обеспечивать многопоточность;
- поддерживать распределенных индексов;
- обеспечивать индексацию в режиме «реального» времени;
- обеспечивать добавление полей в индекс без полного перестроения;
- поддерживать различные языки разработки: Java, JavaScript (Node.js), Go, .NET (C#), PHP, Perl, Python, Ruby;
- поддерживать REST API;
- иметь визуальный веб-интерфейс управления;

- осуществлять поиск по критериям (точное совпадение по одному значению или по списку значений);
- осуществлять поиск по диапазону (числа, даты);
- осуществлять полнотекстовый поиск (морфология, шаблоны, wildcard);
- осуществлять булевый поиск (объединение критериев поиска по И/ИЛИ);
- обеспечивать гибкость поисковых фильтров, включая нечеткий поиск и мультиарендность;
- иметь встроенных анализаторов текста (автоматическая токенизация, лемматизация, стемминг и пр.);
- поддерживать функции автодополнения;
- поддерживать библиотеку Lucene.

4.2.5 Требования к сервису СУБД аналитического хранилища данных

Сервис СУБД аналитического хранилища данных ЕЦП «ГосТех» должен соответствовать следующим основным требованиям:

- программное обеспечение, использованное для реализации сервиса, должно быть включено в Реестр отечественного ПО и/или иметь сертификат ФСТЭК России;
- поддерживать протокол подключения PostgreSQL или JDBC;
- иметь следующие лимиты на аренду:
 - отсутствие ограничений на размер базы данных;
 - отсутствие ограничений на максимальное количество записей;
 - отсутствие ограничений на количество индексов;
 - отсутствие ограничений на максимальный размер таблицы;
 - максимальный размер строки – не менее 1,6 ТБ;
 - максимальный размер значения в поле – не менее 1 ГБ;
 - количество столбцов таблицы – не менее 1600.
- обеспечивать производительность для одной аренды:
 - не менее 50000 qphH (TPC-H) для SF = 10 ТБ;
 - скорость загрузки не менее 1 ТБ/ч;
 - пропускную способность на сканировании (TPC-H Q1, 100 ТБ) не менее 20 ГБ/с;
- обеспечивать автоматическое подключение вторичного ведущего узла при сбое первичного не позднее, чем через 120 с;
- обеспечивать автоматическую активацию резервного сегмента при сбое активного не позднее, чем через 60 с;

- обеспечивать возможность горизонтального масштабирования путем добавления серверов хранения;
- иметь встроенные механизмы отказоустойчивости данных;
- обеспечивать возможность организации хранения данных таблиц как по записям, так и по столбцам;
- иметь механизмы резервного копирования и восстановления;
- иметь единую точку входа для SQL-запросов к компонентам сред, обеспечивающих хранение данных;
- иметь инструменты для формирования федерации данных без увеличения времени доступа к данным, при этом должна обеспечиваться возможность подключения в федерацию любых источников данных, поддерживающих ODBC/JDBC-стандарты взаимодействия;
- обеспечивать возможность распространения параметров секции «where» SQL-запроса в любую систему-поставщик федерации данных для ограничения размера перемещаемой выборки данных;
- обеспечивать шардирование/сегментирование данных с обеспечением локальности исполнения запросов;
- иметь возможность настройки прав доступа к очередям сообщений, строкам и столбцам таблиц баз данных, отдельным файлам распределённой иерархической файловой системы. В том числе с использованием доменной авторизации по протоколу LDAP;
- поддерживать стандарт ANSI SQL версии 2008 или выше;
- иметь эффективные алгоритмы сжатия данных (например, Zstandard);
- иметь встроенную систему развертывания и управления.

