ПРОГРАММНО-ТЕХНИЧЕСКИЙ КОМПЛЕКС, ОБЕСПЕЧИВАЮЩИЙ ДИСТАНЦИОННОЕ ЭЛЕКТРОННОЕ ГОЛОСОВАНИЕ ИЗБИРАТЕЛЕЙ (УЧАСТНИКОВ РЕФЕРЕНДУМА) ВНЕ ЗАВИСИМОСТИ ОТ МЕСТА ИХ НАХОЖДЕНИЯ

Техническое описание реализации ПТК ДЭГ к выборам, голосование на которых состоится 17, 18 и 19 сентября 2021 г.

2021

Содержание

1 Основные технические решения

1.1 Решения по комплексу технических средств, его размещению на объекте

1.1.1 Размещение ПТК ДЭГ

ПТК ДЭГ располагается на четырех площадках:

- два ЦОД для размещения компонентов, включая высоконагруженные: «Портал ДЭГ», «Распределенное хранение данных и учёт голосов» и «Центр наблюдения за голосованием», (далее ЦОД-1 и ЦОД-2);
- ЦОД для размещения компонентов «Распределенное хранение данных и учёт голосов», «Список избирателей, (далее ЦОД-3);
- техническая площадка, определенная ЦИК России (далее ЦОД-4).

Инфраструктура каждого ЦОД зарезервирована по электропитанию и охлаждению.
В целях обеспечения бесперебойной обработки запросов пользователей обеспечен режим функционирования площадок ЦОД-1 и ЦОД-2 в режиме Active/Active.

ПТК ДЭГ защищён (способен функционировать) при следующих типах сбоев:
− однократный сбой элемента КТС в пределах площадки (ЦОД);
− сбой площадки (ЦОД) целиком.

Компонент каждой подсистемы соответствует уровню резервирования не ниже N+1.

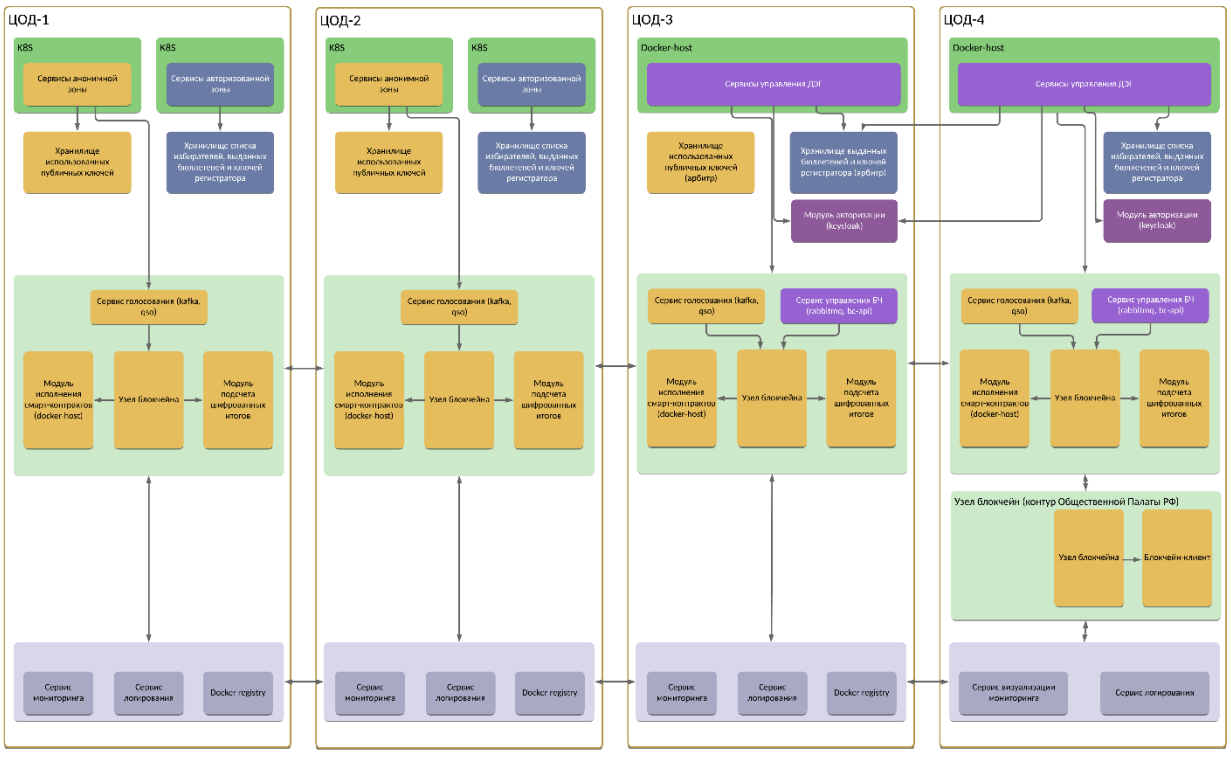

Рисунок 1 – Структурная схема распределения оборудования по ЦОДам

1.1.2 Вычислительная подсистема

Вычислительная подсистема предназначена для предоставления вычислительных ресурсов для ПТК ДЭГ и формирует следующие группы серверов:

- сервер баз данных (Сервер БД);

- сервер блокчейн (Сервер БЧ);
- сервер балансировки;
- сервер кластера oVirt/TIONIX #1;
- сервер кластера oVirt/TIONIX #2;
- сервер кластера OKD #1;
- сервер кластера OKD #2;
- сервер кластера OKD #3.

Вычислительные ресурсы группы «Сервер БД» предоставлены в виде выделенных физических серверов. На серверах группы ПО СУБД Postgres Pro/ Postgres Pro Certified версии 11 (сертифицированное ПО из реестра МНЦ, имеет сертификат ФСТЭК России № 3637 от 05.10.2016 г., продлен до 05.10.2024 г.).
Для обеспечения доступности данных используются встроенные механизмы СУБД.
Вычислительные ресурсы группы «Сервер БЧ» предоставлены в виде выделенных физических серверов. На серверах группы установлено ПО блокчейн - Блокчейн-платформа Waves Enterprise (Запись в Едином реестре российских программ для электронных вычислительных машин и баз данных №6485 от 07.04.2020 произведена на основании приказа Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 07.04.2020 №162). Целостность и доступность данных обеспечивается ПО блокчейн.
Вычислительные ресурсы группы «Сервер балансировки» предоставлены в виде выделенных физических серверов. На серверах группы установлено ПО балансировки нагрузки. В пределах площадки серверы объединены в кластер для обеспечения отказоустойчивости.
Вычислительные ресурсы группы «Сервер кластера oVirt/TIONIX #1» и группы «Сервер кластера oVirt/TIONIX #2» предоставлены в виде вычислительных кластеров из выделенных физических серверов. На серверах группы установлено ПО виртуализации oVirt, обеспечивающее возможность создания виртуальных вычислительных ресурсов для ПТК ДЭГ, а также агент безопасности TIONIX Virtual Security Agent, обеспечивающие возможности управления и контроля виртуальными вычислительными ресурсами в среде TIONIX (сертифицированное ПО из реестра МНЦ, которое имеет сертификат ФСТЭК России № 4348 от 24.12.2020 г.).
Каждый кластер построен по схеме N+1, где N – количество узлов, необходимое для предоставления ресурсов ПТК ДЭГ и 1 узел для обеспечения отказоустойчивости группы.В случае отказа одного из серверов группы, ПО виртуализации перезапускает виртуальную машину на другом сервере группы.
Для вычислительных ресурсов группы «Сервер кластера oVirt/TIONIX #1» выполняется соотношение 1:1 виртуальных ресурсов к физическим.
Для вычислительных ресурсов в группы «Сервер кластера oVirt/TIONIX #2» выполняется соотношение 2:1 виртуальных ресурсов к физическим.
Вычислительные ресурсы группы «Сервер кластера OKD #1», группы «Сервер кластера OKD #2» и группы «Сервер кластера OKD #3» предоставлены в виде вычислительных кластеров из выделенных физических серверов. На серверах группы установлено ПО контейнеризации, позволяющее управлять контейнерами с программным обеспечением ПТК ДЭГ.
Каждый кластер построен по схеме N+1, где N – количество узлов, необходимое для предоставления ресурсов ПТК ДЭГ и 1 узел для обеспечения отказоустойчивости группы. В случае отказа одного из серверов группы, ПО контейнеризации перезапускает контейнер на другом сервере группы.

1.1.3 Подсистема хранения данных

Подсистема хранения данных предназначена для предоставления ресурсов хранения для ПТК ДЭГ и включает в себя локальные хранилища данных серверов и общее хранилище данных.
Локальные хранилища данных представляют собой локальные диски серверов групп «Сервер БД» и «Сервер БЧ» ёмкостью 3,2 ТБ, выполненные по технологии SSD с использованием протокола NVMe. Для обеспечения сохранности данных диски объединены в Raid 1.
Общее хранилище данных реализовано на СХД и предоставляет ресурсы хранения полезным объёмом 30 ТБ для серверов групп «Сервер кластера oVirt/TIONIX #1» и «Сервер кластера oVirt/TIONIX #2».

Общее хранилище данных обеспечивает следующие показатели производительности:

- время отклика – не более 2 мс;
- не менее 1000 IOPS/TB;
- не менее 150 МБ/сек.

