СПЕЦИАЛЬНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ПРОГРАММНО-ТЕХНИЧЕСКОГО КОМПЛЕКСА, ОБЕСПЕЧИВАЮЩЕГО ДИСТАНЦИОННОЕ ЭЛЕКТРОННОЕ ГОЛОСОВАНИЕ ИЗБИРАТЕЛЕЙ (УЧАСТНИКОВ РЕФЕРЕНДУМА) ВНЕ ЗАВИСИМОСТИ ОТ МЕСТА ИХ НАХОЖДЕНИЯ

Методические материалы ПТК ДЭГ по работе с компонентом «Центр наблюдения за голосованием»

Листов 61

АННОТАЦИЯ

В документе описаны инструкции по работе с компонентом «Центр наблюдения за голосованием» программного технического комплекса ДЭГ (далее – Портал наблюдения).

Инструкции представлены как для неавторизованных пользователей, так и для пользователей с ролью «Наблюдатель» в системе ДЭГ.

Портал наблюдения размещён в общем доступе по адресу stat.vybory.gov.ru.

СОДЕРЖАНИЕ

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ И ОБОЗНАЧЕНИЙ

Сокращение / обозначение	Полное наименование / описание
БЧ	Блокчейн (англ. blockchain, изначально block chain – цепь из блоков) – выстроенная по определенным правилам непрерывная последовательная цепочка блоков, содержащих записи (транзакции). Используемые при построении цепочки криптографические алгоритмы (хеш-функция и электронная подпись) гарантируют, что ни одна запись из этой цепочки не будет удалена или изменена незаметно. Цепочка из блоков и транзакций хранится на множестве узлов одновременно, что позволяет защититься от потери данных. Узлы, в свою очередь, между собой приходят к соглашению о корректности цепочки по определенному математическому алгоритму, называемому алгоритмом консенсуса.
Гомоморфное шифрование	Способ шифрования данных, позволяющий производить некоторые вычислительные операции над зашифрованными данными так, что результат после расшифрования совпадает с результатом операций над открытыми данными
ДЭГ	Дистанционное электронное голосование
Исходные данные	Совокупность данных, формируемых организующими выборы избирательными комиссиями, включающие в себя: • наименование выборов и уровень их проведения; • систему выборов и количество бюллетеней по каждой избирательной кампании; • территориально-выборное деление на округа и территории, по которым будут устанавливаться итоги; • текст каждого бюллетеня с учетом территориально выборного деления; • время начала и время окончания выдачи бюллетеней; • количество вариантов по каждому бюллетеню; • максимальное количество отметок в бюллетене; • описатель строк протокола; и другие данные, необходимые для запуска смарт-контракта
ПТК ДЭГ	Программно-технический комплекс, обеспечивающий дистанционное электронное голосование избирателей

Сокращение / обозначение	Полное наименование / описание
	(участников референдума) вне зависимости от места их нахождения
Рутокен	Российское средство аутентификации пользователя, который хранит электронную подпись и цифровой сертификат
Смарт-контракт	Алгоритмическая программа, обеспечивающая выполнение определенного набора операций (вызовов программы) и формирование транзакций в сети блокчейн в результате исполнения этих операций
Смарт-контракт голосования	Экземпляр смарт-контракта, создаваемый по команде ТИК ДЭГ для всех выборов, содержащихся в исходных данных, для каждой территории и избирательного округа.
ТИК ДЭГ	Территориальная избирательная комиссия дистанционного электронного голосования
Транзакция	Набор зашифрованных данных, подписанных электронной подписью создателя транзакции и записанный в один из блоков в цепочке блоков распределенной базы данных (блокчейн). Подпись транзакции обеспечивает неизменность ее данных, а запись транзакций в блоки обеспечивает неизменность всех данных в распределенной базе данных (транзакции не могут быть изменены, исключены или добавлены из блока)
GitHub	Веб-сервис для хостинга IT-проектов и их совместной разработки, ресурс, на котором хранится исходный код
zkp	zero knowledge proof –доказательство с нулевым разглашением

1. НАЗНАЧЕНИЕ ПРОГРАММЫ

Портал наблюдения является частью программно-технического комплекса ДЭГ и предназначен для наблюдения за подготовкой, проведением ДЭГ и установлением его итогов. Указанный ресурс размещён в открытом доступе в сети Интернет stat.vybory.gov.ru и содержит две зоны:

- неавторизованную;
- авторизованную;

Доступ к неавторизованной зоне имеют все пользователи сети Интернет, желающие отслеживать процесс ДЭГ в режиме реального времени, и ознакомиться с результатами ДЭГ после установления его итогов и подписания протокола ТИК ДЭГ.

В неавторизованной зоне пользователям предоставляется возможность отслеживать соблюдение следующих показателей по каждому голосованию (в том числе в разрезе избирательных участков):

- количество участников ДЭГ не увеличивается за весь период голосования;
- количество выданных бюллетеней (предоставленных доступов к бюллетеню) не превышает количество участников ДЭГ;
- число принятых бюллетеней не превышает количество выданных бюллетеней.

! *Необходимо принять во внимание, что избирателям, которые участвуют в нескольких голосованиях, система ДЭГ выдает несколько бюллетеней, однако избиратель вправе проголосовать не по всем полученным бюллетеням. В связи с этим общее количество выданных бюллетеней может отличаться от количества принятых.*

Также, в неавторизованной зоне доступны:

- почасовой график выдачи и получения бюллетеней;
- сведения о формировании цепочек блоков информации в БЧ;
- сведения о транзакциях в БЧ (перечень транзакций указан в Приложении 2), в том числе просмотр их содержимого;
- возможность проверить учёт своего голоса по идентификатору транзакции, который отображается после успешного волеизъявления;
- просмотр протокола об итогах ТИК ДЭГ, после его подписания и публикации.

Доступ к авторизованной зоне имеют наблюдатели, для которых был указан СНИЛС при подаче списков наблюдателей в ТИК ДЭГ. В авторизованной зоне доступны те же возможности, что и для неавторизованных пользователей, а также файловые выгрузки транзакций БЧ (для избирательных кампаний, в рамках которых пользователь назначен наблюдателем) и дополнительные инструменты наблюдения,

техническая документация, полезные ссылки, исходные коды программ, инструкции по работе с инструментами наблюдения.

2. ОПИСАНИЕ ПРОЦЕССОВ ДЭГ

2.1.Действия ТИК ДЭГ при подготовке, проведении и установлении итогов ДЭГ

При проведении ДЭГ в ТИК ДЭГ выполняются следующие действия:

- получение из ГАС «Выборы» исходных данных (состав указан в Приложении 1), сформированных избирательными комиссиями, на которые возложены полномочия по организации выборов;
- получение данных заявлений избирателей для участия в ДЭГ;
- загрузка исходных данных и данных заявлений в ПТК ДЭГ для формирования списков участников ДЭГ отдельно по каждому избирательному округу (соответствующей территории);
- создание голосований в сети БЧ на основании данных смарт-контрактов;
- загрузка списков участников ДЭГ в каждый экземпляр смарт-контракта;
- генерация ключей шифрования и расшифрования, и разделение ключа расшифрования на части (выполняется с использованием отдельного программного обеспечения);
- загрузка ключа шифрования в ПТК ДЭГ;
- отправка команды начала выдачи бюллетеней;
- исключение избирателей из списков участников ДЭГ до окончания времени голосования на основании информации, поступившей из организующих выборы избирательных комиссий;
- отправка команды остановки выдачи бюллетеней;
- отправка команды о завершении приема голосов;
- выгрузка списка участников ДЭГ;
- сборка ключа расшифрования (выполняется с использованием отдельного программного обеспечения);
- загрузка ключа расшифрования в ПТК ДЭГ;
- получение итогов ДЭГ;
- формирование протокола об итогах ДЭГ и его подписание;
- передачу данных об итогах ДЭГ в ГАС «Выборы» для подведения итогов выборов организующими избирательными комиссиями.

Действия избирательной ТИК ДЭГ, выполняемые с использованием автоматизированного рабочего места ТИК ДЭГ, отображаются на Портале наблюдения в виде соответствующих транзакций (указано в Приложении 2).

2.2.Подготовка БЧ к проведению ДЭГ

В ходе подготовки системы ДЭГ к проведению голосования создаются чистые блокчейн-сети, которые не содержат данные и не относятся к проводимым голосованиям. В каждой сети записана информация об определенном количестве голосований. Каждое голосование представлено своим смарт-контрактом. Общее количество смарт-контрактов соответствует количеству проводимых голосований на всех уровнях (в ЕДГ-2022 региональном и муниципальном).

3. НЕАВТОРИЗОВАННАЯ ЗОНА ПОРТАЛА НАБЛЮДЕНИЯ

3.1.Доступ к Порталу наблюдения

Для того чтобы открыть Портал наблюдения необходимо указать ссылку stat.vybory.gov.ru в браузере, установленном на устройстве.

! *Для работы с Порталом наблюдения понадобится персональный компьютер или ноутбук, подключенный к Интернету с установленным браузером. Также возможно использовать планшет или смартфон. Рекомендуемые браузеры: «Спутник», Google Chrome, Яндекс.Браузер.*

При переходе пользователю отобразится главная страница Портала наблюдения (рис.1).

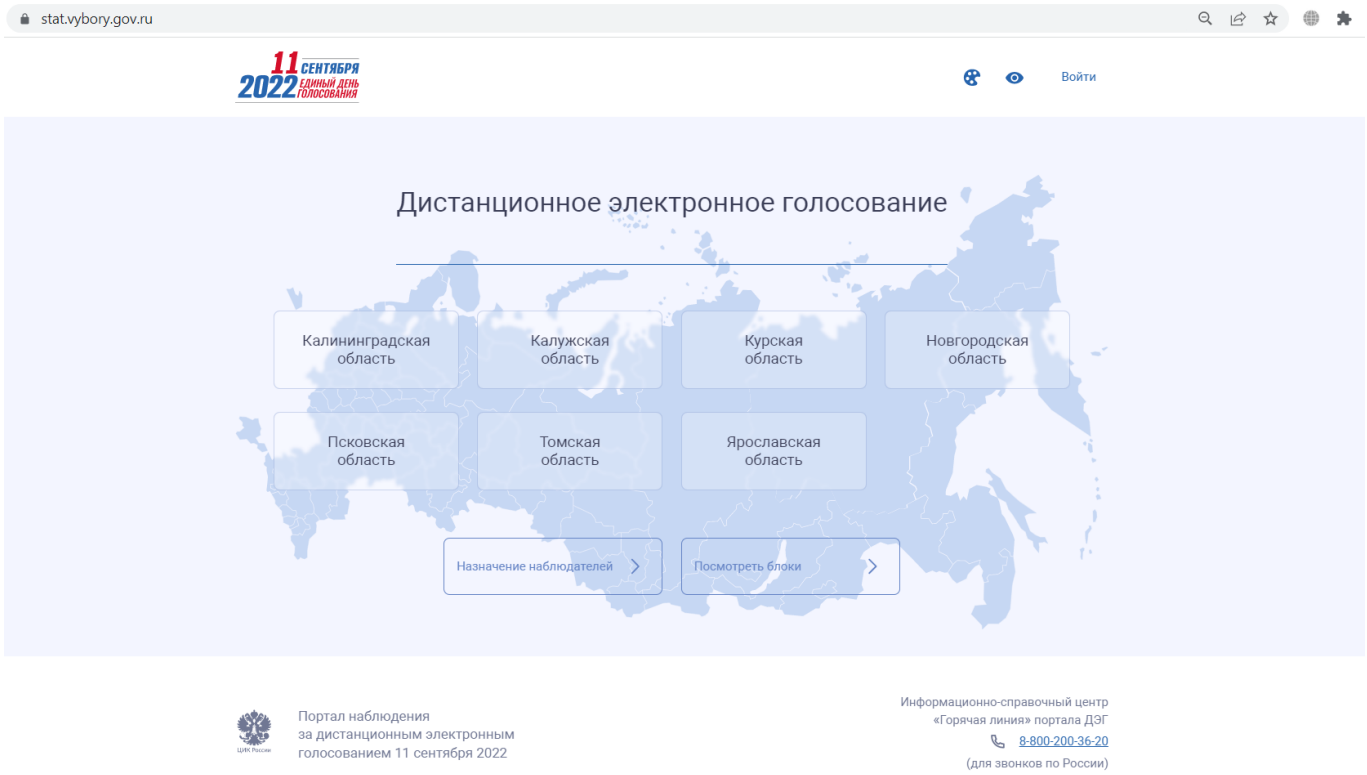

Рисунок 1 – Главная страница Портала наблюдения

3.2.Дополнительные возможности Портала наблюдения

На всех страницах Портала наблюдения присутствуют сквозные элементы в верхней и нижней частях страницы.