4.2.6 Требования к сервису СУБД аналитических витрин хранилища данных

Сервис СУБД аналитических витрин хранилища данных ЕЦП «ГосТех» должен соответствовать следующим основным требованиям:

- программное обеспечение, использованное для реализации сервиса, должно быть включено в Реестр отечественного ПО и/или иметь сертификат ФСТЭК России;
- поддерживать протокол подключения Clickhouse-client или JDBC;
- обеспечивать следующие лимиты на аренду:
 - отсутствие ограничений на размер базы данных;
 - отсутствие ограничений на максимальное количество записей;
 - отсутствие ограничений на количество индексов;

- отсутствие ограничений на максимальный размер таблицы;
- максимальный размера строки – не менее 1,6 ТБ;
- максимальный размер значения в поле – не менее 1 ГБ;
- количество столбцов таблицы – не менее 1600.
- обеспечивать производительность для одной аренды:
 - не более 200 с TPC-H Q1 при SF = 10 ТБ и одиночном запуске;
 - не более 400 с TPC-H Q1 при SF = 10 ТБ и одновременном запуске 20 запросов;
- скорость загрузки не менее 1 ТБ/ч;
- пропускную способность на сканировании (TPC-H Q1, 100 ТБ) не менее 20 ГБ/с.
- поддерживать базовый SQL Select;
- обеспечивать возможность пакетного обновления данных (>1000 строк);
- обеспечивать выполнение простых запросов с задержкой не более 50 мс;
- обеспечивать функционал работы с запросами объёмом в миллиарды строк по малому количеству столбцов;
- иметь возможность обработки запросов не по столбцам, а по векторам (частям столбцов);
- иметь эффективные алгоритмы сжатия данных (например, Zstandard);
- поддерживать конструкции языка SQL: group by, order by, подзапросы в секциях FROM, IN, JOIN, а также скалярные подзапросы;
- поддерживать индексы;
- обеспечивать возможность быстрого индексного доступа за счёт хранения данных в отсортированном виде (merge tree);
- обеспечивать возможность выполнения запросов над частью выборки с выводом приближенного результата, возможность выполнения агрегации по ограниченному набору случайных ключей;
- обеспечивать репликацию данных и возможность выполнения распределённых запросов;
- поддерживать шардирование/сегментирование данных с обеспечением локальности исполнения запросов;
- обеспечивать возможность горизонтальной и вертикальной масштабируемости;
- иметь встроенные механизмы отказоустойчивости данных;
- обеспечивать возможность реализации отказоустойчивости за счёт использования асинхронной репликации;
- иметь встроенную систему развёртывания и управления.

4.2.7 Требования к сервису СУБД хранения неструктурированных данных

Сервис СУБД хранения неструктурированных данных ЕЦП «ГосТех» должен соответствовать следующим основным требованиям:

- программное обеспечение, использованное для реализации сервиса, должно быть включено в Реестр отечественного ПО и/или иметь сертификат ФСТЭК России;
- поддерживать протокол подключения JDBC;
- обеспечивать возможность поддержки работы в кластере из нескольких серверов;
- обеспечивать возможность сегментирования данных;
- работать в мультикластерном режиме с разделением ролей на подкластеры: управление узлами (NameNode), хранение данных (DataNode), подкластеры обработки данных (YARN NodeManager);
- поддерживать фреймворки обработки больших данных: Tez, MapReduce;
- поддерживать фреймворк микропакетной обработки больших данных Spark;
- поддерживать службы обеспечивающие взаимодействие через REST-интерфейс;
- поддерживать декомиссию хостов без остановки и прерывания рабочей нагрузки;
- иметь поддержку автоматического распределения данных между серверами кластера и возможностью балансировки нагрузки на серверах кластера;
- обеспечивать возможность хранения данных как в реляционном виде, так и в виде файлов в распределённой иерархической сетевой файловой системе;
- обеспечивать высокую доступность для следующих сервисов: HDFS, MapReduce, YARN;
- иметь версию нереляционную распределённую базу данных, работающую поверх HDFS;
- иметь СУБД для выполнения SQL-подобных запросов и анализа данных, хранящихся на HDFS;
- иметь встроенную систему развертывания и управления.

