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

Описание ПТК ДЭГ

2021

Содержание

1. ОБЩИЕ ПОЛОЖЕНИЯ

Дистанционное электронное голосование представляет собой голосование без использования избирательного бюллетеня, изготовленного на бумажном носителе, с использованием специального программного обеспечения, установленного на программно-техническом комплексе дистанционного электронного голосования (далее – ПТК ДЭГ), доступ к которому избирателю (участнику референдума) предоставляется на специальном портале, размещенном в сети Интернет.

Пользователями ПТК ДЭГ являются избиратели, участники референдума, члены избирательных комиссий, задействованных в проведении ДЭГ, и наблюдатели.

2. ОСНОВНЫЕ УЧАСТНИКИ ПРОЦЕССА ДЭГ

В настоящем разделе кратко перечислены основные участники процесса ДЭГ и их роли.

Участник ДЭГ

Гражданин РФ, обладающий:

- подтверждённой учётной записью в федеральной государственной информационной системе «Единый портал государственных и муниципальных услуг (функций)» (далее – ЕПГУ), данные которой сопоставлены с данными Регистра избирателей, участников референдума ГАС «Выборы»;

- поданным в электронной форме на ЕПГУ заявлением для участия в ДЭГ в статусе «Учтено».

Оператор Единой системы идентификации и аутентификации

Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации (далее – Минцифры России), оператор федеральной государственной информационной системы «Единая система идентификации и аутентификации» (далее – ЕСИА).

В процессе ДЭГ ЕСИА используется в качестве внешней по отношению к ПТК ДЭГ системы идентификации и аутенфикации участника ДЭГ. Администраторы ЕСИА не имеют доступа к ПТК ДЭГ и не совмещают функции администраторов ПТК ДЭГ.

Оператор ЕПГУ

Минцифры России.

На ЕПГУ гражданин РФ в электронной форме подает заявление для участия в ДЭГ (далее – заявление ДЭГ), отправка которого подтверждается вводом СМС-кода, направленного на номер мобильного телефона, указанный в профиле пользователя ЕПГУ.

Заявление в виде xml-файла подписывается электронной подписью ЕПГУ и средствами Единой системы межведомственного электронного взаимодействия (далее – СМЭВ) направляется в Центральную избирательную

комиссию Российской Федерации (далее – ЦИК России). Результат обработки заявления ДЭГ ЦИК России отображается в личном кабинете пользователя ЕПГУ.

Администраторы ЕПГУ не имеют доступа к ПТК ДЭГ и не совмещают функции администраторов ПТК ДЭГ.

Регистратор

ЦИК России.

Регистратором осуществляется обработка поступивших заявлений ДЭГ, а также формирование данных для составления списков участников ДЭГ.

Кроме того, он является держателем ключей регистратора по каждому голосованию, и сервиса подписи вслепую открытого ключа участника ДЭГ, обеспечивающего доступ к бюллетеню.

Организатор ДЭГ

Территориальная избирательная комиссия ДЭГ (далее – ТИК ДЭГ). Формирование ТИК ДЭГ осуществляется в соответствии с порядком дистанционного электронного голосования (далее – Порядок ДЭГ), утверждаемым Постановлением ЦИК России. Функции Организатора ДЭГ реализуются с помощью компонента «Организация и проведение ДЭГ», имеющего разграничение прав доступа с помощью сертифицированных средств защиты информации.

К основным функциям Организатора ДЭГ относятся:

- генерация ключевой пары и разделение первого ключа шифрования бюллетеня между держателями частей ключа по схеме Шамира с помощью изолированного от сети компонента «Генерация и разделение ключей шифрования» в присутствии средств массовой информации;

- загрузка исходных данных о голосованиях, полученных от Организующих выборы избирательных комиссий;

- загрузка данных о поданных и учтенных заявлениях от Регистратора для формирования списка участников ДЭГ;

- формирование запроса на создание ключей регистратора по каждому голосованию;

- генерация ключевой пары для формирования итогового ключа шифрования бюллетеней для каждого голосования;

- запуск и остановка голосования;

- сборка ключа из частей, полученных от держателей части ключа с помощью изолированного от сети компонента «Генерация и разделение ключей шифрования» в присутствии средств массовой информации и наблюдателей;

- загрузка собранного ключа расшифрования в блокчейн (ключа комиссии);

- запуск подсчета голосов: формирование итогового бюллетеня и его расшифровка;

- получение данных об итогах голосования и протокола об итогах голосования;

- подписание протокола об итогах голосования с помощью электронной подписи.