Функциональность, доступная из верхней части страницы:

- По нажатию на логотип единого дня голосования в левом верхнем углу страницы осуществляется переход к главной странице Портала наблюдения.
- По нажатию на пиктограмму происходит переключение светлой и темной темы Портала наблюдения;

- По нажатию на пиктограмму  открывается панель для настройки размера текста и цветового решения на страницах Портала наблюдения, а также переключение на версию для слабовидящих;
- По нажатию на кнопку «Войти» реализуется переход на страницу авторизации.

Функциональность, доступная из нижней части страницы:

- По нажатию на ссылку информационно-справочного центра «Горячая линия» портала ДЭГ браузер запрашивает разрешение на совершение звонка (в случае работы с порталом Наблюдения с мобильного телефона).

3.3. Структура главной страницы Портала наблюдения

Пользователю, вошедшему на Портал наблюдения, на главной странице отображаются:

- Перечень субъектов РФ, в которых проводится ДЭГ. По нажатию на выбранный субъект осуществляется переход к списку голосований в этом субъекте.
- «Назначение наблюдателей» – функциональность назначения наблюдателей на портале наблюдения доступна для зарегистрированных кандидатов, выдвинутых в порядке самовыдвижения. По нажатию на кнопку осуществляется переход на страницу авторизации Госуслуг. При подтверждении системы, что авторизованный пользователь является кандидатом, отобразится функциональность назначения наблюдателей.
- «Посмотреть блоки» – при переходе по кнопке отображается страница, содержащая сведения о формировании цепочек блоков информации в БЧ. Для поиска конкретного блока пользователь может воспользоваться выбором сети в поле «Выбрать сеть» и указать значение в поле «Высота блока». Для просмотра результатов поиска необходимо нажать на пиктограмму  или на клавишу Enter на клавиатуре. Для возврата к полному списку блоков необходимо удалить значение в поисковой строке и нажать на пиктограмму  или на клавишу Enter на клавиатуре (рис.2).

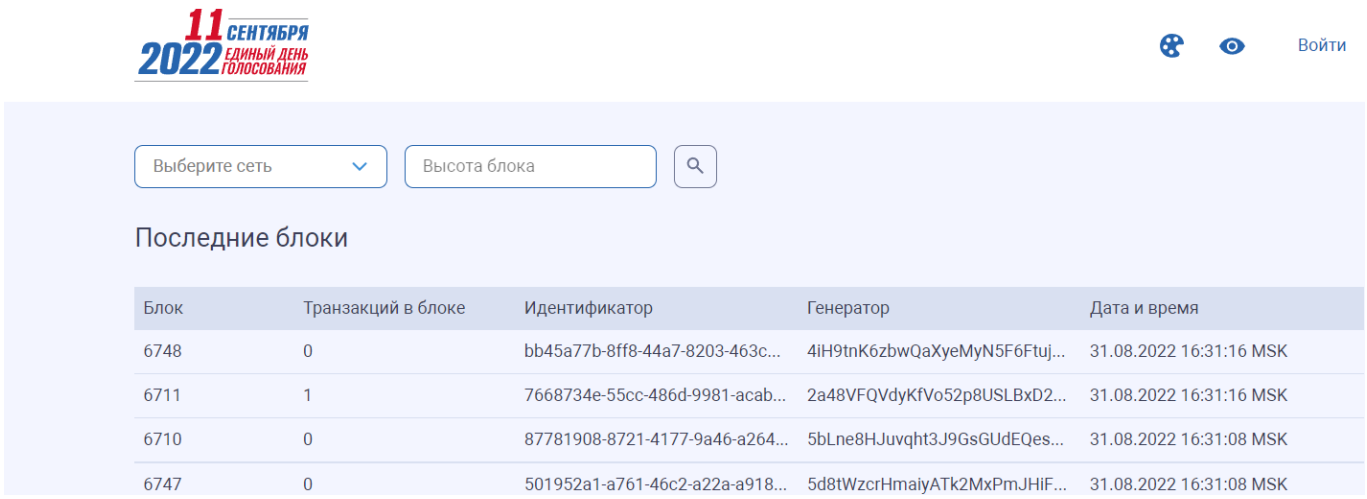

Рисунок 2 – Отображение страницы просмотра блоков

3.3.1. Перечень субъектов РФ, где проводится ДЭГ

На главной странице Портала наблюдения отображены все субъекты, где проводится ДЭГ на федеральной платформе (система ДЭГ ЦИК России).

По нажатию кнопки с наименованием субъекта РФ осуществляется переход к списку избирательных кампаний, проходящих в регионе, с разбивкой по уровням выборов (рис.3).

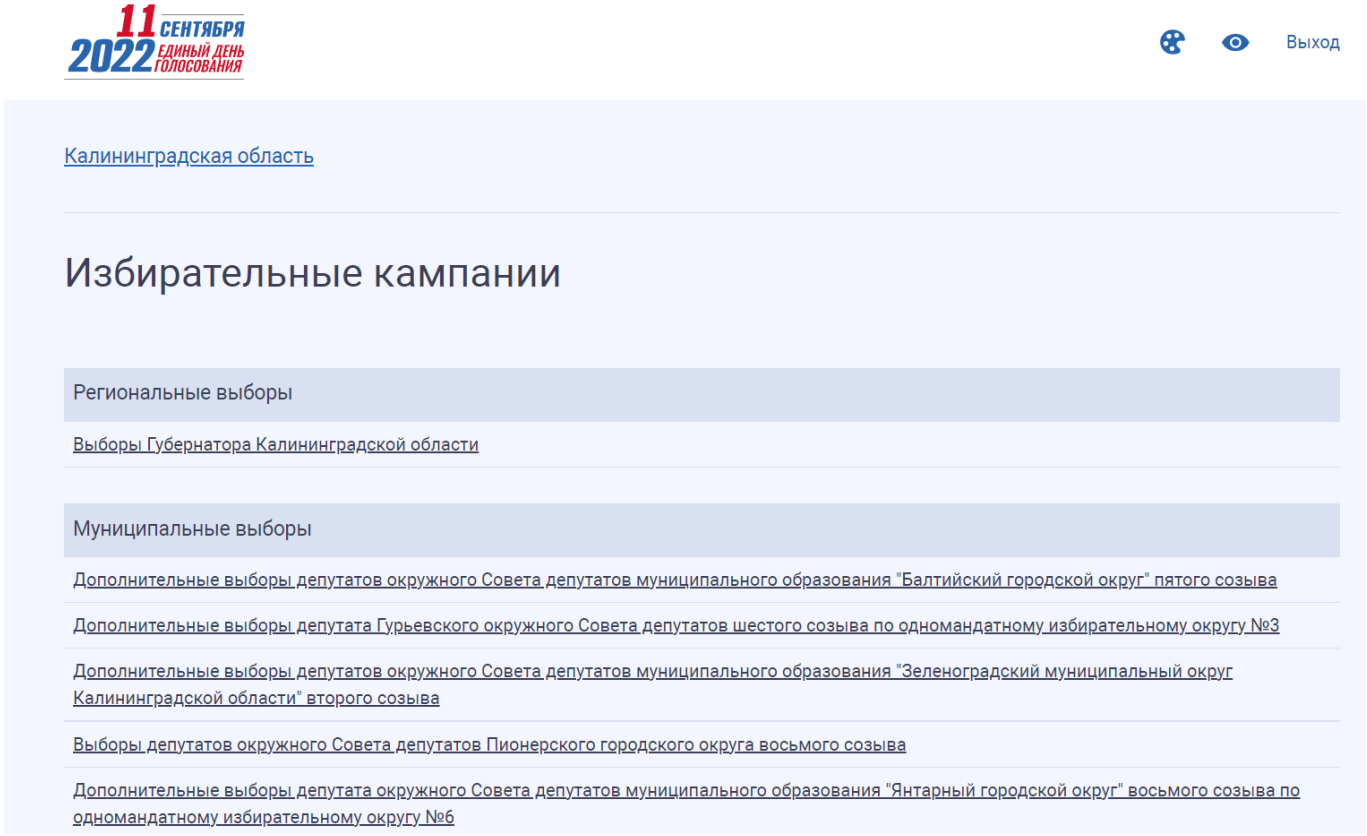

Рисунок 3 – Отображение списка избирательных кампаний в выбранном субъекте

Для перехода на детальную страницу выборов необходимо нажать на их наименование. Для возврата к списку субъектов РФ нужно нажать на логотип

выборов в левой части страницы или воспользоваться стандартной кнопкой браузера «Назад».

3.4.Просмотр статистической информации

3.4.1. Общая статистическая информация

При переходе на детальную страницу избирательной кампании пользователю в верхней части страницы доступен просмотр статистической информации в текстовом и графическом представлении по:

- Общему количеству бюллетеней, которое соответствует числу участников ДЭГ;
- Общему количеству выданных бюллетеней;
- Общему количеству принятых бюллетеней.

Если выборы проводятся по смешанной системе, отображаются сводные данные по единому пропорциональному округу и по одномандатным (многомандатным) округам. Количество участников ДЭГ в статистических данных может отличаться, если в списке участников есть избиратели, голосующие только по единому пропорциональному округу (рис.4).

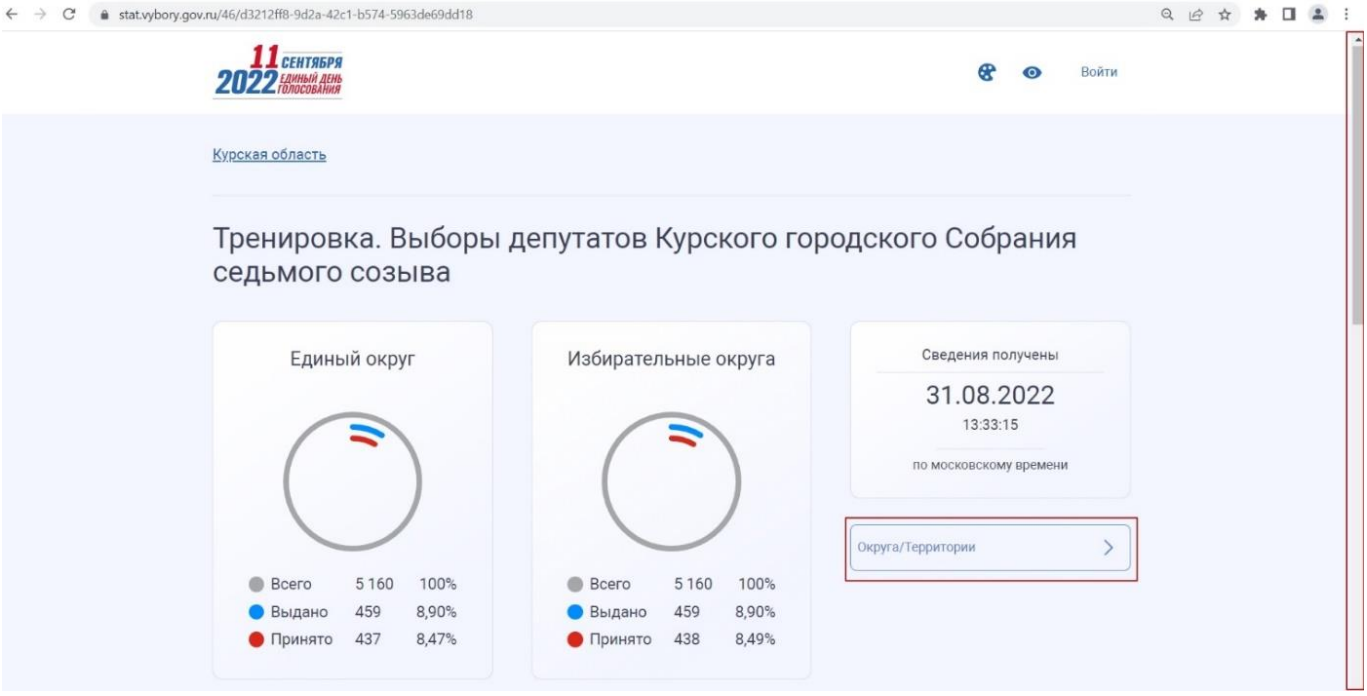

Рисунок 4 – Отображение общей статистической информации по выбранному из списка голосованию (смешанная система)

Если выборы проходят по мажоритарной системе, отображается статистика только по единому округу (рис. 5).