4.2.8 Требования к сервису объектного хранилища

Сервис объектного хранилища ЕЦП «ГосТех» должен соответствовать следующим основным требованиям:

- программное обеспечение, использованное для реализации сервиса, должно быть включено в Реестр отечественного ПО и/или иметь сертификат ФСТЭК России;
- работать на сертифицированной ОС;
- обеспечивать сохранность данных, хранящихся в объектном хранилище при выходе из строя, как минимум одного хоста;
- иметь возможность одновременного использования дисков SSD, SAS HDD и SATA HDD разной емкости для реализации распределенного дискового хранилища;
- иметь возможность предоставлять доступ к хранилищу по протоколам iSCSI, S3;
- поддерживать масштабирование не менее чем до 8 ПБ и 2 миллиардов объектов;
- иметь возможность хранения данных с использованием технологии Erasure coding;
- иметь возможность использования SSD под задачи кэширования операций записи/чтения для HDD;
- обеспечивать реализацию объектного хранилища с доступом по протоколу, совместимому с Amazon S3;
- поддерживать протоколы S3, HTTP/REST;
- поддерживать версию объектов;
- поддерживать возможность разграничения прав доступа администраторов и групп администраторов к объектам системы;
- поддерживать возможность создания пользовательского набора прав для разграничения доступа;
- поддерживать возможность интеграции с внешним LDAP-каталогом учетных записей администраторов;
- обеспечивать ведение журналов системы с фиксацией действий администраторов;
- поддерживать геораспределенную защиту данных с использованием асинхронной репликации;
- иметь CLI интерфейс управления объектным хранилищем.

4.3 Основные требования к интеграционным сервисам

4.3.1 Требования к сервисам интеграционного взаимодействия

Сервис для создания и управления API, а также настройки интеграции приложений и сервисов – сервисы интеграционного взаимодействия ЕЦП «ГосТех» должны соответствовать следующим основным требованиям:

- должны поддерживать аутентификацию и авторизацию вызовов;
- должны поддерживать балансировку запросов между несколькими экземплярами или версиями приложения на основе различных стратегий (равномерно по всем узлам (round-robin), с использованием весов, в привязке к конкретному адресу (affinity))
- должны поддерживать маршрутизацию запросов на основе различных стратегий (доступность приложения, поля заголовка, принадлежность определенной зоне);
- должны поддерживать динамическое изменение интеграционных политик (правила маршрутизации, политики доступа, стратегия балансировки) в режиме runtime (без остановки приложения);
- должны поддерживать применение интеграционных политик на различных уровнях транспортных протоколов (tcp, http);
- должны поддерживать развертывание в виде отдельных элементов (в том числе режим sidecar) без влияния на прикладной код;
- должны поддерживать квотирование максимального количества одновременных подключений к приложению с помощью конфигурационных файлов Kubernetes;
- должны поддерживать формирование метрик трассировки запросов и мониторинга компонент;
- должны поддерживать управление жизненным циклом API, включающим: создание, публикацию, перемещение и удаление API;
- наличие возможности управления API с использованием спецификации в форматах YAML и JSON с описанием по стандарту OpenAPI 3.0;
- должны поддерживать функциональность управления версиями API;
- должны поддерживать протоколы HTTP, HTTPS, WebSocket, POP, IMAP, SMTP;
- должны поддерживать форматы JSON, XML, SOAP, EDIFACT, FHIR, ISO 8583, FIX;
- должны поддерживать интеграцию с объектными хранилищами по протоколу S3.

4.3.2 Требования к сервису управления очередями сообщений

Сервис управления очередями сообщений ЕЦП «ГосТех» должен соответствовать следующим основным требованиям:

- должен обеспечивать надежную (исключающую потерю данных как при потере узла, так и при аварийной остановке всего кластера) доставку сообщений приложений, в том числе: о возможность горизонтального масштабирования с увеличением пропускной способности за счет добавления узлов;

- наличие инструментария администрирования и управления;

- наличие возможности создания новых потоков событий со следующими параметрами:

- срок хранения событий в транспортном слое и/или максимальный размер потока событий;

- число копий события для обеспечения отказоустойчивости публикации событий;

- наименование потока событий согласно правилам наименования;

- максимальный размер события для данного потока;

- допустимый параллелизм обработки события;

- наличие возможности назначения прав на публикацию и подписку по каждому потоку событий на основании модели авторизации, базирующейся на полном наименовании сертификата, используемого при подключении;

- поддержка соединения с узлами передачи событий на основе протокола TLS;

- наличие возможности публикации события (plaintext, json и xml-нотации) с сохранением его в транспортном слое;

- наличие возможности потребления события из потока по следующим правилам:

- потребители могут объединяться в группы для обеспечения масштабирования обработки;

- все активные экземпляры потребителей, принадлежащих одной группе, получают суммарно весь актуальный поток событий;

- каждая активная группа потребителей получает весь актуальный поток событий;

- поддержка удаления события по достижению заданного срока хранения/максимального размера потока.