Администраторы Организатора ДЭГ имеют доступ к ПТК ДЭГ в пределах компонента «Организация и проведение ДЭГ», а также имеют доступ к интерфейсам мониторинга компонентов «Портал ДЭГ», «Распределенное хранение и учет голосов» в части отдельных узлов, формирующих блоки.

При этом, администраторы Организатора ДЭГ не имеют учетных записей в компоненте «Распределенное хранение и учет голосов» и доступа к хранилищу ключей регистратора.

Организующие избирательные комиссии

Избирательные комиссии, организующие выборы (определяющие результаты выборов на территории): ЦИК России, ИКСРФ, ТИК, осуществляют подготовку в ГАС «Выборы» исходных данных (текст

бюллетеня, форма протокола) для передачи Организатору ДЭГ через «воздушный зазор».

После завершения голосования получают от Организатора ДЭГ данные об итогах ДЭГ для загрузки в ГАС «Выборы».

Внутренний наблюдатель

Участник, осуществляющий наблюдение за процессом голосования из специализированного помещения, оснащенного средствами доступа к отдельным узлам компонента «Распределенное хранение и учет голосов».

Может осуществлять действия по поиску данных в распределенной БД, просмотр этих данных, просмотр списков избирателей, исходных данных. Имеет доступ к расширенным метрикам мониторинга работы системы.

С помощью специализированного инструмента с открытым кодом, может выгружать и проверять корректность расшифровки итогового бюллетеня.

Не имеет доступа к другим компонентам ПТК ДЭГ.

Внешний наблюдатель

Любой пользователь, осуществляющий наблюдение за процессом голосования с портала наблюдения, публикующего статистические данные о голосовании в информационно-телекоммуникационную сеть Интернет. Имеет возможность получить выгрузку транзакций из сети блокчейн в виде файлов, публикуемых на портале наблюдения.

Используя программный инструментарий с открытым кодом, внешний наблюдатель может:

- проверить целостность транзакции;
- проверить криптографические доказательства корректности бюллетеня;
- проверить корректность суммарного шифротекста;
- проверить криптографические доказательства корректности расшифровки;
- проверить корректность суммирования частичных расшифровок суммарного бюллетеня.

3. ОСНОВНЫЕ КОМПОНЕНТЫ ПТК ДЭГ

3.1. Компонент «Портал ДЭГ»

(vybory.gov.ru – основная точка контакта с участниками ДЭГ)

Компонент включает в себя:

- приложение, исполняемое в браузере участника ДЭГ, отображающее страницы Портала ДЭГ. После прохождения идентификации отображает участнику ДЭГ доступные для него бюллетени (голосования), осуществляет генерацию ключевой пары, обращение с сервисом регистратора для подписания открытого ключа слепой подписью, сохранение ключевой пары, формирование анкор-ссылки (ссылки, сформированной таким образом, что часть информации, находящаяся за символом # (анкор) не передается на сервер, а остается в браузере пользователя) для перехода в анонимную зону;
- сервис аутентификации и идентификации участника ДЭГ с помощью ЕСИА (deg-auth-service);
- сервис, взаимодействующий с приложением пользователя (portal front);
- сервис, проверяющий возможность исполнения криптографических функций и функций отображения страниц на устройстве пользователя, запускается автоматически во время проведения голосования (deg-voting-test-service);
- сервис, вызывающийся по ссылке с главной страницы, проверяет версию веб-браузера пользователя на совместимость, доступен и до, и во время проведения голосования (portal-checkup);
- сервис, отправляющий пользователю код подтверждения в качестве второго фактора аутентификации (deg-sms-sender);
- сервис, формирующий обращение в службу технической поддержки при сложностях при использовании портала голосования (deg-support-service);