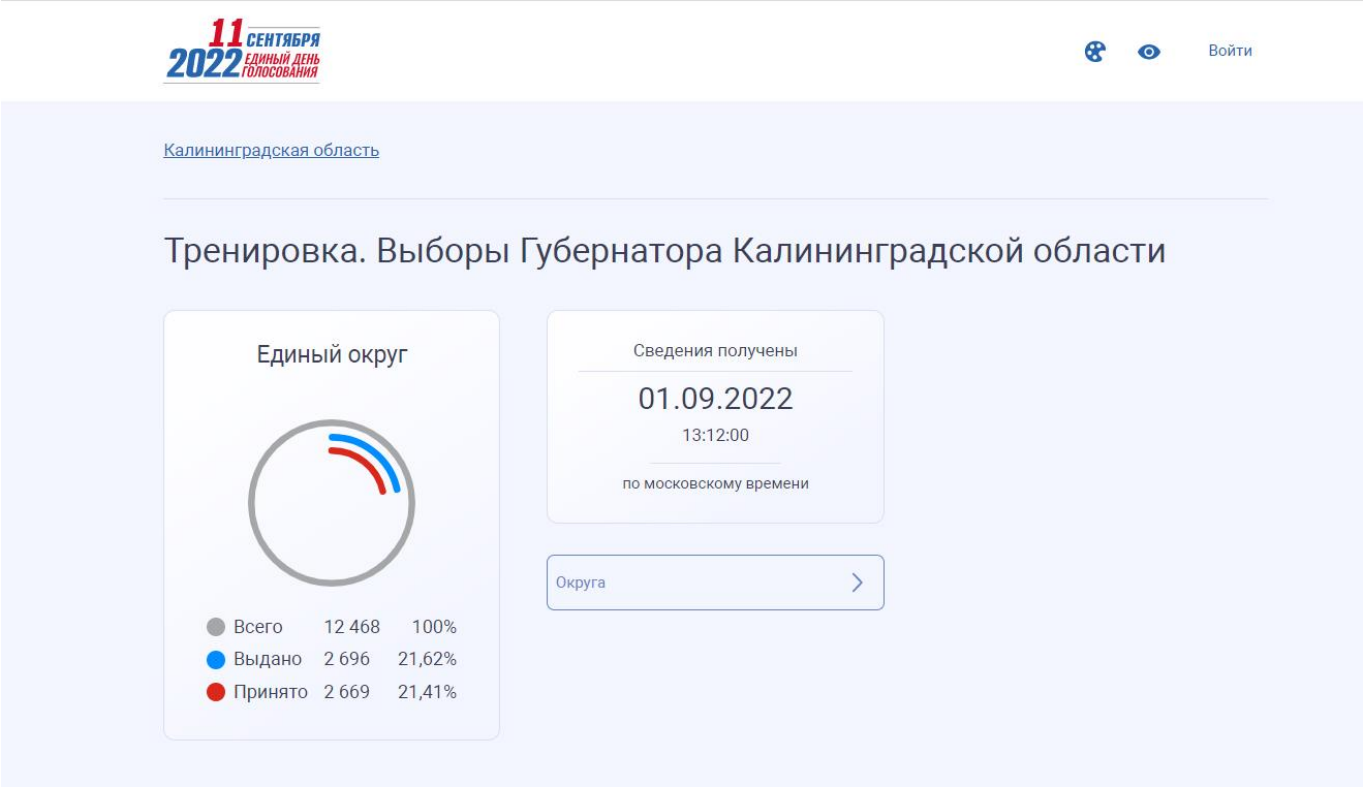

Рисунок 5 – Отображение общей статистической информации по выбранному из списка голосованию (мажоритарная система)

3.4.2. Работа с голосованиями

Для перехода к детальным сведениям по голосованиям на каждой территории или в избирательном округе, необходимо на экране избирательной кампании нажать на кнопку «Округа/Территории» или перейти ниже по странице при помощи полосы прокрутки (рис.4) и выбрать необходимый избирательный округ или территорию (рис. 6)

Рисунок 6 – Отображение списка округов

В верхней части страницы отобразится статистическая информация с данными округа в текстовом и графическом представлении по:

- Общему количеству бюллетеней, которое соответствует числу участников ДЭГ;
- Общему количеству выданных бюллетеней;
- Общему количеству принятых бюллетеней.

Если территориально-выборное деление по единому округу совпадает с границами одномандатных (многомандатных) округов, отображается две карточки округов со статистикой по территории единого округа и одномандатного (многомандатного) округа (рис.7)

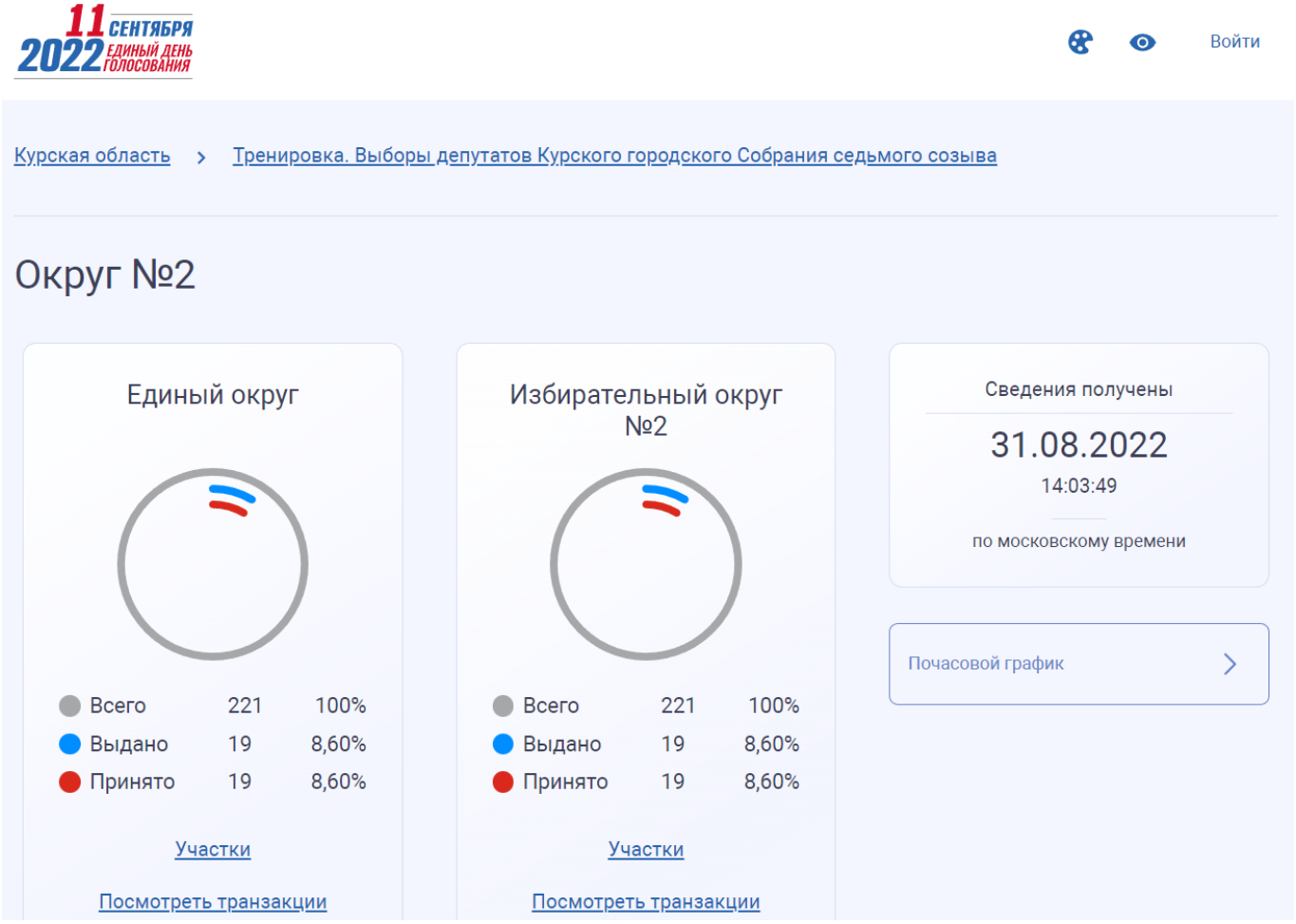

Рисунок 7 – Отображение детальной страницы со статистикой по округу

Если территориально-выборное деление по единому округу не совпадает с границами одномандатных (многомандатных) округов, на детальной странице округа отображаются статистические данные только по округу (рис. 8).

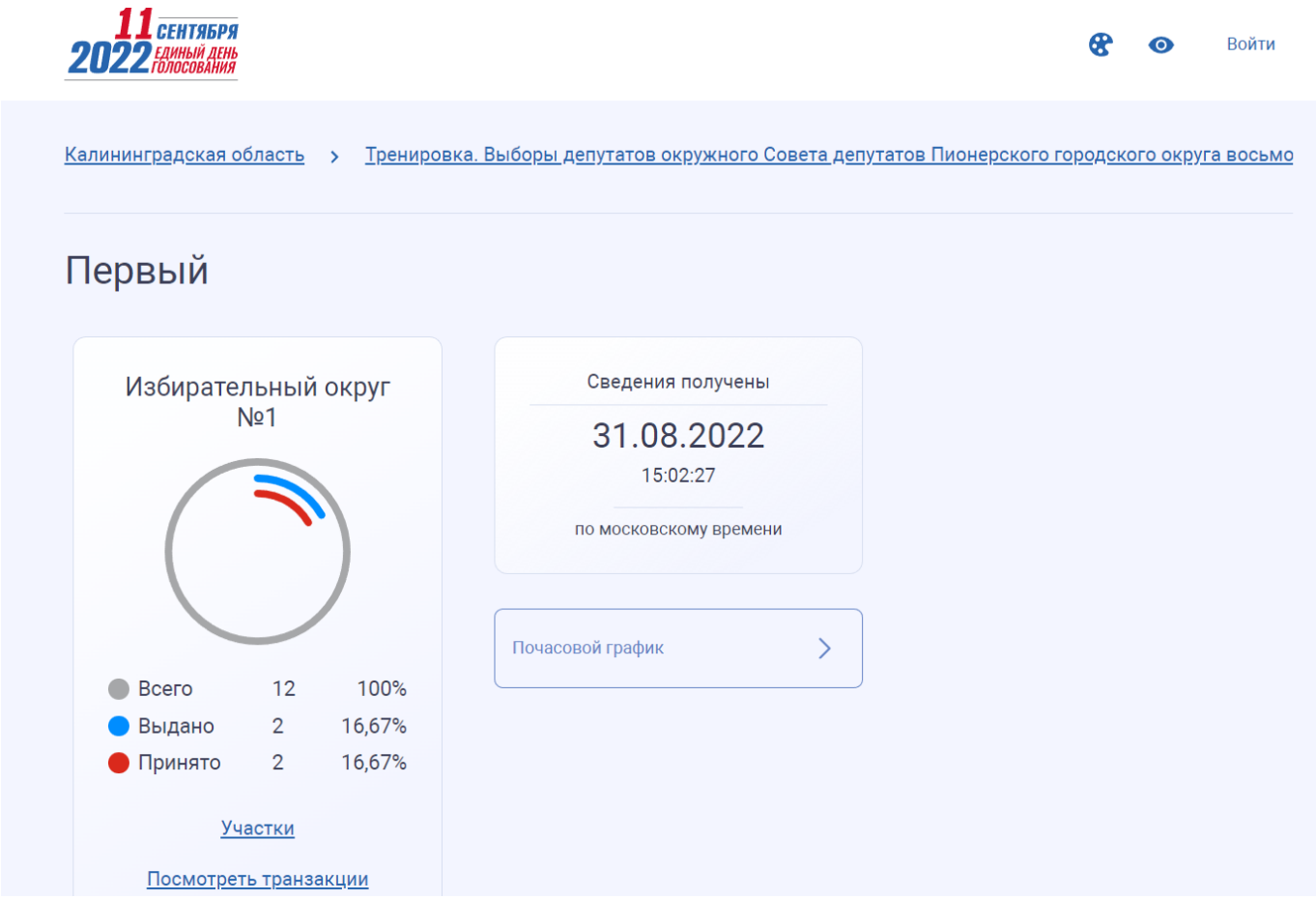

Рисунок 8 – Отображение данных при не совпадающем территориально-выборном делении

Из карточки округа/территории доступен переход по ссылкам:

- «Участки» – на страницу для просмотра статистической информации по количеству участников ДЭГ и выдаче бюллетеней в разрезе избирательных участков.
- «Посмотреть транзакции» – на страницу для просмотра транзакций по округу (голосованию), зафиксированных в БЧ, с момента загрузки исходных данных в БЧ до получения итогов ДЭГ.

