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 «СТАНДАРТ ПО УПРАВЛЕНИЮ ДИНАМИЧЕСКОЙ ИНФРАСТРУКТУРОЙ ЕДИНОЙ ЦИФРОВОЙ ПЛАТФОРМЫ «ГОСТЕХ»

2022 г.

Содержание

1. Нормативная база

Постановление Правительства Российской Федерации от 24.07.2021 г. № 1260 «О внесении изменений в некоторые акты Правительства Российской Федерации»;

Постановление Правительства Российской Федерации от 12.10.2020 г. № 1674 «О проведении эксперимента по созданию, переводу и развитию государственных информационных систем и их компонентов на единой цифровой платформе Российской Федерации «ГосТех»;

Постановление Правительства Российской Федерации от 06.07.2015 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» (с изменениями и дополнениями);

Положение о единой цифровой платформе Российской Федерации «ГосТех»;

Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

Федеральный закон от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд»;

Федеральный закон от 18.07.2011 № 223-ФЗ «О закупках товаров, работ, услуг отдельными видами юридических лиц»;

Приказ ФСТЭК России от 18.02.2013 № 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 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

Приказ ФСБ России от 10.07.2014 № 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».

2. Назначение документа

Данный документ описывает обязательные требования, предъявляемые к поставщикам услуг - как Сервисов IaaS, которые планируется включить в ЕЦП «ГосТех». Так же настоящий документ описывает требования для конфигурации инфраструктуры как кода. Это позволит обеспечить автоматизированную базовую подготовку инфраструктуры для обеспечения размещения экземпляров Единой цифровой платформы Российской Федерации «ГосТех» (далее – ЕЦП, ЕЦП «ГосТех», Платформа) и государственных информационных систем. Поддержка динамической конфигурации инфраструктуры, позволит провайдерам, предоставляющим инфраструктуру как сервис, участвовать в размещении государственных информационных систем на мощностях, находящихся под их управлением.

Также в документе указаны требования к процессу предоставления доступа к ресурсам на уровне провайдеров и изоляции контура промышленной эксплуатации системы от других контуров Платформы.

3. Общие положения

В рамках документа рассматривается перечень обязательных требований к поставщикам услуг-как сервисов, а также описание необходимых ресурсов, создаваемых посредством модуля управления динамической инфраструктурой, для конфигурации сетей, виртуальных машины и иных описанных далее объектов у любого провайдера, представляющего инфраструктуру как услугу.

4. Термины, определения и сокращения

В настоящем документе применены термины с соответствующими определениями:

Термин, сокращение	Определение
ВС	Виртуальная сеть
ГИС	Государственная информационная система
ЕСИА	Единая система идентификации и аутентификации
Инфраструктура как услуга	Категория служб облачных вычислений, в которой потребителю службы облачных вычислений предоставляется следующий тип возможностей облака: тип возможностей инфраструктуры

Термин, сокращение	Определение
Категории служб облачных вычислений	Группа служб облачных вычислений, обладающих некоторым набором общих качеств
Compute	Совокупность ресурсов, которые эмулируют поведение реальной вычислительной машины
Контур Платформы	Комплекс программных и технических средств, размещенный в облачной инфраструктуре, являющейся частью Платформы
Модуль управления динамической инфраструктурой	Модуль, входящий в состав облачной платформы и реализующий описание типов вычислительных ресурсов. Модуль исполняется в доверенной среде поставщика облачных услуг.
Модуль управления микросервисами	Инструмент для оркестровки контейнеризированных приложений и сервисов для автоматизации их развёртывания, масштабирования и координации в условиях кластера. Должен являться сертифицированным компонентом облачной платформы.
Облачные вычисления	Модель дистанционной обработки данных за счет использования сетевого доступа к масштабируемому и эластичному пулу физических или виртуальных ресурсов, а также платформенных сервисов с предоставлением самообслуживания и администрированием по требованию
ОГВ	Орган государственной власти
ПО	Программное обеспечение
Потребитель службы облачных вычислений	Лицо, использующее службу облачных вычислений
Провайдер	Лицо, обеспечивающее предоставление вычислительных ресурсов по форме «Инфраструктура как услуга»
Сервис, Продукт	Программное обеспечение, реализующее функциональные возможности, предназначенное