3.2. Компонент «Сервис анонимного волеизъявления»

(edg.gov.ru, физически изолированное место, позволяющее участнику ДЭГ осуществить волеизъявление сохранив тайну голосования)

Компонент, который является анонимной зоной Портала ДЭГ и проверяет использование ключей участников ДЭГ, передает текст бюллетеня на клиентскую часть, принимает обратно заполненные зашифрованные бюллетени, и отправляет их в компонент «Распределенное хранение и учет голосов». Компонент включает в себя:

- приложение, исполняемое в браузере участника ДЭГ, отображающее бюллетени Анонимной зоны Портала ДЭГ, которое извлекает зашифрованные ключи из анкор-ссылки, отображает участникам ДЭГ форму и текст бюллетеней в браузере, получает от серверной части ключ шифрования голосования, шифрует бюллетень, формирует доказательство корректности бюллетеня (zkp) перед отправкой, подписывает бюллетень анонимным ключом участника ДЭГ;
- сервис взаимодействия с клиентским приложением (deg-voting-ssr)
- сервис отображения статичной информации (portal-anon-nginx)
- сервис, отвечающий за прием бюллетеня и осуществляющий контроль двойного голосования, а также осуществляющий передачу бюллетеня в очередь брокера сообщений (deg-voting-box)
- вычислительно-сетевой сегмент, в котором располагается БД ключей голосования на базе сертифицированной СУБД PostgrePro SQL (сертифицированное ПО из реестра МНЦ).

3.3. Компонент «Организация и проведение ДЭГ»

Компонент включает в себя:

- приложение, исполняемое в браузере Председателя и члена ТИК ДЭГ (Организатора ДЭГ), отображающее страницы административного интерфейса;

- сервис, обеспечивающий исполнение функций портала администратора: загрузка описателей (моделей) избирательных кампаний, голосований, бюллетеней и протоколов, загрузка списка участников ДЭГ, создание голосований в БД, исключение из списка участников ДЭГ и восстановление, создание голосований и загрузка списков избирателей в компоненте «Распределенное хранение данных и учёт голосов», старт выдачи бюллетеней, остановка выдачи бюллетеней и приема голосов (deg-admin-service);

3.4. Компонент «Список участников ДЭГ»

Компонент включает в себя:

- сервис, участвующий в процессе загрузки списка участников ДЭГ, проверки избирательного права и отметки о получении бюллетеня (deg-registry-service);
- сервис, предназначенный для генерации ключей регистратора и выдачи слепых подписей (deg-crypto-service);
- вычислительно-сетевой сегмент, в котором располагается БД Списка участников ДЭГ на базе СУБД PostgrePro SQL (сертифицированное ПО из реестра МНЦ)

3.5. Компонент «Распределенное хранение данных и учёт голосов»

Узлы сети блокчейн, которые принимают данные от Избирательного ящика, хранят все данные о голосовании (зашифрованные бюллетени, параметры для выработки ключей, данные о начале/окончании голосования и т.д.), обеспечивают их целостность и общедоступность. Компонент включает в себя:

- сервисы, формирующие обмен информации с сегментом сети блокчейн;
- сервис Декриптор, осуществляющий генерацию второго ключа шифрования, создание смарт-контракта, суммирование зашифрованных бюллетеней, расшифровку суммарного бюллетеня после завершения

голосования и загрузки собранного ключа, публикацию частичных расшифровок и итоговых результатов голосования;

- сервис создания и запуска смарт-контракта голосования;
- сегмент сети блокчейн (ноды в сети блокчейн);
- вычислительно-сетевой сегмент на аппаратных серверах для работы с сегментом блокчейн.

3.6. Компонент «Генерация и разделение ключей шифрования»

Компонент включает в себя:

- приложение для разделения и сбора ключей шифрования.

3.7. Компонент «Центр наблюдения за голосованием»

Компонент включает в себя:

- сервис, отображающий страницы Портала наблюдения (observer-front);
- сервис, подготавливающий страницу для портала наблюдения (deg-observer-service);
- сервис, обращающийся к аналитической БД, содержащей все произведенные транзакции и созданные блоки в процессе голосования (beg-statistics-service);
- вычислительно-сетевой сегмент, в котором располагаются аналитические базы данных.