4.4 Основные требования к сервисам управления

4.4.1 Требования к сервису управления микросервисами

Сервис управления микросервисами ЕЦП «ГосТех» должен соответствовать следующим основным требованиям:

- обеспечивать автоматизацию и управление жизненным циклом контейнеров и сервисов. В жизненный цикл контейнера должны входить: планирование ресурсов, управление масштабируемостью, правила балансировки нагрузки и контроль доступности, а также организация виртуальных сетей;
- иметь инструменты для создания, развертывания, запуска и управления приложениями в контейнерной среде;
- обеспечивать полную совместимость с нативными версиями Kubernetes и Docker;
- поддерживать процессы автоматического развертывания Docker контейнеров с собранными внутри приложениями (как платформенными, так и прикладными);
- иметь механизмы автоматического масштабирования кластера и приложений путём мониторинга утилизации ресурсов приложениями и автоматического запуска дополнительных экземпляров приложений в случае превышения пороговых значений;
- иметь инструменты управления кластером, развертываниями, подами (pods) и другими ресурсами через графический интерфейс, командную строку и REST API;
- поддерживать декларативное управление кластером совместимое с Terraform;
- иметь встроенные средства планирования ресурсов кластера и балансировки нагрузки;
- обеспечивать возможность резервного копирования данных из групп узлов кластеров и хранения их в объектном хранилище;
- иметь механизмы ролевого доступа к ресурсам кластера.

4.4.2 Требования к сервису управления процессами

Сервис управления процессами ЕЦП «ГосТех» должен соответствовать следующим основным требованиям:

- обеспечивать возможность создания бизнес-процессов в нотации BPMN2;
- обеспечивать автоматическое исполнение бизнес-процессов;
- иметь инструменты контроля исполнения процессов;

- обеспечивать инструменты контроля инцидентов по процессам;
- иметь API для управления бизнес-процессами;
- иметь функциональность управления задачами пользователей;
- иметь механизмы контроля SLA задач;
- иметь функциональность отчётности по задачам;
- обеспечивать визуализацию статистики работы пользователей на портале задач.

4.5 Основные требования к служебным технологическим сервисам

4.5.1 Требования к сервисам IAM

Сервисы IAM (сервисы управления идентификацией и доступом к информационным ресурсам) ЕЦП «ГосТех» должны соответствовать следующим основным требованиям:

- обеспечивать взаимодействие с другими сервисами и их компонентами по одному из протоколов: OpenID Connect 1.0, SAML 2.0, Kerberos, LDAP;
- обеспечивать загрузку в IAM ролевой модели сервиса через интерфейс администрирования, либо при разворачивании или запуске сервиса с привилегированным доступом по одному из доступных протоколов;
- обеспечивать идентификацию и аутентификацию Конечных пользователей сервисов через сервисы IAM с использованием учетных записей единой системы идентификации и аутентификации (ЕСИА);
- наличие инструментов управления пользователями и группами;
- наличие инструментов управления доступом к ресурсам и сервисам;
- наличие инструментов управления ключами авторизации;
- иметь поддержку федерации удостоверений: обеспечивать настройку Single Sign-On аутентификации с помощью внешнего доверенного поставщика удостоверений, либо пользовательского брокера удостоверений;
- централизованное управление политикой безопасности, контроль списка доступа (ACL).