Термин, сокращение	Определение
	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.
Служба облачных вычислений	Одна или более возможностей, предоставляемых через облачные вычисления
Тип возможностей облака	Классификация функциональности, предоставленной службой облачных вычислений
Тип возможностей инфраструктуры	Тип возможностей облака, в котором потребитель службы облачных вычислений может получить и использовать вычислительные ресурсы, ресурсы для хранения данных или сетевые ресурсы
Поставщик	Юридическое лицо или индивидуальный предприниматель, предоставляющие Сервис на ЕЦП «ГосТех»
ФГИС У ГЕОП	Федеральная государственная информационная система управления государственной единой облачной платформой
Federation	Объединение идентификационной информации о пользователях в различных доменах безопасности, каждый из которых поддерживает свою систему управления доступом
ЦОД	Центр обработки данных
API	Прикладной программный интерфейс
IDP	Поставщик удостоверений (IdP) – это служба, которая хранит цифровые удостоверения и управляет ими
Worker Node	Отдельная физическая или виртуальная машина в составе кластера, на которой развёрнуты и выполняются контейнеры приложений

Термин, сокращение	Определение
Pod	Базовая единица для запуска и управления приложениями
Snapshot	Блочная или файловая копия диска (тома/раздела) или Compute, выполняемая без остановки служб, включающая папки, файлы и информацию о состоянии системы на определенный момент времени
ЕЦП «ГосТех»	Единая цифровая платформа Российской Федерации «ГосТех»

5. Определение единиц измерения ресурсов, предоставляемых в рамках Государственных контрактов

В связи с многообразием оборудования, предоставляемого в форме «Инфраструктура как услуга» провайдерами облачных вычислений, стандарт определяет следующие единицы ресурсов, если государственным контрактом не определено иное:

a. **Виртуальный процессор** (vCPU):

ядро CPU с базовой тактовой частотой не менее 2,4 GHz и коэффициентом переподписки, равным 3;

vCPU обслуживаются физическими процессорами на базе архитектуры x86-64 (Intel®64, AMD64, EM64T) или ARM или e2k или аналоги.

b. **Виртуальная память** (vRAM):

Максимальное значение единицы измерения «виртуальная память» для одной виртуальной машины – 128 Гб.

Коэффициент переподписки vRAM равен 0,97 (ноль целых, девяносто семь сотых).

c. **Виртуальный накопитель SSD**:

не менее 2000 IOPS на каждые 1000 Гб пространства.

среднее время доступа к каждому виртуальному накопителю SSD виртуального сервера – не более 5 мс.

d. **Виртуальный жесткий диск SAS**:

не менее 500 IOPS на каждые 1000 Гбайт пространства.

среднее время доступа к каждому виртуальному жесткому диску SAS

виртуального сервера – не более 25 мс.

е. **Виртуальный жесткий диск SATA**:

не менее 100 IOPS на каждые 1000 Гбайт пространства.

среднее время доступа к каждому виртуальному жесткому диску SATA виртуального сервера – не более 30 мс.

6. Требования к процессу предоставления доступа к ресурсам на уровне провайдеров

Управление заявками на создание ресурсов осуществляется через подсистему управления заявками на услуги федеральной государственной системы управления государственной единой облачной платформой (ФГИС У). Реквизиты доступа к выделенным ресурсам будут предоставлены в личном кабинете после формирования заявки.

Дальнейшее взаимодействие органа государственной власти с поставщиком услуг должно осуществляться через подсистему управления технической поддержки ФГИС У путем подачи заявок из личного кабинета.

Типовая схема взаимодействия указана на рисунке 1.