3.4.3. Работа с почасовым графиком

Для просмотра почасового графика хода голосования необходимо нажать на кнопку «Почасовой график» или перейти ниже по странице при помощи полосы прокрутки (рис.9).

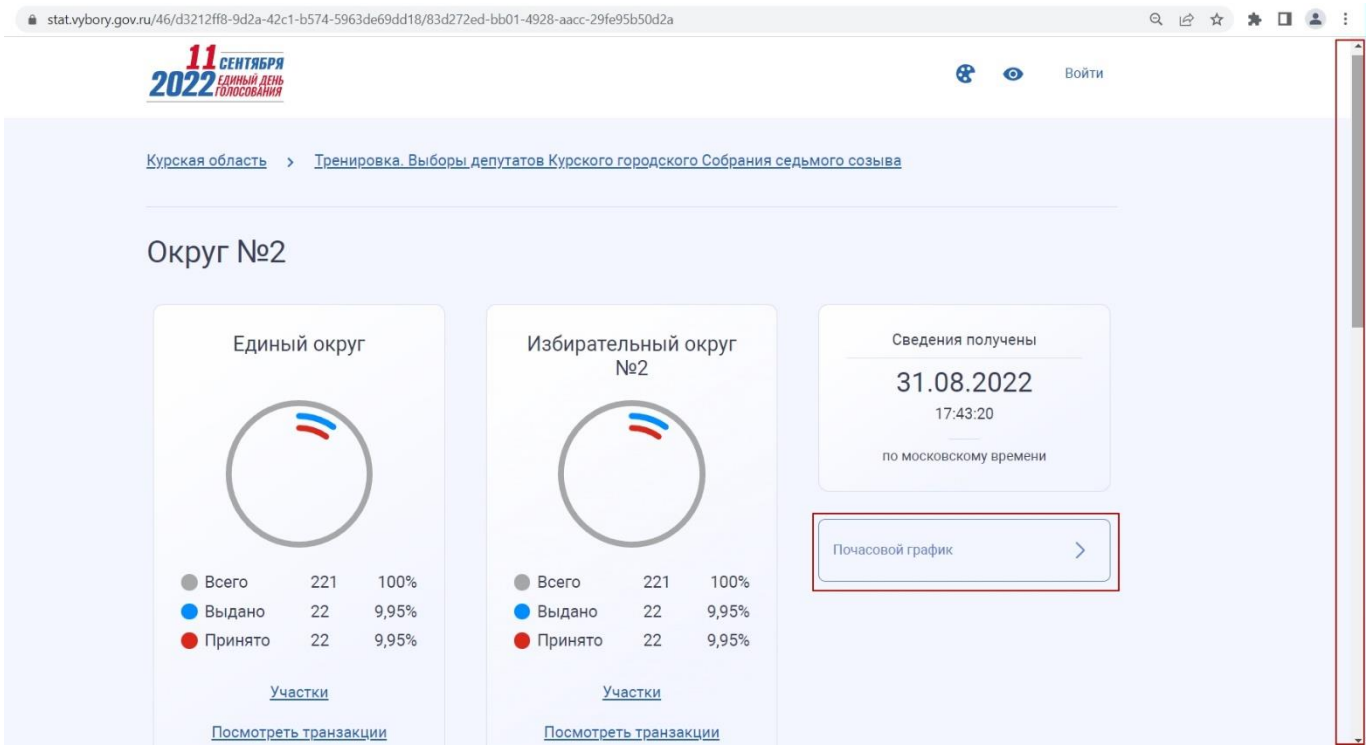

Рисунок 9 – Переход к отображению почасового графика хода голосования

Просмотр почасового графика доступен на странице со статистической информацией по округу и содержит сведения по количеству выданных бюллетеней и полученных голосов за каждый час с момента запуска голосования.

При голосовании по смешанной системе и совпадении выборно-территориального деления территории единого округа с границами одномандатных (многомандатных) округов отображаются показатели по территории единого округа и избирательному округу с возможностью отключения одного из них (рис.10).

При голосовании по мажоритарной системе или несовпадении выборно-территориального деления территории единого округа с границами одномандатных (многомандатных) округов отображается показатель только по избирательному округу (рис.11).

По нажатию на флажок рядом с округом производится отключение отображения показателя.

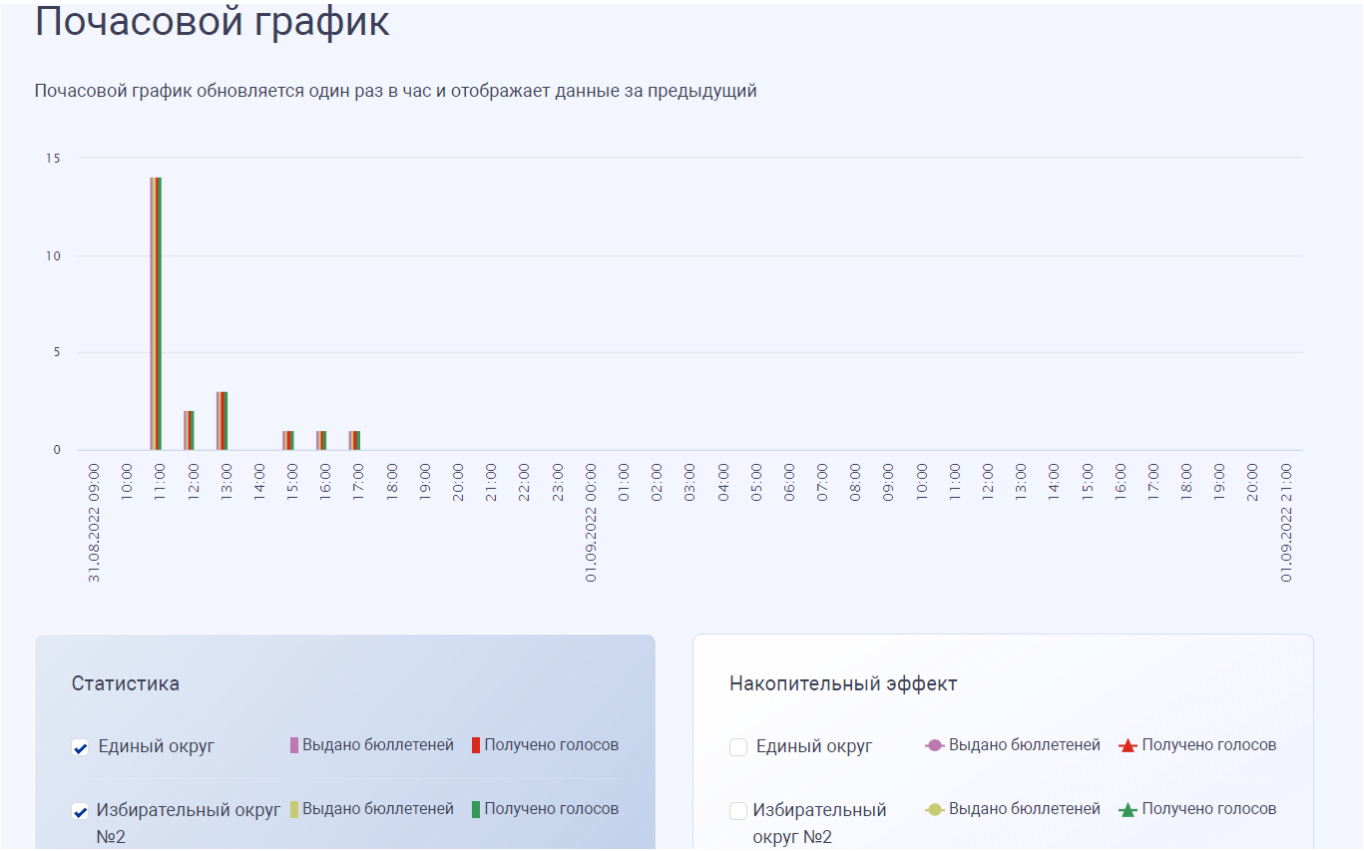

Рисунок 10 – Отображение статистики на почасовом графике по смешанной системе и совпадению выборно-территориального деления единого округа с границами одномандатных (многомандатных) округов

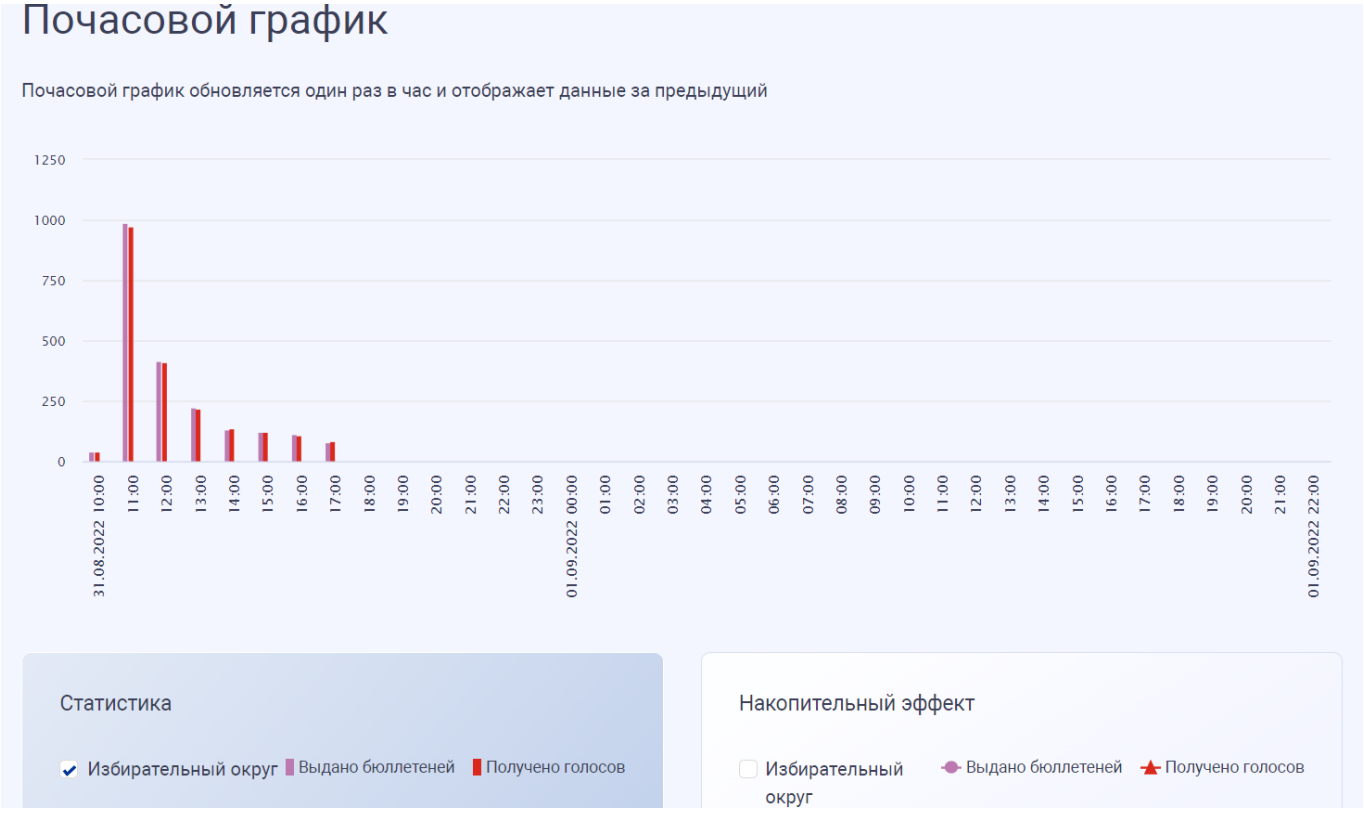

Рисунок 11 – Отображение статистики на почасовом графике по мажоритарной системе

Для пользователя доступно переключение на линейный тип графика, в блоке «Накопительный эффект». На графике с накопительным эффектом отображается общее количество выданных бюллетеней и полученных голосов в почасовом срезе.