4.5.2 Требования к сервису журналирования

Сервис журналирования ЕЦП «ГосТех» должен соответствовать следующим основным требованиям:

- обеспечивать управление сервисом через web-консоль, CLI и API;
- обеспечивать централизованный сбор и хранение журналов сервисов и их компонент;

- для интеграции с сервисами расширения базовых сервисов ЕЦП «ГосТех», определенных в Методических рекомендациях по включению сервисов в ЕЦП «ГосТех» (далее – сервисы расширения) иметь возможность принимать данные в формате плоского JSON с использованием REST и gRPC API, содержащего следующие поля:

Наименование	Тип переменной	Описание
Datetime	long	Дата и время события в формате system time milli seconds since epoch
className	String	Имя класса, породившего событие
message	String	Текст события
traceId	String	Идентификатор, который позволяет отследить события в разных сервисах в рамках одного входящего запроса
logLevel	String	Уровень журналирования
serviceName	String	Имя сервиса, однозначно определяющее его при поиске событий
serviceVersion	String	Версия сервиса
instanceID	String	Уникальный идентификатор экземпляра Сервиса

- инструменты Сервиса журналирования и собранные им данные должны позволять однозначно указать элемент или группу элементов, в которой произошли;

- обеспечивать агрегацию данных о работе различных ресурсов в лог-группу;

- обеспечивать управление лог-группами;

- обеспечивать сбор, обработку и хранение логов в течение установленного срока;

- обеспечивать изолированное хранение логов для каждой лог-группы;

- предоставлять возможность фильтрации и поиска записей с помощью запросов;

- обеспечивать ролевой доступ на чтение и запись логов.

4.5.3 Требования к сервису аудита

Сервис аудита ЕЦП «ГосТех» должен соответствовать следующим основным требованиям:

- обеспечивать централизованный сбор и хранение событий безопасности, связанных с действиями пользователей в системе и в сервисах;
- для интеграции с сервисами расширения обеспечивать приём событий аудита через REST и gRPC API со следующими значениями в теле запроса:

Наименование	Тип переменной	Описание
tags	string[]	Сквозные идентификаторы и метки, позволяющие группировать события
Datetime	integer	Unix time. Время возникновения события в миллисекундах, прошедших с полуночи (00:00:00 UTC) 1 января 1970 года. (Fri Apr 03 2020 10:28:37 соответствует 1585909717000)
serviceName	string	Идентификатор Сервиса
seviceVersion	string	Версия Сервиса
name	string	Наименование события аудита
params	object[]	Список параметров события аудита в формате: Name (string): наименование параметра события аудита Value (string): значение параметра события
sessionID	string	Идентификатор сессии (если есть)
userLogin	string	Логин пользователя
userName	string	Имя пользователя
userNode	string	Узел (IP/FQDN), с которого пользователь выполняет действия

- собранные события безопасности должны быть доступны для экспорта во внешние SIEM-системы.

Перечень регистрируемых событий безопасности прорабатывается на этапе проектирования информационной безопасности решения и проработки модели угроз.

4.5.4 Требования к сервису мониторинга

Сервис мониторинга ЕЦП «ГосТех» должен соответствовать следующим основным требованиям:

- обеспечивать ролевой доступ к сервису и данным мониторинга;
- обеспечивать автоматический сбор и долговременное хранение метрик состояния ресурсов в ЕЦП «ГосТех»;
- отображать метрики на сервисных панелях (dashboards);
- поддерживать загрузку собственных метрик, с использованием API;
- поддерживать выгрузку метрик ресурсов и пользовательских метрик с помощью API;
- обеспечивать создание собственных панелей и графиков;
- поддерживать метки для идентификации и описания характеристик временных рядов;
- поддерживать настройки уведомлений («тревожных сигналов», alerts) об изменении состояния ресурса ЕЦП «ГосТех»;
- поддерживать каналы уведомлений: электронной почты, SMS;
- поддерживать агрегации значений всех метрик в соответствии с *политикой прореживания*;
- автоматическое удаление устаревших метрик (TTL) в соответствии с заданными правилами;
- для интеграции с сервисами расширения поддерживать два режима загрузки метрик: режимы pull и push;
- в режиме pull Сервис мониторинга должен осуществлять сбор метрик с объекта контроля в формате Prometheus с заданной периодичностью;
- в режиме push Сервис мониторинга должен предоставлять REST и gRPC API и принимать через него информацию по метрикам объектов со следующими полями в теле запроса:

