**Определения и сокращения**

|  |  |
| --- | --- |
| БЧ | Блокчейн |
| ДИТ | Департамент информационных технологий г. Москвы |
| ДЭГ | Дистанционное электронное голосование |
| ИС | Информационная система |
| КЗ | Контролируемая зона |
| МДМ | Master Data Managment (MDM) |
| ПАК | Программно-аппаратный комплекс |
| ПО | Программное обеспечение |
| СБ | Сервис бюллетеней |
| СШБ | Сервис шифрования бюллетеней |
| СШ ДИ | Сервис шифрования данных избирателя |
| СЗИ | Средство защиты информации |
| СКЗИ | Средство криптографической защиты информации |
| СУДИР | Система управления доступом к информационным ресурсам г. Москвы |
| СБ | Сервис бюллетеней |
| СТП | Служба технической поддержки |
| УИК | Участок избирательной комиссии |
| ЭП | Электронная подпись |
| API | Application Programming Interface |
| HMAC | Hash-based message authentication code |
| TLS | Протокол Transport Layer Security |

### Участники ДЭГ

В настоящем разделе кратко перечислены основные участники системы ДЭГ и их функции, а также компоненты, которыми они представлены.

**Избиратель**

Участник, являющийся гражданином, обладающим активным избирательным правом и включенным в списки избирателей.

Осуществляет доступ к серверным компонентам системы ДЭГ посредством браузера или МП (мобильного приложения).

**Организатор**

Участник, осуществляющий организацию процесса голосования. Данный участник, в частности, осуществляет управление голосованием с использованием компонента:

*АРМ Председателя*

Компонент, осуществляющий взаимодействие с другими компонентами ДЭГ при старте и окончании голосования.

**Комиссия**

Распределенный участник, обеспечивающий конфиденциальность промежуточных итогов. Генерирует и разделяет ключ шифрования бюллетеней с использованием компонента:

*Доверенный компонент генерации ключа шифрования бюллетеней*

На данном компоненте комиссия генерирует ключ шифрования бюллетеней и разделяет его.

**Регистратор**

Участник, осуществляющий идентификацию и аутентификацию избирателей с помощью СУДИР и предоставляющий избирателям право получения бюллетеня. Этим правом является значение HMAC. В настоящей системе данный участник состоит из следующих компонент.

*Форма БЭК*

Компонент, осуществляющий идентификацию и аутентификацию избирателей с помощью СУДИР и выдающий доступ к бюллетеню (бюллетеням). Этим доступом является значение HMAC.

*МДМ*

Компонент, осуществляющий проверку нахождения избирателя в списках для голосования и замену идентификатора избирателя СУДИР на обезличенный идентификатор.

*Компонент Х + СШ ДИ*

Компонент Х и Сервис шифрования данных избирателя (СШ ДИ) независимые компоненты шифрования. Далее по тексту под Компонентом Х понимается Компонент Х + СШ ДИ. Данные участники вычисляет обезличенный групповой идентификатор избирателя.

**Урна**

Участник, выдающий избирателям бюллетени и принимающий обратно заполненные зашифрованные бюллетени. В настоящей системе данный участник представлен в виде компонента СБ + СШБ.

*СБ + СШБ*

Компонент Сервис бюллетеней (СБ) и Сервис шифрования бюллетеней (СШБ) логически отдельные компоненты. Далее по тексту под СБ понимается СБ + СШБ. Данный участник выдает избирателям бюллетени и принимает обратно заполненные зашифрованные бюллетени. Также данный участник направляет зашифрованные бюллетени и другие данные в БЧ1 и БЧ2 через общий интерфейс Сервиса взаимодействия с БЧ.

**Учетчик**

Участник, представляющий собой публичное хранилище бюллетеней и других данных, к которому есть постоянный доступ на чтение у всех участников, а также осуществляющий подсчет итогов. В системе данный участник представлен в виде компонент БЧ1 и БЧ2. Отправка данных в эти компоненты осуществляется с использованием Сервиса взаимодействия с БЧ.

*Сервис взаимодействия с БЧ*

Предоставляет интерфейс для направления данных в БЧ. Разбирает входящий запрос и распределяет данные между БЧ1 и БЧ2.

*БЧ1 (публичный)*

Компонент, представляющий собой хранилище зашифрованных бюллетеней.

*БЧ2 (закрытый)*

Компонент, представляющий собой хранилище связей обезличенных групповых идентификаторов избирателя с бюллетенями, а также осуществляющий подсчет итогов.

*Портал наблюдения*

Компонент, представляющий внешний доступ на чтение к БЧ1.

**Подведение итогов**

*Прекращение выдачи бюллетеней*

1. Организатор останавливает работу Формы БЭК через СТП (участок закрыт). После этого пройти аутентификацию и зайти на Форму БЭК невозможно.

*Прекращение приема бюллетеней*

1. Через 15 минут после закрытия Формы БЭК Организатор направляет команду в АРМ Председателя об окончании голосования. АРМ Председателя направляет уведомление в Сервис взаимодействия с БЧ об окончании голосования. После смены статуса в Сервисе взаимодействия с БЧ АРМ Председателя направляет уведомления компонентам МДМ, Х и СБ об окончании голосования. Получение и отправка бюллетеня становится невозможной.

*Церемония восстановления закрытого ключа шифрования бюллетеней*

1. По команде Организатора Комиссия проводит церемонию восстановления закрытого ключа шифрования бюллетеней **sk**.
2. Организатор загружает **sk** через АРМ Председателя в БЧ1 и направляет команду на расшифрование голосов. При этом проверяется соответствие закрытого ключа sk открытому ключу pk.

*Подсчет и расшифрование итогов*

Описанные ниже взаимодействия между всеми компонентами осуществляются через Сервис взаимодействия с БЧ.

1. БЧ1 расшифровывает ключом **sk** все голоса evotes и осуществляет проверку расшифрованных голосов votes на корректность. В частности, осуществляется проверка того, что бюллетень содержит верные идентификаторы кандидатов (опубликованные в БЧ1 при старте голосования), нет повторов идентификаторов, количество выбранных кандидатов находится в допустимом диапазоне, который задается также при старте голосования.
2. БЧ2 направляет запрос в СБ на расшифрование egid2.
3. СБ расшифровывает egid: gid = DK2(egid).

СБ генерирует случайный идентификатор mgid, соответствующий gid.

СБ возвращает mgid в БЧ2.

1. БЧ2 группирует значения H(evote) по значениям mgid.

БЧ2 для каждого mgid выбирает H(evote) с наибольшим временем time.

БЧ2 направляет H(evote) в БЧ1.

1. БЧ1 находит соответствующий расшифрованный голос vote и возвращает его в БЧ2.

БЧ2 учитывает полученный голос.

1. После учета всех голосов в Сервисе взаимодействия БЧ меняется статус голосования. Организатор с использованием АРМ Председателя периодически опрашивает Сервис взаимодействия с БЧ и как только видит изменение статуса, запрашивает итоги голосования. БЧ2 возвращает итоги голосования на АРМ Председателя через Сервис взаимодействия с БЧ.

На рисунке ниже представлен этап подведения итогов.