3.8. Компонент «Центр мониторинга ПТК ДЭГ»

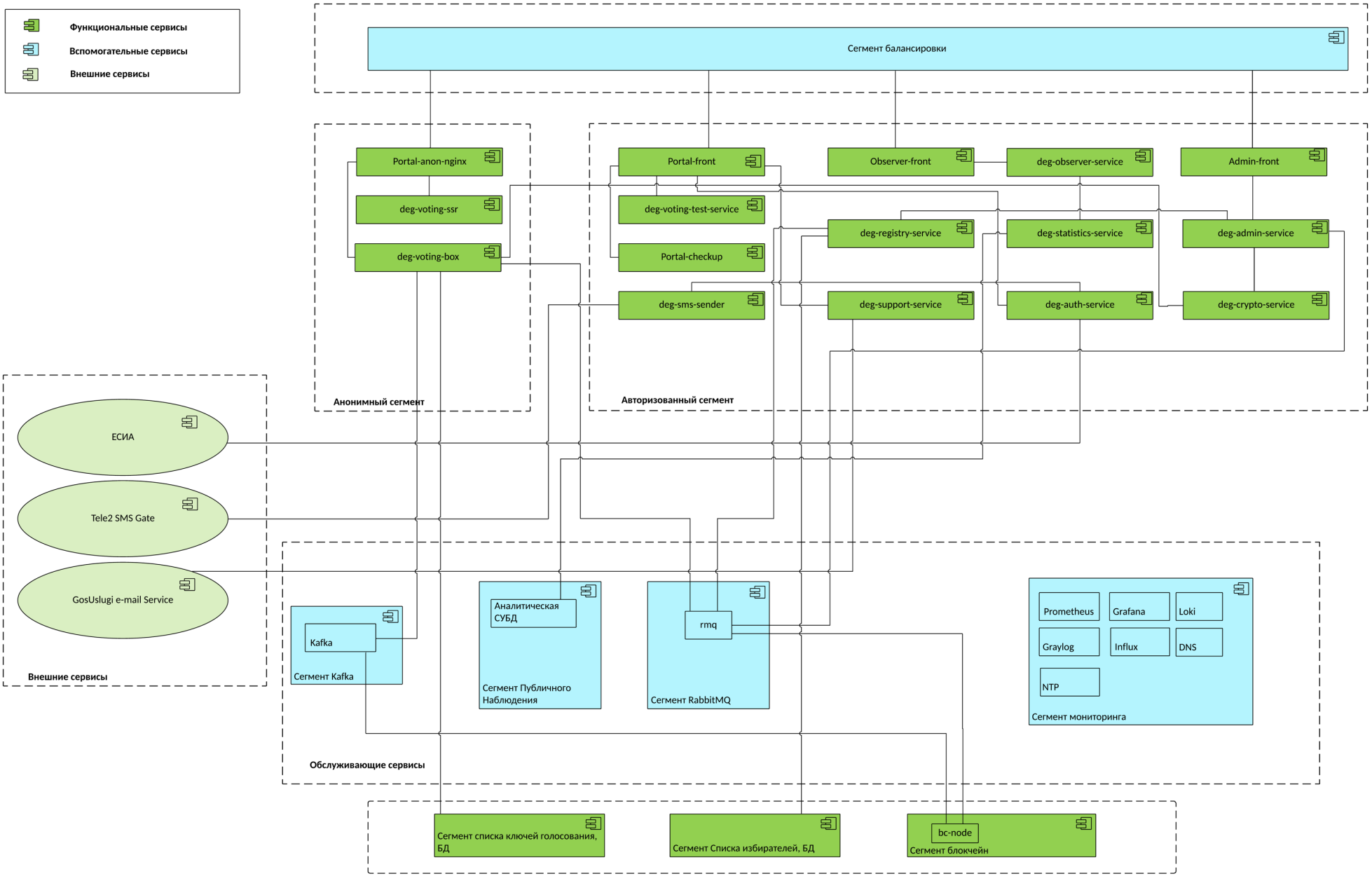
Компонент включает в себя:

- NTP - сервис точного времени для синхронизации сигнала точного времени по радиоканалу (метрологические сертификаты);
- виртуальные машины, собирающие как метрики производительности аппаратных и программных компонентов, так и бизнес-метрики СПО;
- виртуальные машины, собирающие текстовые сообщения об ошибках ОС, ОПО и СПО;

- виртуальные машины, обеспечивающие функционирование внутренних графических представлений компонентов мониторинга;
- виртуальные машины СУБД временных рядов компонента «Распределенное хранение данных и учёт голосов», накапливающие бизнес-метрики производительности;
- виртуальные машины, собирающие текстовые сообщения об ошибках компонента «Распределенное хранение данных и учёт голосов»;
- виртуальные машины, обеспечивающие разрешение имён внутри СПО ПТК ДЭГ (на время проведения голосования разрешение имен ресурсов сети Интернет недоступно);
- сервис, отображающий страницы портала системного администратора компонента «Центр мониторинга ПТК ДЭГ» (admin)

3.9. Схема компонентов и их взаимосвязи

Взаимосвязи функциональных компонентов представлены на схеме:


Функциональные сервисы
Вспомогательные сервисы
Внешние сервисы
Сегмент балансировки
Portal-anon-nginx
deg-voting-ssr
deg-voting-box
Portal-front
deg-voting-test-service
Portal-checkup
deg-sms-sender
Observer-front
deg-observer-service
Admin-front
deg-registry-service
deg-statistics-service
deg-admin-service
deg-support-service
deg-auth-service
deg-crypto-service
Анонимный сегмент
Авторизованный сегмент
ЕСИА
Tele2 SMS Gate
GosUslugi e-mail Service
Внешние сервисы
Kafka
Сегмент Kafka
Аналитическая СУБД
Сегмент Публичного Наблюдения
rmq
Сегмент RabbitMQ
Prometheus
Grafana
Loki
Graylog
Influx
DNS
NTP
Сегмент мониторинга
Обслуживающие сервисы
Сегмент списка ключей голосования, БД
Сегмент Списка избирателей, БД
bc-node
Сегмент блокчейн

4. СТРУКТУРА И СЕГМЕНТАЦИЯ ПТК ДЭГ

ПТК ДЭГ разделен на следующие ключевые внутренние сетевые сегменты

Наименование компонента	Сервис	Наименование внутреннего сетевого сегмента	Перечень аппаратных компонентов
Портал ДЭГ	portal-front	Сегмент портала, усиленный сетевыми политиками	Кластер серверных узлов #1
	deg-voting-test-service	Сегмент портала, усиленный сетевыми политиками	Кластер серверных узлов #1
	portal-checkup	Сегмент портала, усиленный сетевыми политиками	Кластер серверных узлов #1
	deg-sms-sender	Сегмент портала, усиленный сетевыми политиками	Кластер серверных узлов #1
	deg-auth-service	Сегмент портала, усиленный сетевыми политиками	Кластер серверных узлов #1
	deg-support-service	Сегмент портала, усиленный сетевыми политиками	Кластер серверных узлов #1
Сервис анонимного волеизъявления	portal-anon-nginx	Анонимный сегмент, усиленный сетевыми политиками	Кластер серверных узлов #2
	deg-voting-ssr	Анонимный сегмент, усиленный сетевыми политиками	Кластер серверных узлов #2
	deg-voting-box	Анонимный сегмент, усиленный сетевыми политиками	Кластер серверных узлов #2
	keyz	Фронтальный сегмент СУБД ключей голосования	Аппаратный сервер СУБД #2
	keyz	Сегмент синхронной репликации СУБД ключей голосования	
	kafka1	Сегмент брокера сообщений #1	Кластер серверных узлов виртуализации #1
Проведения и организация ДЭГ	admin-front	Сегмент проведения и организации ДЭГ	Кластер серверных узлов #3
	admin-service	Сегмент проведения и организации ДЭГ	Кластер серверных узлов #3
	deg-crypto-service	Сегмент проведения и организации ДЭГ	Кластер серверных узлов #3
	rmq	Сегмент очереди сообщений	Кластер серверных узлов виртуализации #1
Список участников ДЭГ	elecdb	Фронтальный сегмент СУБД	Аппаратный сервер СУБД #1
	elecdb	Сегмент синхронной репликации СУБД	
	deg-registry-service	Фронтальный сегмент списка участников	Кластер серверных узлов #1
	deg-crypto-service	Сегмент проведения и организации ДЭГ	Кластер серверных узлов #3