при следующем профиле нагрузки:

- соотношение операций чтение/запись – 20/80;
- блок данных– 8 КБ.

1.1.4 Подсистема сети хранения данных

Подсистема сети хранения данных предназначена для подключения общего хранилища к серверам групп «Сервер кластера oVirt/TIONIX #1» и «Сервер кластера oVirt/TIONIX #2» в пределах одного ЦОД.
Подсистема реализована по принципу dual fabric, что обеспечивает работоспособность сети даже при выходе из строя целиком одной фабрики. В пределах каждой площадки каждый сервер подключенной в сеть группы хранения данных и каждый контроллер СХД включён в 2 коммутатора портами пропускной способностью не менее 16 ГБит/с.

1.1.5 Подсистема сети передачи данных

Подсистема сети передачи данных предназначена для обеспечения сетевого взаимодействия между компонентами ПТК ДЭГ в пределах одного ЦОД.
Коммутаторы сети передачи данных поддерживают подключения устройств пропускной способностью не менее 10 Гб/с.
Для всех компонентов инфраструктуры ПТК ДЭГ, поддерживающих технологию агрегирования каналов, подключение в сеть передачи данных выполнено не менее, чем двумя физическими интерфейсами в режиме active/active.

1.1.6 Подсистема телекоммуникаций

Подсистема телекоммуникаций предназначена для обеспечения отказоустойчивой сетевой связности и сетевого взаимодействия компонентов комплекса технических средств, расположенных на разных площадках между собой, а также с внешними сетями.
Подсистема телекоммуникаций состоит из следующих ресурсов:

- телекоммуникационные ресурсы для взаимодействия с сетью Интернет;
- телекоммуникационные ресурсы для взаимодействия между ЦОД;
- телекоммуникационные ресурсы для взаимодействия с закрытыми сетями ЦИК России.

1.1.7 Телекоммуникационные ресурсы для взаимодействия с сетью Интернет

Взаимодействие с сетью Интернет обеспечено в двух ЦОД: ЦОД-1 и ЦОД-2. Пропускная способность каждого ЦОД составляет не менее 29 Гбит/с.
Каждый ЦОД подключён двумя интерфейсами к разным маршрутизаторам для обеспечения отказоустойчивости.
Телекоммуникационные ресурсы для взаимодействия с сетью Интернет зарезервированы по схеме: основной ресурс – резервный ресурс и не имеют общих точек отказа. Балансировка запросов осуществляется с помощью технологии AnyCast DNS.

1.1.7.1 Телекоммуникационные ресурсы для взаимодействия между ЦОД

Все площадки размещения комплекса технических средств для ПТК ДЭГ объединены между собой в сеть DCI. Сеть защищена с помощью СКЗИ, объединённых в отказоустойчивый кластер.
Пропускная способность соединения между ЦОД-1, ЦОД-2 и ЦОД-3 составляет не менее 5 Гбит/с. Пропускная способность соединения между ЦОД-4 и ЦОД-1, ЦОД-2, ЦОД-3 составляет не менее 3 Гбит/с.
Каждый ЦОД включён в сеть DCI двумя интерфейсами для обеспечения отказоустойчивости.
В рамках одного TCP-соединения обеспечивается пропускная способность не менее 2,5 Гб/с.

1.1.7.2 Телекоммуникационные ресурсы для взаимодействия с закрытыми сетями ЦИК России

Для взаимодействия ПТК ДЭГ с закрытыми сетями ЦИК России используются телекоммуникационные ресурсы ЦОД-3 и ЦОД-4. Взаимодействие с закрытыми сетями ЦИК России защищено с помощью СКЗИ, объединённых в отказоустойчивый кластер.
ЦОД-3 и ЦОД-4 подключены к закрытым сетям ЦИК России двумя интерфейсами для обеспечения отказоустойчивости.

1.1.8 Подсистема резервного копирования

Подсистема резервного копирования предназначена для осуществления резервного копирования и восстановления данных.
Подсистема резервного копирования и восстановления данных соответствует следующим характеристикам и обладает следующей функциональностью:

- создание резервных копий и восстановление данных СУБД Postgres Pro/ Postgres Pro Certified версии 11;
- резервное копирование высоконагруженных компонентов выполняется каждые 15 минут. Полное резервное копирование производится ежедневно с 08:00 до 09:00 и с 23:00 до 00:00, между этими периодами выполняется инкрементальное резервное копирование;
- полное резервное копирование выполняется четыре раза за период повышенной готовности;
- объём защищаемых данных – не менее 960 ГБ;
- глубина хранения - 2 недели;
- RPO одной СУБД объемом до 240 ГБ – не более 15 минут;
- RTO одной СУБД объёмом до 240 ГБ – не более 1 часа.