При голосовании по смешанной системе и совпадении выборно-территориального деления территории единого округа с границами одномандатных (многомандатных) округов отображаются показатели по территории единого округа и избирательному округу с возможность отключения одного из них (рис.12).

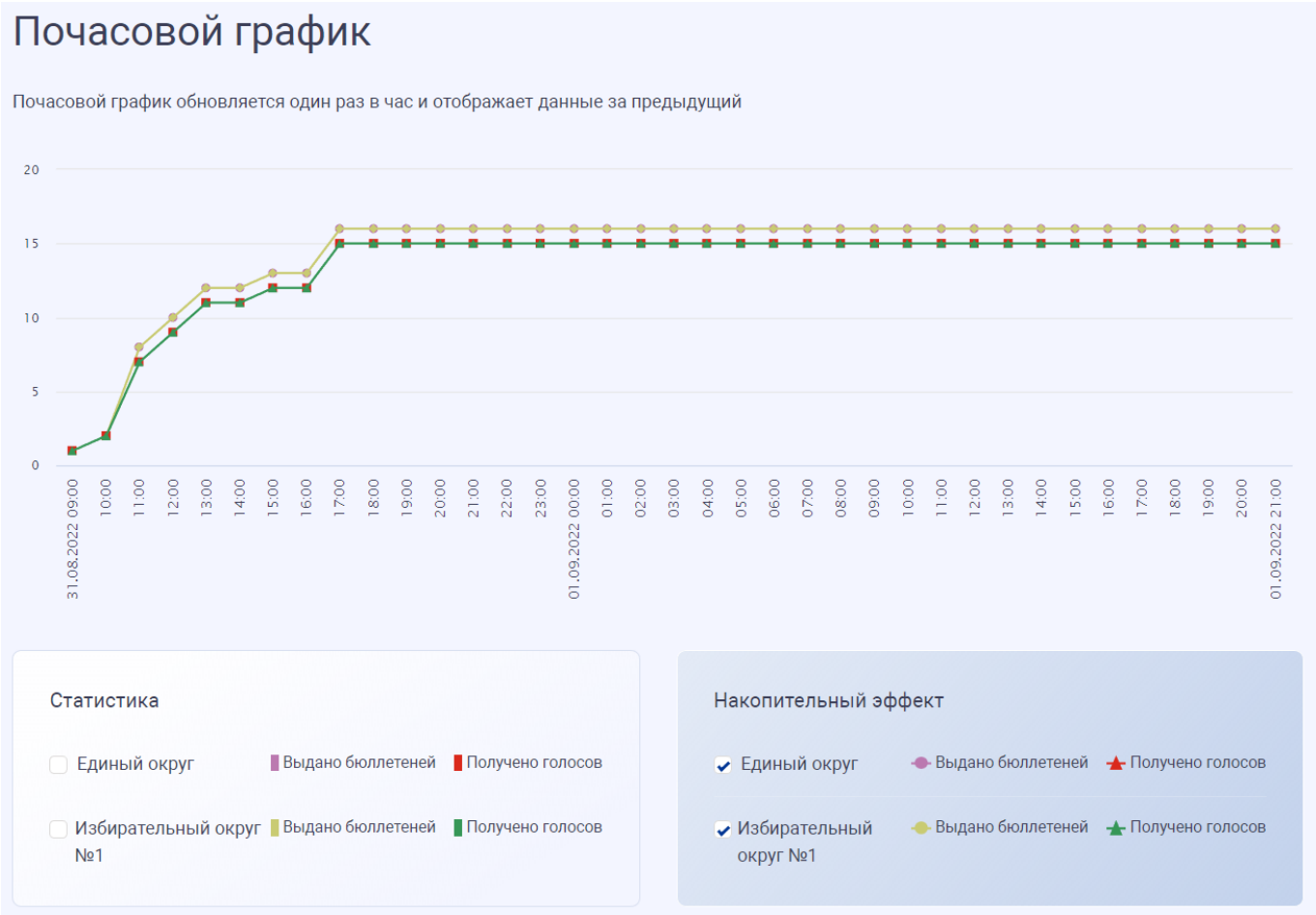

Рисунок 12 – Отображение накопительного эффекта на почасовом графике по смешанной системе

При голосовании по мажоритарной системе или несовпадении выборно-территориального деления территории единого округа с границами одномандатных (многомандатных) округов отображается показатель только по избирательному округу (рис.13).

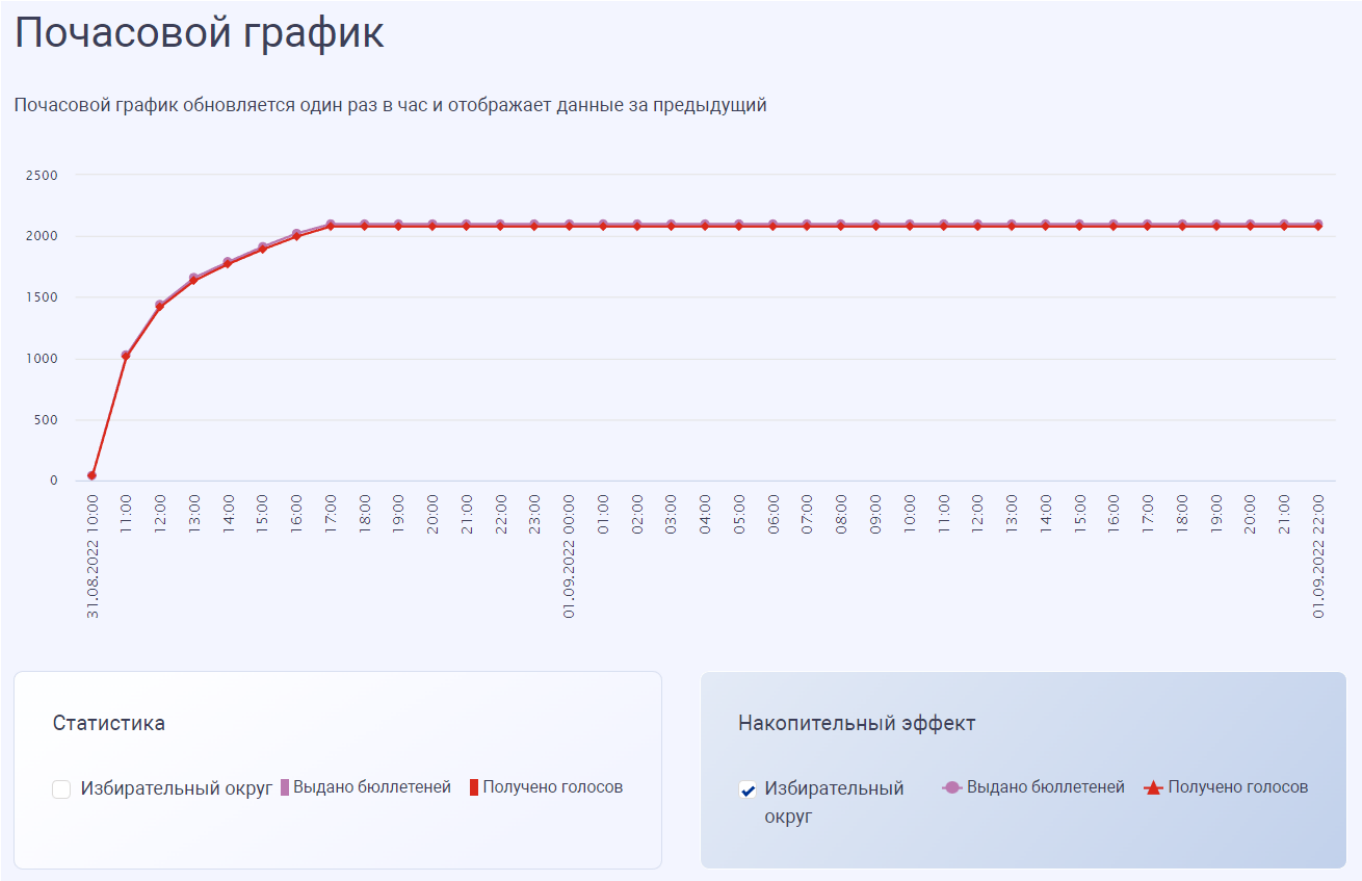

Рисунок 13 – Отображение накопительного эффекта на почасовом графике по мажоритарной системе

При наведении на шкалу графика отображается всплывающая подсказка с информацией о времени, типе шкалы и количественном показателе.

Обновление почасового графика производится раз в час, данные отображаются за прошедший час.

3.4.4. Страница со статистикой в разрезе избирательных участков

При переходе со страницы сведений по округу на страницу «Участки» отображается статистическая информация по количеству участников ДЭГ и выданным бюллетеням в разрезе участков.

В таблице отображены данные по:

- «Номер участка» – номер участка, соответствующий избирательному участку в ГАС «Выборы».
- «Всего участников» – количество участников ДЭГ по избирательному участку.
- «Приняли участие» – количество участников ДЭГ по избирательному участку, получивших бюллетени в процессе ДЭГ.

- «Явка» – относительный показатель, который показывает соотношение количества всех участников ДЭГ по избирательному участку к количеству получивших бюллетени в процессе ДЭГ.

При необходимости поиска данных по номеру участка, пользователю доступна поисковая строка.

Для просмотра результатов поиска нужно ввести номер участка и нажать на пиктограмму или на клавишу Enter на клавиатуре. Для возврата к списку участков по умолчанию необходимо удалить значение в поисковой строке и нажать на пиктограмму или на клавишу Enter на клавиатуре (рис.14).

Сортировка списка на странице «Участки» осуществляется по столбцу «Приняли участие» в порядке убывания.

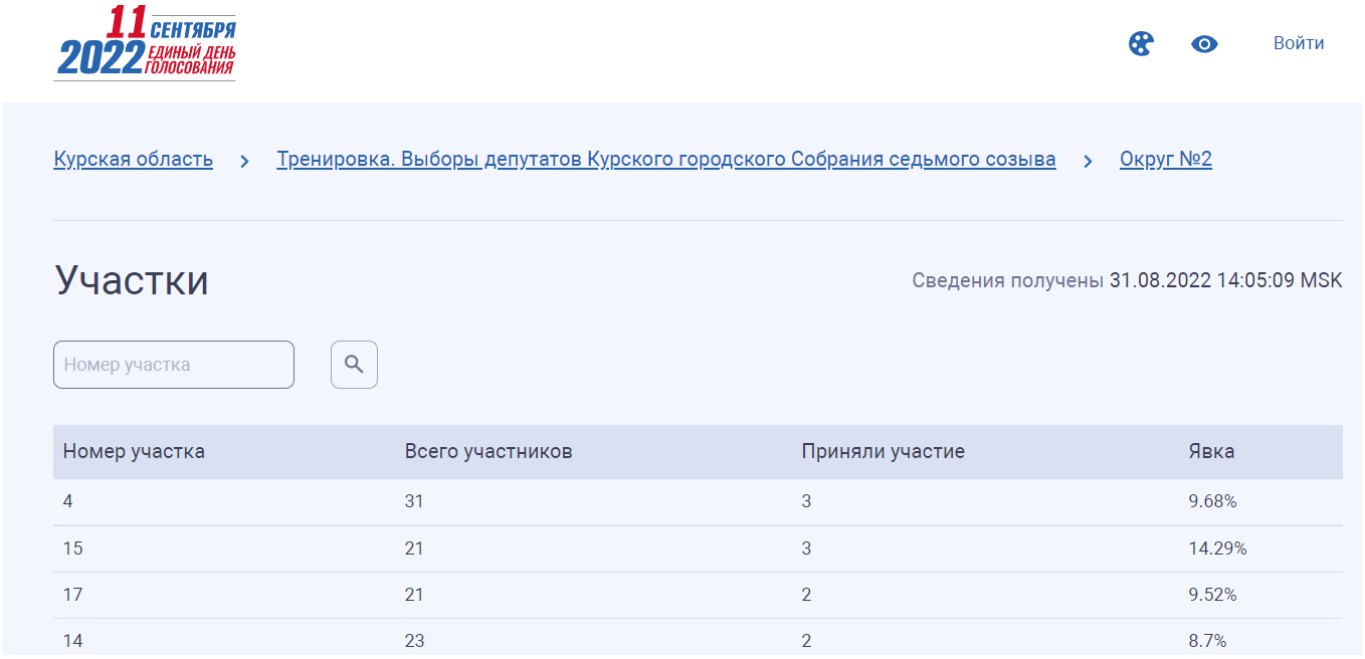

Рисунок 14 – Отображение страницы со списком участков

3.4.5. Страница просмотра транзакций БЧ по округу (голосованию)

По нажатию на кнопку «Посмотреть транзакции» отображаются транзакции БЧ по голосованию в конкретном округе.