Наименование компонента	Сервис	Наименование внутреннего сетевого сегмента	Перечень аппаратных компонентов
Распределенное хранение данных и учёт голосов	bc-node	Сегмент создания блоков и производства транзакций	Кластер серверных узлов #БЧ
Генерация и Разделение ключей шифрования	Генерация и Разделение ключей шифрования	Сетевой доступ отсутствует	Мобильная рабочая станция #1
Центр наблюдения за голосованием	observer-front	Сегмент портала, усиленный сетевыми политиками	Кластер серверных узлов #1
	deg-observer-service	Сегмент портала, усиленный сетевыми политиками	Кластер серверных узлов #1
	deg-statistics-service	Сегмент портала, усиленный сетевыми политиками	Кластер серверных узлов #1
	kafka2	Сегмент брокера сообщений #2	Кластер серверных узлов виртуализации #1
	СУБД онлайн-обработки аналитических запросов	Фронтальный сегмент аналитической СУБД	Кластер серверных узлов виртуализации #1
Центр мониторинга ПТК ДЭГ	NTP и другие сервисы	Сегмент мониторинга, усиленный сетевыми политиками	Кластер серверных узлов виртуализации #2

5. ОСНОВНЫЕ ЭТАПЫ ПРОЦЕССА ДЭГ

ФАЗА 1. Подготовка к голосованию

5.1. Формирование данных для списка участников ДЭГ

Избиратель на ЕПГУ подает заявление для участия в ДЭГ. Регистратор осуществляет проверку заявления и формирует данные для списка участников ДЭГ, которые записываются на внешний носитель информации с возможностью однократной записи информации (далее – внешний носитель).

Включенные в список исключаются из списков избирателей на традиционных участках.

5.2. Разделение ключа шифрования Организатора ДЭГ

Организатор ДЭГ в присутствии СМИ с помощью отдельного компонента «Генерация и разделение ключей шифрования» производит генерацию ключевой пары и разделение ключа расшифрования между держателями частей ключа. Ключ шифрования записывается на внешний носитель.

5.3. Подготовка ПТК ДЭГ

Организатор ДЭГ получает на внешнем носителе:

- данные для формирования списка участников голосования;
- исходные данные о голосовании: описатель протокола, текст бюллетеня, количество вариантов, идентификаторы организующих и определяющих результаты выборов на территории избирательных комиссий;

и загружает данные в ПТК ДЭГ с использованием компонента «Организация и проведение ДЭГ».

После загрузки данных Организатор ДЭГ дает команду создания экземпляров смарт-контракта голосования (по соответствующим выборам и каждому избирательному округу (территории) в компоненте «Распределенное хранение данных и учет голосов» (сети блокчейн).

Для этого по каждому голосованию (по соответствующим выборам и каждому избирательному округу (территории):

- дается команда на генерацию отдельной ключевой пары регистратора, которая будет использоваться в процедуре анонимизации (слепой подписи);
- дается команда на генерацию отдельной ключевой пары организующей комиссии, которая будет использоваться для создания общего ключа шифрования бюллетеней;
- сервис Декриптор создает экземпляр смарт-контракта с публикацией транзакции в сети блокчейн, с параметрами ключа регистратора, датой и временем начала голосования, размерностью бюллетеня и результатами хеш-функции от текста бюллетеня;

После создания смарт-контракта в сети блокчейн начинается загрузка списка участников голосования. Для этого результаты HMAC функции от идентификаторов участников ДЭГ загружаются в сеть блокчейн в каждый экземпляр смарт-контракта.