Заголовок			
Название заголовка	Тип	Обязательно	Описание

serviceName	string	Да	Имя Сервиса	
serviceVersion	string	Да	Версия Сервиса	
instanceID	string	Да	Уникальный идентификатор экземпляра Сервиса	
Тело				
Название переменной	Тип	Обязательно	Описание	
metrics	Array (MetricData[])	Да	Метрики	
Элементы массива metrics				
	Название переменной	Тип	Обязательность	Описание
	name	string	Да	Имя метрики
	value	string	Да	Значение метрики в указанной точке
	timestamp	string	Да	Временная метка
	labels.xxx	string	Нет	Любые пользовательские метки
Ответ				
string				

Обязательным набором метрик является:

- метрики использования системных ресурсов (CPU, RAM, Memory);
- время исполнения входящих запросов;
- количество успешных/неуспешных выполнений входящих запросов;
- время исполнения исходящих запросов или обращений к СПО;
- количество успешных/неуспешных выполнений исходящих запросов или обращений к СПО.

4.6 Основные требования к сервисам интеграции с инфраструктурой электронного правительства

4.6.1 Требования к сервису «Типовое тиражируемое программное обеспечение витрин данных» («Витрина НСУД»)

Сервис «Типовое тиражируемое программное обеспечение витрин данных» («Витрина НСУД») ЕЦП «ГосТех» должен соответствовать следующим основным требованиям:

- обеспечивать загрузку логической модели данных из ПОДД СМЭВ;
- обеспечивать загрузку данных из внешних систем посредством одного или нескольких интеграционных сервисов (см. подраздел 4.3);
- обеспечивать загрузку данных из БД, размещенных на ЕЦП «ГосТех», с использованием сервисов работы с данными (см. подраздел 4.2);
- обеспечивать загрузку данных из структурированного файла CSV, XLS, WebForm;
- поддерживать обработку регламентированных запросов, написанных с использованием расширенного синтаксиса языка SQL;
- поддерживать обработку запросов с использованием стандарта JDBC;
- поддерживать выполнение распределённых регламентированных запросов;
- поддерживать протокол коммуникации агента ПОДД;
- предоставлять возможность проверки полномочий потребителя данных перед выполнением регламентированного запроса;
- обеспечивать публикацию конечных точек API для обработки запросов с использованием спецификации OpenAPI версии 3;
- поддерживать горизонтальную масштабируемость;
- обеспечивать восстановление данных в непротиворечивое состояние после сбоя;
- поддерживать логирование событий в шлюзе СМЭВ с использованием служебных технологических сервисов: журналирование, мониторинг, аудит (см. подраздел 4.5).

4.6.2 Требования к сервису «Шлюз Единой системы идентификации и аутентификации»

Сервис «Шлюз Единой системы идентификации и аутентификации» (далее – шлюз ЕСИА) ЕЦП «ГосТех» должен соответствовать следующим основным требованиям:

- поддерживать возможность аутентификации с применением одного из протоколов: OpenID Connect 1.0, SAML 2.0;
- поддерживать обмен данными с использованием технологии REST API;
- обеспечивать обмен всеми необходимыми данными для идентификации и аутентификации пользователей через ЕСИА;
- поддерживать возможность работы с несколькими мнемониками и различными скоупами;
- поддерживать различные способы аутентификации, в том числе двухфакторную;
- поддерживать уровни достоверности идентификации пользователей;
- поддерживать горизонтальную масштабируемость;
- поддерживать логирование событий в шлюзе ЕСИА с использованием служебных технологических сервисов: журналирование, мониторинг, аудит (см. подраздел 4.5).