Страница отображает (рис.15):

1) Идентификатор контракта голосования;
2) Блок поиска и фильтрации для нахождения одной или группы транзакций:

   Для поиска группы транзакций по:

   - отрезку времени необходимо задать диапазон начала и/или окончания. После выбора даты поле с выбором времени становится активным;
   - типу транзакций нужно выбрать из выпадающего списка значение.

При наличии идентификатора транзакции пользователь может ввести его значение в поле «Введите идентификатор транзакции» для поиска конкретной записи.

Для просмотра результатов поиска нужно воспользоваться поиском и фильтрацией и нажать на пиктограмму или на клавишу Enter на клавиатуре. Для возврата к списку участков по умолчанию необходимо нажать на кнопку «Сбросить все фильтры».

3) Список транзакций с указанием даты и времени транзакции, ее идентификатора и типа, к которому относится транзакция.

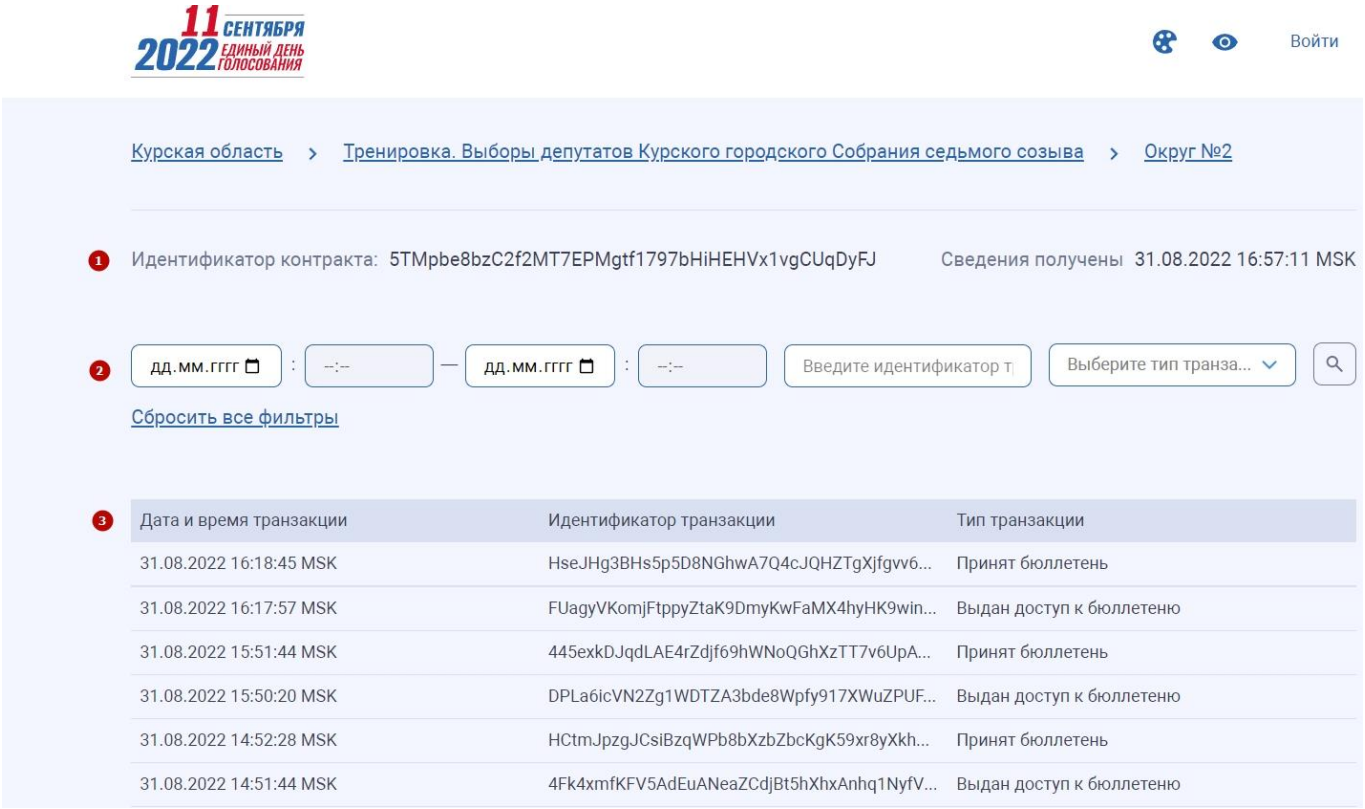

Рисунок 15 – Страница с транзакциями конкретного голосования

По нажатию на транзакцию в списке осуществляется переход на страницу с детальной информацией о ней (рис.16).

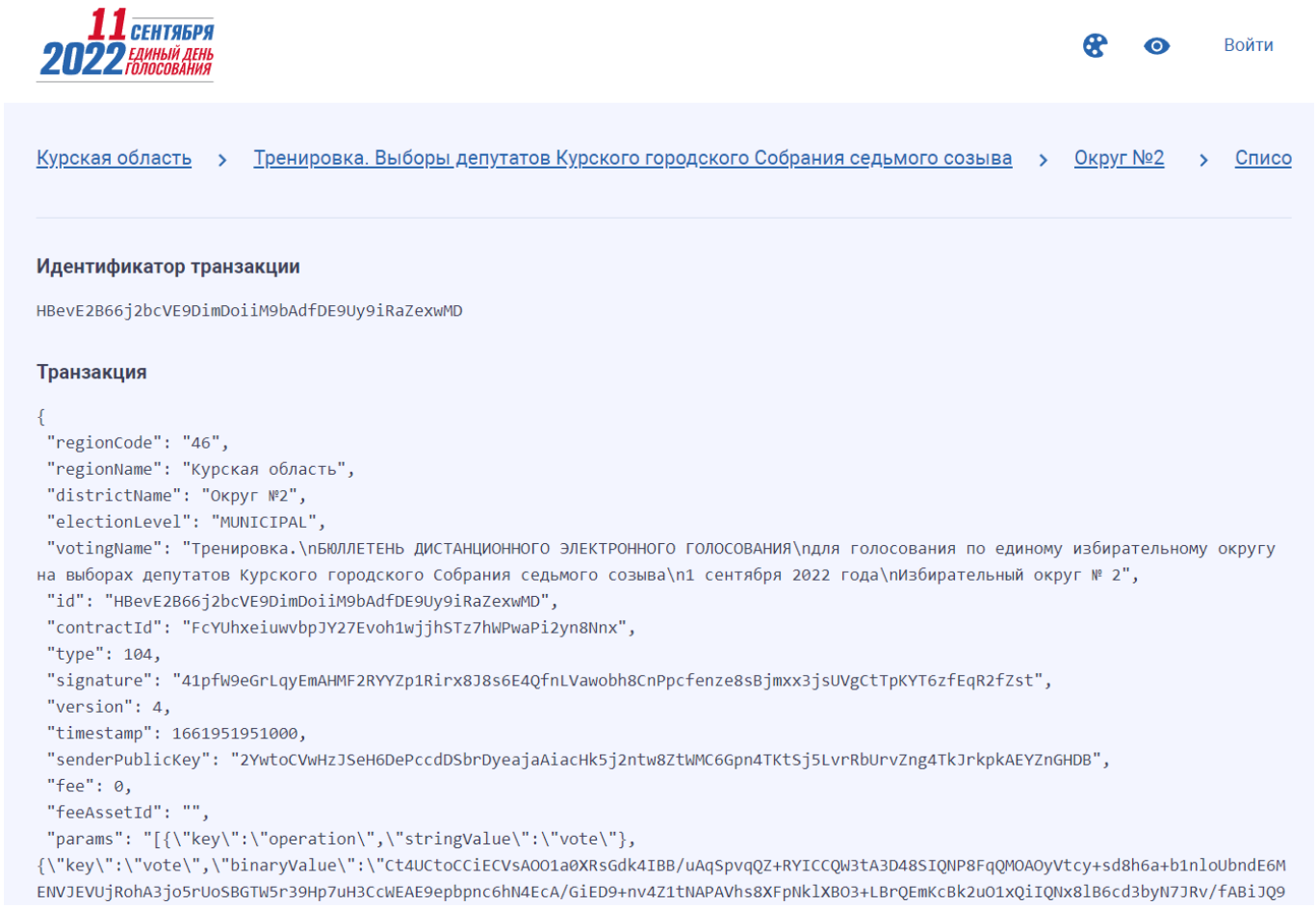

Рисунок 16 - Детальная страница транзакции

Для возврата на предыдущие страницы необходимо воспользоваться цепочкой навигации, расположенной в верхней части экрана.

3.4.5.1. Проверка учёта своего голоса

После осуществления голосования в анонимной зоне портала ДЭГ по каждому бюллетеню на экране «Вы проголосовали» отображается информация о транзакции, содержащей голос в зашифрованном виде, для ее просмотра необходимо нажать на кнопку «Информация о транзакции» (рис.17).

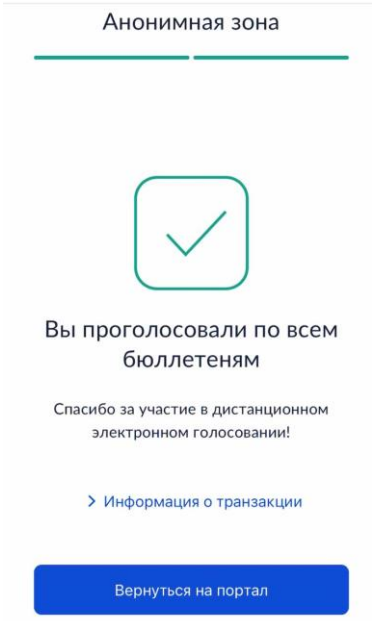

Рисунок 17 – Экран мобильного приложения после осуществления голосования в анонимной зоне портала ДЭГ. Отображение информации о транзакции, содержащей голос в зашифрованном виде

При сохранении идентификатора транзакции доступна проверка учёта своего голоса на Портале наблюдения. Для сохранения идентификатора необходимо скопировать значение из раздела «Идентификатор транзакции» (рис.18).