На последнем этапе подготовки с внешнего носителя загружается ключ шифрования Организатора ДЭГ (созданный согласно п. 5.2). Декриптор создает общий ключ шифрования из ключа шифрования Организатора ДЭГ и ключа шифрования организующей комиссии и отправляет транзакцию в сеть блокчейн для каждого экземпляра смарт-контракта голосования.

ФАЗА 2. Получение доступа к бюллетеню

5.4. Аутентификация пользователя с помощью ЕСИА:

Участник ДЭГ переходит на страницу vybory.gov.ru и приступает к голосованию. Портал ДЭГ формирует и отправляет в ЕСИА запрос на аутентификацию и перенаправляет браузер пользователя на страницу предоставления доступа.

Открывается окно ввода логина и пароля профиля в ЕСИА, пользователь вводит свои данные.

ЕСИА осуществляет аутентификацию пользователя. После аутентификации ЕСИА сообщает пользователю, что система (портал) запрашивает данные о нем в целях проведения идентификации и аутентификации, предоставляя перечень запрашиваемых сведений.

Если пользователь дает разрешение на проведение аутентификации системой, то ЕСИА выдает системе авторизационный код.

Система формирует в адрес ЕСИА запрос на получение маркера идентификации, включая в запрос полученный ранее авторизационный код.

ЕСИА проверяет корректность запроса (в том числе, факт регистрации системы в ЕСИА) и авторизационного кода и передает системе маркер идентификации.

После получения маркера идентификации система использует REST-сервисы ЕСИА для получения дополнительных данных о пользователе, предварительно получив соответствующий маркер доступа.

Набор атрибутов, которые запрашиваются в ЕСИА со стороны ПТК ДЭГ:

- firstName – Имя;
- lastName – Фамилия;
- middleName – Отчество;
- birthDate – Дата рождения;
- snils – СНИЛС;
- phone_number – Номер мобильного телефона;
- type – Паспорт гражданина РФ;
- series – Серия документа;
- number – Номер документа;
- issueDate – Дата выдачи документа;
- issuedBy – Кем выдан;
- issueId – Код подразделения.

5.5. Тестирование браузера

Тестирование браузера производится автоматически для всех пользователей, прошедших успешную идентификацию в ЕСИА.

Тестирование браузера осуществляется путем выполнения процедуры получения тестовой слепой подписи.

Если браузер не проходит проверку, то пользователю выводится сообщение о том, что голосование с использованием этого браузера невозможно.

5.6. Поиск в списке участников ДЭГ

Портал ДЭГ обращается к компоненту «Список участников ДЭГ» с запросом информации по идентификатору участника ДЭГ (СНИЛС). В ответе возвращается результат поиска по спискам участников ДЭГ - все доступные участнику избирательные кампании и бюллетени. Если в результате поиска ничего не найдено, пользователю выводится сообщение о том, что он не включен в список участников ДЭГ.

5.7. Ознакомление с техническими условиями ДЭГ

На следующем шаге участник ДЭГ предупреждается о возможности голосования только один раз по каждому из доступных бюллетеней и о том, что необходимо использовать то же устройство и браузер, если процедура голосования будет прервана по какой-либо причине.

5.8. Подтверждение СМС-кодом

На номер мобильного телефона участника ДЭГ отправляется код подтверждения в СМС-сообщении. Участник ДЭГ вводит полученный СМС-код на экранной форме. При корректном вводе кода участник ДЭГ информируется об успешном подтверждении личности.

5.9. Процедура анонимизации

На следующем шаге участник ДЭГ проходит процедуру анонимизации. При запуске процедуры в браузере пользователя генерируется ключевая пара из публичного и приватного ключа для каждого бюллетеня.

На публичный ключ браузером накладывается ослепляющий слой (маскирование ключа), и Регистратору отправляется пакет для каждого

голосования состоящий из массива данных – идентификатор голосования (voting_id) и ослепленный публичный ключ (Компонент «Список участников ДЭГ»)

Компонент проверяет наличие участника ДЭГ в списке и факт того, что по таким идентификаторам слепая подпись не выдавалась ранее, и, если проверка пройдена, начинает протокол выдачи слепой подписи. При успешном завершении протокола транзакция факта выдачи слепой подписи публикуется в сеть блокчейн (записывается commitment идентификатора участника ДЭГ и маскированная подпись).