4.6.3 Требования к сервису «Платформа государственных сервисов»

Сервис «Платформа государственных сервисов» (далее – ПГС) ЕЦП «ГосТех» должен соответствовать следующим основным требованиям:

- обеспечивать возможность конструирования и исполнения процессов предоставления услуг (функций) пользователями с использованием стандартных элементов процесса;
- поддерживать возможность конфигурирования интерактивных экранных форм заявлений;
- обеспечивать автоматическое направление межведомственных запросов на получение сведений посредством СМЭВ в процессе предоставления;
- обеспечивать проверку соответствия критериями принятия решения;
- обеспечивать формирование проектов решений;
- обеспечивать взаимодействие с ЕПГУ в процессе предоставления;
- поддерживать реестровую модель;
- поддерживать горизонтальную масштабируемость;
- обеспечивать восстановление данных в непротиворечивое состояние после сбоев;
- поддерживать логирование событий с использованием служебных технологических сервисов: журналирование, мониторинг, аудит (см. подраздел 4.5).

5. Требования к поставщику

Поставщик должен соответствовать следующим требованиям:

1) наличие общей и специальной гражданской правоспособности в полном объеме для заключения и исполнения государственного контракта (договора) по использованию Сервиса;

2) наличие лицензий на осуществление отдельных видов деятельности, в случаях если деятельность по созданию Сервиса подлежит лицензированию в соответствии с требованиями законодательства Российской Федерации;

3) непроведение ликвидации юридического лица и отсутствие решения арбитражного суда о признании юридического лица несостоятельным (банкротом) и об открытии конкурсного производства;

4) неприостановление деятельности юридического лица в порядке, установленном Кодексом Российской Федерации об административных правонарушениях;

5) отсутствие у юридического лица недоимки по налогам, сборам, задолженности по иным обязательным платежам в бюджеты бюджетной системы Российской Федерации (за исключением сумм, на которые предоставлены отсрочка, рассрочка, инвестиционный налоговый кредит в соответствии с законодательством Российской Федерации о налогах и сборах, которые реструктурированы в соответствии с законодательством Российской Федерации, по которым имеется вступившее в законную силу решение суда о признании обязанности заявителя по уплате этих сумм исполненной или которые признаны безнадежными к взысканию в соответствии с законодательством Российской Федерации о налогах и сборах) за прошедший календарный год, размер которых превышает двадцать пять процентов балансовой стоимости активов юридического лица, по данным бухгалтерской отчетности за последний отчетный период. Юридическое лицо считается соответствующим установленному требованию в случае, если им в установленном порядке подано заявление об обжаловании указанных недоимки, задолженности и решение по такому заявлению на дату рассмотрения заявки на включение Сервиса в ЕЦП «ГосТех» не принято;

6) отсутствие у руководителя юридического лица, членов коллегиального исполнительного органа, лица, исполняющего функции единоличного исполнительного органа, или главного бухгалтера юридического лица судимости за преступления в сфере экономики и (или) преступления, предусмотренные статьями 289, 290, 291, 291.1 Уголовного кодекса Российской Федерации (за исключением лиц, у которых такая судимость погашена или

снята), а также неприменение в отношении указанных физических лиц наказания в виде лишения права занимать определенные должности или заниматься определенной деятельностью, которые связаны с поставкой товара, выполнением работы, оказанием услуги, являющихся объектом осуществляемой закупки, и административного наказания в виде дисквалификации;

7) отсутствие привлечения юридического лица к административной ответственности за совершение административного правонарушения, предусмотренного статьей 19.28 Кодекса Российской Федерации об административных правонарушениях, в течение двух лет до момента подачи заявки на включение в ЕЦП «ГосТех»;

8) обладание Поставщиком интеллектуальными правами на результаты интеллектуальной деятельности (Сервис и его компоненты);

9) юридическое лицо не является офшорной компанией, не имеет в составе участников (членов) корпоративного юридического лица или в составе учредителей унитарного юридического лица офшорной компании, а также не имеет офшорных компаний в числе лиц, владеющих напрямую или косвенно (через юридическое лицо или через несколько юридических лиц) более чем десятью процентами голосующих акций хозяйственного общества либо долей, превышающей десять процентов в уставном (складочном) капитале хозяйственного товарищества или общества;

10) отсутствие информации о юридическом лице в реестрах недобросовестных поставщиков (подрядчиков, исполнителей), предусмотренных Федеральным законом от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» и Федеральным законом от 18.07.2011 № 223-ФЗ «О закупках товаров, работ, услуг отдельными видами юридических лиц».