! *Информация о транзакции отображается только один раз, сразу после осуществления голосования по бюллетеню. При переходе к следующему бюллетеню или выходе из анонимной зоны получить доступ к сведениям повторно будет невозможно.*

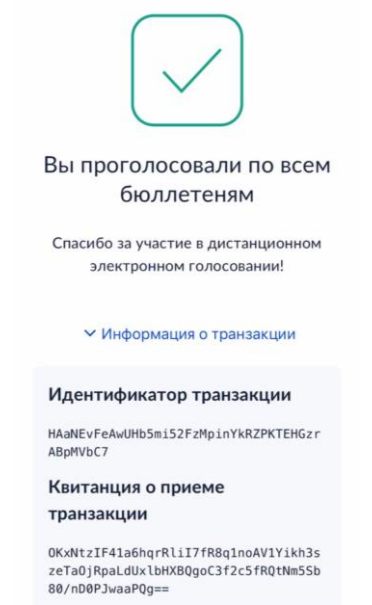

Рисунок 18 – Экран мобильного приложения после осуществления голосования в анонимной зоне портала ДЭГ. Отображение идентификатора транзакции и квитанции о приёме голоса

Для поиска транзакции требуется:

1) Перейти на страницу на страницу избирательной кампании, по которой осуществлялось голосование;
2) Выбрать округ/территорию, по бюллетеню которого произвелось волеизъявление;
3) В карточке округа нажать на кнопку «Посмотреть транзакции».
4) Вести идентификатор своей транзакции в поле «Идентификатор транзакции» и нажать на пиктограмму или на клавишу Enter на клавиатуре (рис.19).

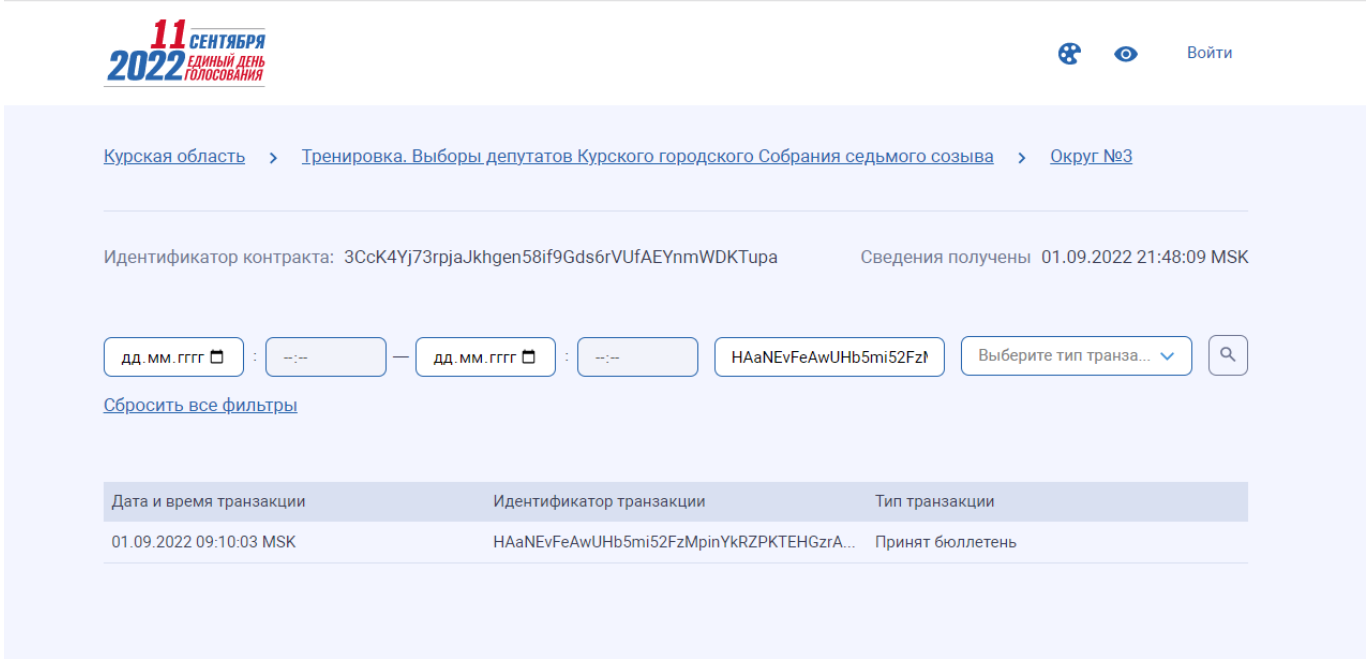

Рисунок 19 – Экран поиска транзакции по идентификатору на портале наблюдения

На экране отобразится результат поиска. Наименование операции «Принят бюллетень» означает, что эта транзакция содержит в себе зашифрованный результат волеизъявления, а само наличие транзакции на портале наблюдения – факт ее записи в систему.

4. АВТОРИЗОВАННАЯ ЗОНА ПОРТАЛА НАБЛЮДЕНИЯ

4.1. Авторизация

Для того чтобы открыть Портал наблюдения пользователю с ролью «Наблюдатель», необходимо выполнить действия, указанные в пункте «Доступ к Порталу наблюдения», после чего нажать на кнопку «Войти» в верхней панели меню для авторизации.

Для входа требуется ввести данные учетной записи Госуслуг.

Авторизация на Портале наблюдения будет успешной в случае:

- Подачи списков наблюдателей с указанием СНИЛС в ТИК ДЭГ;
- Корректно указанного СНИЛС при внесении данных наблюдателя;
- Наличия подтверждённой учетной записи на Госуслугах;
- Исполнения 18 лет на день голосования (11 сентября 2022 года);
- Верно введенных наблюдателем данных учетной записи Госуслуг при входе в авторизованную зону Портала наблюдения.

В случае успешной авторизации вместо кнопки «Войти» отобразится фамилия и инициалы пользователя (рис.20).

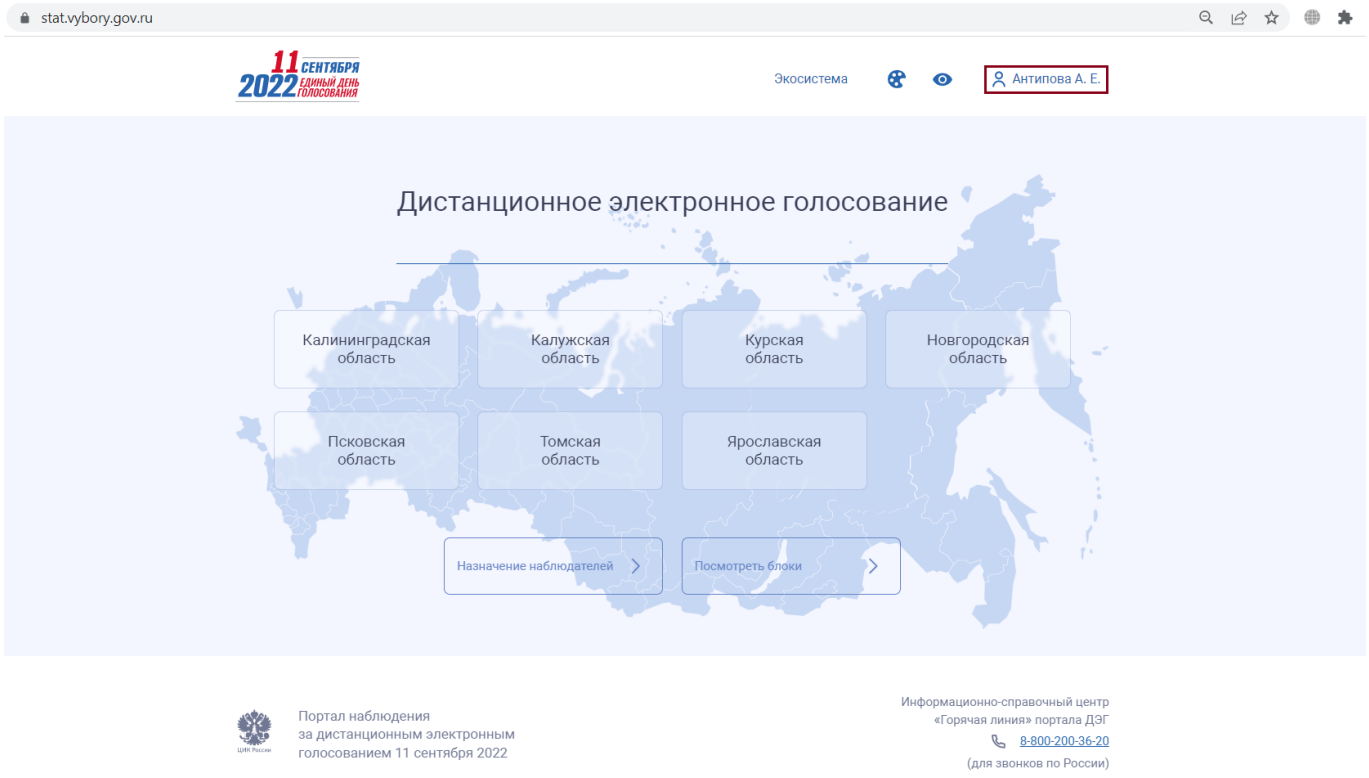

Рисунок 20 – Отображение профиля при входе в авторизованную зону портала наблюдения

При неуспешной авторизации отобразится страница с информацией об отсутствии доступа в авторизованную зону (рис.21).

По нажатию на кнопку «Вернуться на главную» пользователь перейдет к главной странице Портала наблюдения, откуда ему будет доступна функциональность неавторизованной зоны портала.

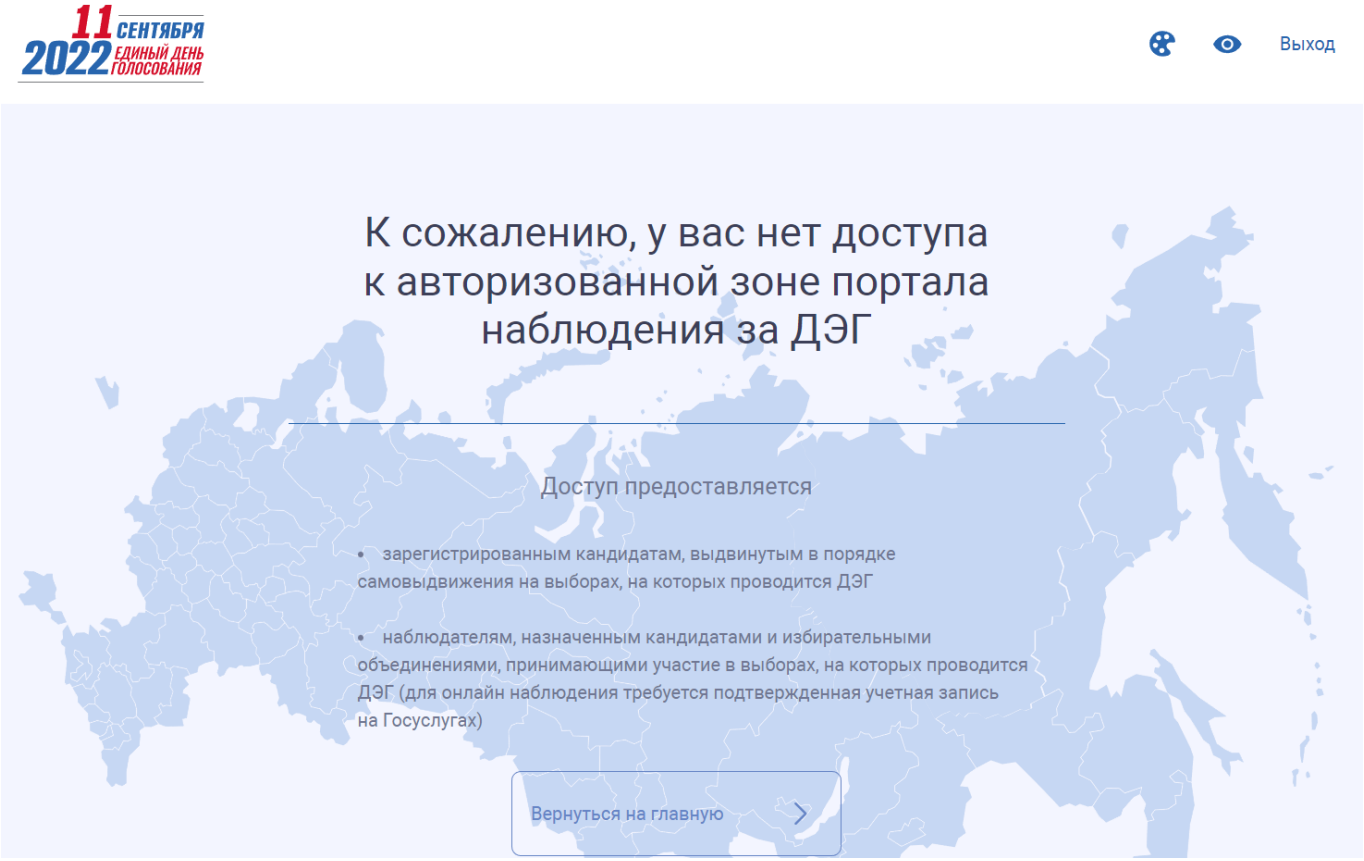

Рисунок 21 – Отображение главной страницы портала наблюдения при отсутствии доступа к авторизованной зоне

4.2.Дополнительные возможности Портала наблюдения авторизованной зоны

На каждой странице Портала наблюдения пользователю авторизованной зоны отображаются сквозные элементы, аналогичные возможностям пользователя неавторизованной зоны, за исключением раздела «Экосистема».