После получения слепых подписей от по всем голосованиям, в браузере участника ДЭГ формируется анкор-ссылка перехода в анонимную зону, содержащая пакет с идентификатором голосования, зашифрованными ключами со снятой маской и их слепыми подписями по каждому голосованию.

ФАЗА 3. Голосование

5.10. Голосование в анонимной зоне Портала ДЭГ

При переходе в анонимную зону участник ДЭГ может воспользоваться дополнительными средствами усиления анонимности: использования VPN, смена IP адреса, использование TOR сети и т.д.

В анонимной зоне в браузере пользователя происходит расшифровка пакета с ключами пользователя, слепой подписи, и идентификатора голосования.

Далее в компоненте «Сервис анонимного волеизъявления» производится проверка полученного публичного ключа на однократность голосования.

Участнику ДЭГ отображается бюллетень по соответствующему голосованию. При выборе одного или нескольких вариантов (в зависимости от правил заполнения бюллетеня) производится шифрование выбора (голоса) с помощью публичного ключа шифрования голоса (public_vote).

После этого в браузере участника ДЭГ формируется транзакция, состоящая из зашифрованного голоса, криптографического доказательства корректности бюллетеня, анонимного публичного ключа и слепой подписи. Сформированная транзакция подписывается анонимной ключевой парой участника ДЭГ и отправляется в компонент «Сервис анонимного волеизъявления»

В компоненте «Сервис анонимного волеизъявления» производится проверка анонимного публичного ключа на однократность голосования. Если участник ДЭГ не голосовал по данному бюллетеню, производится проверка слепой подписи. В случае успешной проверки транзакция отправляется в сеть блокчейн (вызов смарт-контракта), где проверяется корректность формата бюллетеня и подпись регистратора, и подпись транзакции, обеспечивающей ее целостность.

После отправки транзакции с зашифрованным голосов участнику ДЭГ отображается следующий доступный ему бюллетень.

ФАЗА 4. Завершение голосования и установление итогов.

5.11. Прекращение выдачи доступов к бюллетеням

В момент завершения голосования Организатором ДЭГ в компоненте «Организация и проведение ДЭГ» дается команда на прекращение процедур идентификации участников ДЭГ и подписания «слепой» подписью ключей. При этом, участники ДЭГ, ранее подписавшие свои ключи и находящиеся в анонимной зоне Портала ДЭГ могут продолжить голосование до окончания приема голосов (не менее 15 минут).

5.12. Прекращение приема голосов

По истечении установленного промежутка времени по команде Организатора ДЭГ дается команда о завершении голосования в виде транзакции в блокчейн. Смарт-контракт, получив такую транзакцию, прекращает прием транзакций к зашифрованными голосами.

5.13. Церемония сборки ключа расшифрования

После завершения приема голосов проводится сборка ранее распределенного ключа расшифрования бюллетеней из частей, предоставленных держателями частей ключа (п.5.2). Собранный ключ расшифрования загружается в сеть блокчейн Организатором ДЭГ через компонент «Организация и проведение ДЭГ».

5.14. Подсчет итогов

Декриптор получает транзакции из блокчейна, проверяет криптографическое доказательство корректности бюллетеня без его расшифровки (zero knowledge proof, zkp). В случае успешной проверки шифртексты голосов участников ДЭГ гомоморфно складываются, формируя суммарный шифротекст.

После публикации собранного ключа Организатором ДЭГ Декриптор частично расшифровывает на каждом ключе (ключе Организатора ДЭГ и ключе организующей комиссии) суммарный бюллетень, который они получили, формируют криптографические доказательства корректности расшифровки и публикует их в сеть блокчейн.

После публикации частичных расшифровок суммарного бюллетеня Декриптором проводится их суммирование и формирование итогов, которые публикуются в блокчейн в расшифрованном виде

5.15. Аудит

Внутренние и внешние наблюдатели имеют возможность проверить корректность подсчета итоговых результатов голосования с помощью специализированного инструментария.