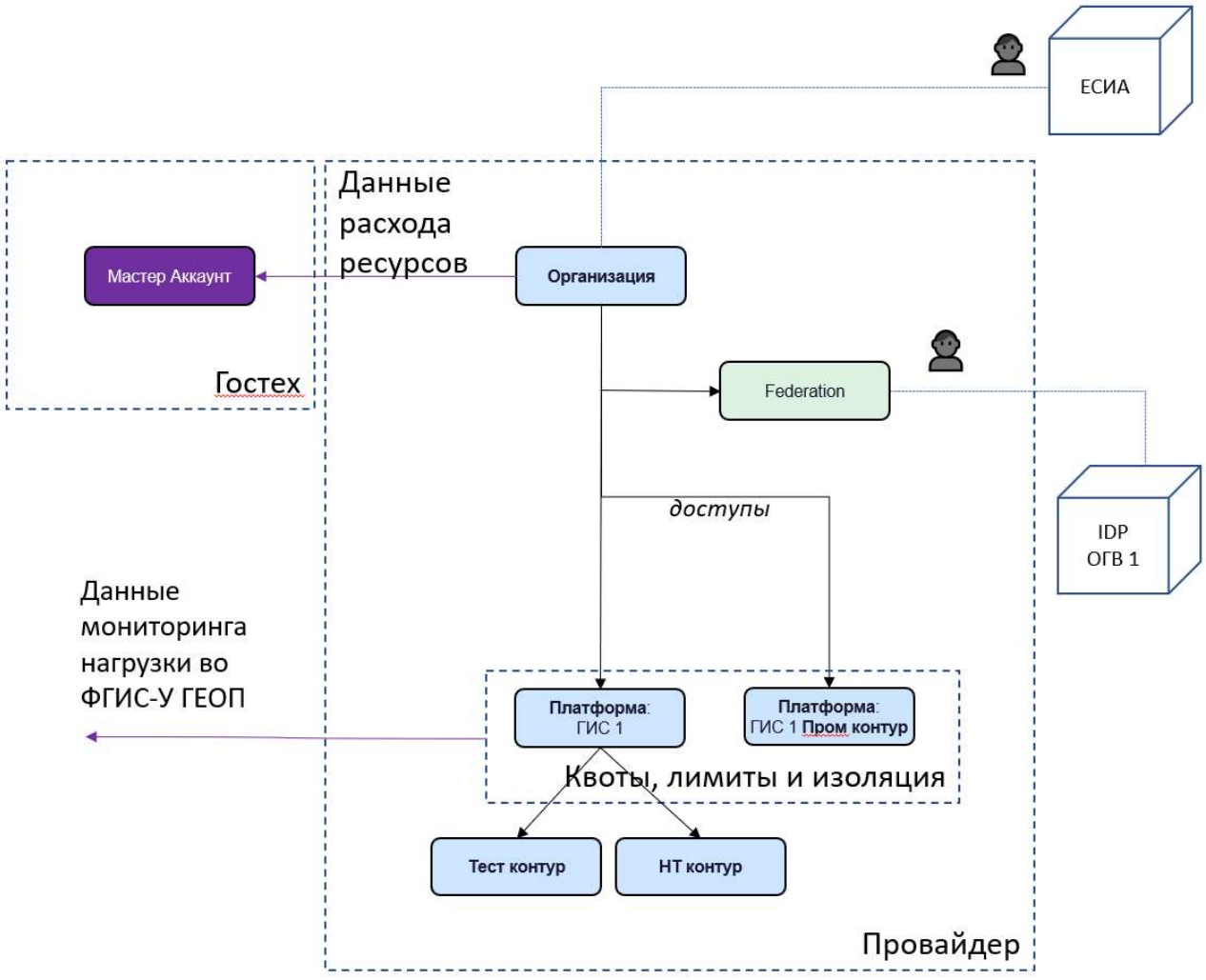

Рисунок 1 – Типовая схема взаимодействия

Управление ресурсами инфраструктуры происходит на уровне контуров Платформы в составе:

- Контур разработки;
- Контур тестирования;
- Контур нагрузочного тестирования;
- Контур приемо-сдаточных испытаний;
- Контур промышленной эксплуатации.

Обязательной является изоляция контура промышленной эксплуатации системы от других контуров. Изоляция остальных контуров должна быть обеспечена при наличии возможности.