Правительством Российской Федерации могут быть утверждены дополнительные требования к Поставщикам, в том числе к наличию:

- 1) финансовых ресурсов;
- 2) на праве собственности или ином законном основании оборудования и других материальных ресурсов, лицензий на используемое инструментальное ПО и библиотеки;
- 3) опыта работы и деловой репутации;
- 4) необходимого количества специалистов и иных работников определенного уровня квалификации.

6. Требования к юридическому оформлению

Право использования Сервиса передается по лицензионному договору. Пределы прав и способы использования Сервиса, предусмотренные лицензионным договором, должны обеспечивать возможность подключения Конечных пользователей на ЕЦП «ГосТех» на территории Российской Федерации без необходимости приобретения Пользователем ЕЦП «ГосТех» дополнительных пользовательских, серверных, процессных или других лицензий.

Поставщик Сервиса обязан передать права на использование охраняемых результатов интеллектуальной деятельности Пользователю ЕЦП «ГосТех» в объеме, необходимом для использования Сервиса Пользователем ЕЦП «ГосТех» в соответствии с назначением ГИС на ЕЦП «ГосТех». Исключительные права на результаты работ, полученные при использовании Сервиса, подлежат передаче Пользователю ЕЦП «ГосТех».

При использовании в составе Сервиса программ (программных комплексов или компонентов), разработанных третьими лицами, условия, на которых передается право на использование (исполнение) этих программ, не должны накладывать ограничений, препятствующих использованию Сервиса по его прямому назначению. Программы для ЭВМ третьих лиц, как подразумевающие, так и не подразумевающие свободное использование, должны быть обеспечены гарантийным обслуживанием Поставщика.

7. Требования к биллингу

Поставщик должен предоставлять Оператору ЕЦП «ГосТех» данные, позволяющие произвести расчёт стоимости потребления Сервисов по модели pay-as-you-go с точностью до минуты и с детализацией до уровня конкретного ресурса (виртуальной машины, диска, БД, кластера Kubernetes).

Начисления должны выполняются с ежедневной периодичностью по состоянию ресурса на день расчёта.

Должна быть возможность использования различных тарифных планов, основывающиеся на количестве экземпляров используемых сервисов и/или количестве используемых виртуальных ресурсов.

8. Требования к порталу самообслуживания

Поставщик должен предоставить для Пользователя ЕЦП «ГосТех» интерактивный портал самообслуживания, с помощью которого можно

самостоятельно заказывать и управлять Сервисами, включая сервисы расширения. Портал самообслуживания должен быть интегрирован с системой биллинга и должен предоставлять информацию о прогнозе стоимости заказываемых Сервисов, а также позволять формировать отчеты по потреблению сервисов.

9. Требования о подключении к ФГИС «Управление ГосТех»

Для контроля объема и качества оказываемых сервисов облачная платформа должна обеспечивать передачу необходимых данных в ФГИС «Управление ГосТех». Передаваемая информация должна быть представлена в виде метрик. Требования к формату передачи данных, способу передачи, к метрикам должны быть разработаны в рамках Протокола взаимодействия ФГИС «Управление ГосТех». Проект Протокола должен быть предоставлен Минцифры России.

Приложение А
(справочное)
Пример целевых показателей по обработке обращений,
классифицированных как инциденты

Ниже в таблице приведен пример целевых показателей по обработке обращений, классифицированных как инциденты:

Категория обращения	Приоритет	График работы, рабочие часы	Время реакции, рабочие минуты	Время решения, рабочие часы
Инцидент	Критический	24x7, круглосуточно	15	12
	Высокий		15	24
	Средний	9x5, с 9:00 до 18:00	15	45
	Низкий		15	198

Время реакции – это время ответа, которое не является временем выполнения обращения. Не позднее указанного срока Поставщик сервиса обязан представить Оператору ГИС или Конечному пользователю сервиса информацию о ходе исполнения заявки и прогноз времени, необходимого для его выполнения. Эта информация является исходной для согласования реального приоритета и срока выполнения обращения.

Время решения обращения определяется как разность моментов окончания и начала исполнения обращения, за вычетом времени ожидания от автора обращения дополнительной информации, необходимой для исполнения обращения.