Объектами для резервного копирования и восстановления являются – БД СУБД Postgres Pro/ Postgres Pro Certified версии 11, файлы конфигураций ПТК ДЭГ.

1.1.9 Инфраструктурные сервисы ЦОД

Для обеспечения функционирования компонентов ПТК ДЭГ предоставляются следующие инфраструктурные сервисы:

- сервис разрешения доменных имён (DNS) внутренней зоны, публичных записей;
- сервис синхронизации точного времени со значением точности не 0 (NTP), функционирующий на базе специализированного оборудования, которое размещено и эксклюзивно используется ПТК ДЭГ в каждом из ЦОД размещения ПТК ДЭГ;
- сервис централизованной аутентификации и авторизации доступа к ОПО и СПО. Не включает в себя аутентификацию и идентификацию в рамках ролевой модели СПО ПТК ДЭГ;
- предоставление удалённого доступа для управления ПТК ДЭГ.

1.2 Решения по составу информации, объему, способам ее организации

1.2.1 Информационное обеспечение

Информационное обеспечение СПО ПТК ДЭГ в части организации и ведения базы данных обеспечивает:

- целостность данных;
- проектирование информационной базы данных проведено с учетом оптимизации по критериям повышения оперативности обработки и снижения объемов хранимых данных;
- дальнейшее развитие информационной базы данных.

Сохранность данных и восстановление работоспособности СПО ПТК ДЭГ при сбоях и авариях обеспечивается применением резервного копирования.
Для обеспечения целостности данных используются встроенные механизмы СУБД.

1.3 Решения по составу программных средств, языкам деятельности, алгоритмам процедур и операций и методам их реализации

СПО ПТК ДЭГ разрабатывается в следующей программной среде:

1) Операционные системы OS на серверах:

- CentOS 8.3 (CentOS Linux – поддерживаемый сообществом дистрибутив, полученный из исходных текстов, свободно предоставленных общественности на Red Hat или CentOS git для Red Hat Enterprise Linux (RHEL). CentOS Linux нацелен на функциональную совместимость с RHEL);
- AltLinux Server 8.2 / Альт 8 СП (AltLinux Server – многофункциональный дистрибутив для серверов с возможностью использования в качестве рабочей станции разработчика комплексных систем, прежде всего, предназначен для использования в корпоративных сетях. Сертификат соответствия № 3866: выдан ФСТЭК России по системе сертификации средств защиты информации 10.08.2018 г., действителен до 10.08.2023 г.).

Центральное место в серверной функциональности занимает комплект «ALT-домен»: взаимосвязанные серверы LDAP, Kerberos, DNS, Samba, DHCP, Postfix, Dovecot, сервер сетевой загрузки, сервер обновлений.

2) Технологический стек:

- Java 11;
- Postgres Pro/ Postgres Pro Certified версии 11;
- Spring Boot 2.3;
- JasperReports;

- Angular 11.

3) Для контейнеризации при разработке используются следующие программные средства:

- OKD 4.5 (это исходная и поддерживаемая сообществом версия платформы Red Hat OpenShift Container Platform (OCP). OpenShift превращает обычный Kubernetes в платформу приложений, предназначенную для масштабного корпоративного использования. Начиная с выпуска OpenShift 4, операционной системой по умолчанию является Red Hat CoreOS, которая обеспечивает неизменяемую инфраструктуру и автоматические обновления.
- Fedora CoreOS 32.2 (Fedora CoreOS, как и OKD, является исходной версией Red Hat CoreOS).

4) Для мониторинга работоспособности в спроектированной системе используются:

- Grafana 7.4 (программное обеспечение для визуализации и аналитики с открытым исходным кодом. Позволяет запрашивать, визуализировать, предупреждать и исследовать метрики независимо от того, где они хранятся. Предоставляет инструменты для преобразования базы данных временных рядов (TSDB) в графики);
- Prometheus 2.18 (набор инструментов с открытым исходным кодом для систем мониторинга и оповещения). Основные функции Prometheus:
    - многомерная модель с данными временных рядов, идентифицированных по метрическим названиям и парам ключ/значение;
    - PromQL, гибкий язык запросов для использования этой размерности.
    - отсутствие зависимости от распределенного хранилища;
    - отдельные серверные узлы автономны;
    - сбор временных рядов происходит через модель «тянуть» по HTTP;
    - толкающие временные ряды поддерживаются через промежуточный шлюз;
    - цели обнаруживаются через обнаружение сервиса или статическую конфигурацию;
    - несколько режимов отображения графиков и поддержки приборных панелей.