7. Требования к модулю проводника, набору ресурсов, создаваемых модулем управления динамической инфраструктуры (функциональная архитектура)

Для соответствия данному документу облачная платформа провайдера должна быть сертифицирована ФСТЭК России, а также провайдер должен иметь опубликованное описание модуля на своем вебсайте, со всей необходимой документацией по его использованию, все каналы связи, выходящие за пределы контролируемой зоны, должны быть защищены средствами криптографической защиты информации, прошедшими установленным порядком процедуру оценки соответствия требованиям ФСБ России, класс которых определен в модели угроз безопасности информации.

Доступ к скачиванию клиентского приложения, ключам доступа должен осуществляться через личный кабинет.

Для управления инфраструктурой на базе облачных вычислений для обеспечения размещения экземпляров Платформы и государственных информационных систем провайдеры должны реализовать возможность создания и управления следующими ресурсами:

1) управление экземплярами Compute;
2) управление виртуальными дисковыми ресурсами;
3) управление образами дисков;
4) управление виртуальными сетями;
5) управление кластерами контейнерных приложений и сервисов ЕЦП ГосТех.

Ниже определены требования к отдельным ресурсам.

7.1. Управление экземплярами Compute

Для управления экземплярами Compute должны быть обеспечены следующие возможности:

1. Создание – должна быть обеспечена возможность указания всех необходимых для создания параметров, а именно: количество выделяемых ей вычислительных ресурсов, загрузочный и дополнительные диски, набор метаданных и иные параметры, необходимые для создания. Так же должна быть обеспечена возможность создания Compute из образов.

2. Удаление – должна быть обеспечена возможность удаления как вместе с подключенными дисками, так и без них. Должна быть обеспечена возможность подключения не удалённых дисков к другим существующим или создаваемым Compute.

3. Запуск – должна быть обеспечена возможность удаленного запуска.

4. Остановка – должна быть обеспечена возможность удаленной остановки машины.

5. Изменение объема вычислительных ресурсов доступных Compute.

6. Создание Snapshot, а также возможность восстановления к состоянию в нем.

7.2. Управление виртуальными дисковыми ресурсами

Для управления виртуальными дисковыми ресурсами должны быть обеспечены следующие возможности для управления виртуальными дисковыми ресурсами:

1. Создание диска – должна быть реализована возможность создания нового диска.
2. Удаление диска – должна быть реализована возможность удаления диска.
3. Подключение диска – должна быть реализована возможность подключения диска.
4. Отключение диска – должна быть реализована возможность отключения диска.
5. Изменение размера диска – должна быть реализована возможность изменения размера диска.

7.3. Управление образами дисков

Для управления образами дисков должны быть обеспечены следующие возможности для управления образами дисков:

1. Создание образа – должна быть реализована возможность создания образа диска с возможностью дальнейшего использования образа при работе с любой VM.
2. Удаление образа – должна быть реализована возможность удаления ранее созданного образа.
3. Обновление образа – должна быть реализована возможность обновления (актуализации) образа.
4. Подключение образа – должна быть реализована возможность подключение образа к экземпляру Compute.

7.4. Управление виртуальными сетями

Для управления виртуальными сетями должны быть обеспечены следующие возможности:

1. Создание внутренней сети – должна быть реализована возможность создания внутренней рабочей сети с настройкой необходимых портов.
2. Создание подсети – должна быть реализована возможность создания подсети с настройкой необходимых портов.
3. Присвоение внешнего статичного IP адреса – должна быть реализована возможность присвоения статичного IP адреса.

7.5. Управление кластерами контейнеризированных приложений

Для управления кластерами модулем управления микросервисами должны быть обеспечены следующие возможности:

1. Создание кластера – должна быть реализована возможность создания управляющих машин кластера.
2. Создание worker node – должна быть реализована возможность создания worker node кластера.
3. Удаление worker node – должна быть реализована возможность удаления worker node кластера.
4. Создание pod – должна быть реализована возможность создания pod.
5. Удаление pod – должна быть реализована возможность удаления pod.
6. Публикация сервиса pod – должна быть реализована возможность публикации pod на порту.
7. Удаление публикации сервиса pod – должна быть реализована возможность удаления публикации pod на порту.