Помимо раздела «Экосистема» пользователю авторизованной зоны представлены расширенные возможности в части выгрузки на ПК файлов с транзакциями БЧ по голосованиям, в рамках которых он назначен наблюдателем.

4.2.1. Файловые выгрузки транзакций

Для авторизованных пользователей на странице со статистикой в разрезе округа/территории, ниже блока с почасовым графиком, представлен список файлов (рис.22). Файлы содержат информацию о транзакциях, записанных в БЧ. Они автоматически формируются и публикуются с интервалом один час (рис.22).

Рисунок 22 – Список файлов с транзакциями БЧ

Файловые выгрузки предназначены для сохранения истории проведения голосований и выполнения проверок корректности учтенных электронных бюллетеней, а также корректности подведения итогов голосования. В выгрузках содержатся все транзакции по голосованию, включая технические, системные, транзакции с ключами шифрования, результатами расшифрования данных об итогах голосований (см. Приложение 2).

Файлы доступны для скачивания как в течение голосования, так и после его завершения. В их корректности можно убедиться, проверив соответствие содержащихся в них данных, данным из БЧ по транзакциям и блокам.

4.2.1.1. Формирование файлов

! *Файл формируется в случае записи хотя бы одной транзакции в БЧ. Если записей в БЧ в течение часа нет, то пустой файл не создается системой.*

4.2.2. Раздел «Экосистема»

Раздел «Экосистема», расположенный в верхней части страницы Портала наблюдения, включает в себя следующе блоки (рис.23):

- «утилита наблюдателя» – блок, в котором доступна ссылка для скачивания программы, предназначенной для проверки полноты и целостности данных в БЧ, а также контроля правильности подсчета голосов;
- «исходный код» – блок для размещения ссылок на исходные коды ПТК ДЭГ;
- «полезные ссылки» – блок, содержащий ссылки на внешние ресурсы и дополнительные инструменты наблюдения, разработанные, в том числе, сторонними разработчиками. В настоящий момент в блоке размещены ссылки на скачивание следующих приложений:
  - «утилита для массовой выгрузки файлов транзакций на ПК» – программное обеспечение, разработанное сторонним разработчиком.
  - «утилита для генерации и разделения ключей» – программа, используемая для генерации открытого и закрытого ключей (ключей шифрования и расшифрования), а также для разделения и сборки закрытого ключа из его фрагментов для получения результатов голосования.
- «документация» – блок для размещения ссылок на документацию ПТК ДЭГ (в том числе нормативно-правовых актов, определяющих порядок применения ДЭГ, и технической документации системы, опубликованной на Портале ДЭГ).

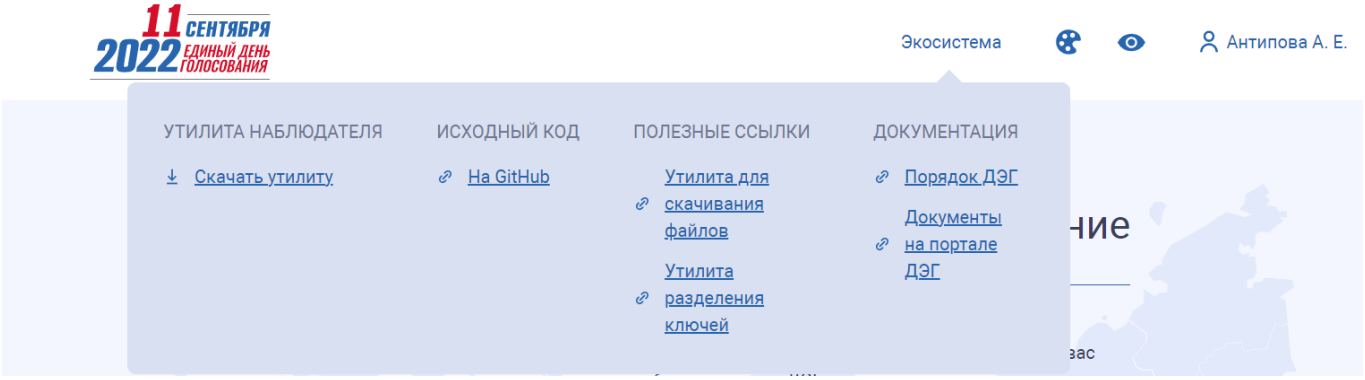

Рисунок 23 – Состав раздела "Экосистема"

4.2.2.1. Утилита для скачивания файлов

Утилита массовой выгрузки файлов транзакций, разработанная сторонним разработчиком, предназначена для пакетной выгрузки на ПК всех файлов с транзакциями из БЧ по каждому доступному пользователю голосованию.

Инструкция по её установке и использованию представлена в Приложении 3.

! *Выгрузить файлы, содержащие транзакции, можно стандартными инструментами Портала Наблюдения, без использования указанной утилиты. Для этого необходимо перейти на страницу округа/территории и нажать на название файла. Файл будет сохранён на вашем ПК.*

Выгруженные файлы необходимы для дальнейшей работы с утилитой наблюдателя.

Помимо работы с «утилитой наблюдателя» выгруженные файлы с транзакциями БЧ можно использовать для исследования и сравнения полученных данных с результатами голосования. Подробная информация о способах анализа данных описана сторонним разработчиком и находится в общем доступе по ссылке habr.com/ru/post/585448/.

Выгрузка файлов транзакций БЧ доступна на любом этапе с момента начала голосования, однако для получения полной картины по всем голосованиям пользователю рекомендуется дождаться процедуры подведения итогов голосований.

4.2.2.2. Утилита наблюдателя

Утилита наблюдателя – программа, используемая для выполнения криптографических проверок корректности учета бюллетеней и подведения итогов голосования. Обеспечивает выполнение следующих действий:

- восстановление истории проведения голосования по файловым выгрузкам из БЧ;
- проверку корректности учтенных бюллетеней на основании сохраненных в транзакциях доказательств корректности зашифрованной информации;
- суммирование бюллетеней без расширования с применением операции сложения в гомоморфном шифровании;
- проверку и формирование заключения о корректности записанных в БЧ расшифрованных результатов голосования.

Для выполнения проверок потребуется установить утилиту наблюдателя и сохранить файлы на компьютер.

Инструкция по установке и использованию утилиты наблюдателя представлена в Приложении 4.

4.2.2.3. Утилита для генерации и разделения ключей

Утилита для разделения ключей используется для генерации открытого и закрытого ключа, а также разделения и сборки закрытого ключа из его фрагментов.

Открытый ключ является публичным и располагается в общем доступе, в том числе в виде транзакции БЧ, которую можно увидеть на Портале наблюдения.

Закрытый ключ разделяется на несколько фрагментов и распределяется между несколькими лицами таким образом, что для его восстановления необходимо присутствие установленного заранее (при генерации и разделении закрытого ключа) количества держателей фрагментов ключа.

После сборки закрытого ключа из фрагментов необходимо загрузить собранный закрытый ключ в ПТК ДЭГ для расшифрования полученных данных об итогах ДЭГ.

Инструкция по сборке утилиты для генерации и разделения ключей представлена в Приложении 5.

Приложение 1

Полный состав исходных данных

№	Атрибут/ Комплексный тип	Обязательность	Тип данных	Описание
1.	Targets			Избирательные комиссии, для которых предназначены исходные данные
2.	TargetCommission			Сведения об избирательной комиссии, для которой предназначены исходные данные
3.	UIKname	Обязательный	string	Наименование УИК
4.	UIKnum	Обязательный	integer	Номер УИК
5.	CorTable			Таблица связи кодов комплектов бюллетеней и идентификаторов голосований
6.	ModNumber			Описание кода комплекта бюллетеней
7.	num	Обязательный	integer	Код комплекта бюллетеней
8.	ids	Обязательный	string	Идентификаторы голосований
9.	name	Рекомендуемый	string	Наименование комплекта бюллетеней
10.	Elections			Список кампаний
11.	Election			Кампания
12.	id	Обязательный	string	Идентификатор избирательной кампании

№	Атрибут/ Комплексный тип	Обязательность	Тип данных	Описание
13.	level	Обязательный		Уровень избирательной кампании (из справочника)
14.	sortLevel	Обязательный	int	Уровень проведения + Субъект выборов
15.	name	Обязательный	string	Наименование голосования
16.	Votings			Список голосований
17.	Voting			Голосование
18.	id	Обязательный	string	Идентификатор голосования
19.	type	Обязательный		Тип голосования из справочника (Основное, Дополнительное, Первичное, Повторное)
20.	districtNumber	Обязательный	integer	Номер округа
21.	districtName	Обязательный	string	Наименование единицы ТВД
22.	regionCode	Рекомендуемый	string	Субъект голосования
23.	timeOffset	Обязательный	integer	Часовой пояс голосования
24.	name	Обязательный	string	Наименование избирательной кампании
25.	startDateTime	Обязательный	dateTime	Дата и время начала избирательной кампании (планируемые)
26.	endDateTime	Обязательный	dateTime	Дата и время окончания избирательной кампании (планируемые)

№	Атрибут/ Комплексный тип	Обязательность	Тип данных	Описание
27.	TabulationComission			Избирательная комиссия, подводящая итоги по голосованию
28.	id	Обязательный	string	Идентификатор избирательной комиссии, подводящей итоги
29.	name	Обязательный	string	Наименование избирательной комиссии, подводящей итоги
30.	Protocol			Сведения о протоколе голосования
31.	id	Обязательный	string	Идентификатор типа протокола
32.	name	Рекомендуемый	string	Наименование типа протокола
33.	Lines			Список строк протокола
34.	Line			Срока протокола
35.	id	Обязательный	string	Идентификатор строки протокола
36.	num	Обязательный	integer	Номер строки протокола
37.	name	Обязательный	string	Наименование строки протокола
38.	votersCount	Рекомендуемый	integer	Число избирателей
39.	type	Рекомендуемый	string	Тип строки протокола
40.	Checks			Список контрольных соотношений протокола
41.	Check			Контрольное соотношение

№	Атрибут/ Комплексный тип	Обязательность	Тип данных	Описание
42.	enabled	Обязательный	boolean	Признак «включено» для контрольного соотношения
43.	expression	Обязательный	string	Выражение для проверки
44.	Ballots			Описатели бюллетеней
45.	Ballot			Описатель бюллетеня
46.	id	Обязательный	string	Идентификатор бюллетеня
47.	lang	Обязательный	integer	Язык бюллетеня
48.	marksType	Обязательный		Тип отметки в бюллетене
49.	maxMarks	Обязательный	integer	Максимальное допустимое количество отметок в бюллетене
50.	name	Обязательный	string	Наименование бюллетеня
51.	Positions			Позиции для голосования
52.	Position			Позиция для голосования
53.	id	Обязательный	string	Идентификатор позиции для голосования
54.	num	Обязательный	integer	Номер позиции для голосования
55.	disabled	Обязательный	boolean	Признак «отключено» для вопроса
56.	name	Обязательный	string	Наименование позиции для голосования
57.	description	Обязательный	string	Описание позиции для голосования
58.	image	Рекомендуемый	string	Изображение к позиции для голосования

№	Атрибут/ Комплексный тип	Обязательность	Тип данных	Описание
59.	Referendums			Список референдумов
60.	Referendum			Референдум
61.	TabulationComission			Избирательная комиссия, подводящая итоги по референдуму
62.	Protocol			Сведения о протоколе референдума
63.	Ballots			Список описателей бюллетеней
64.	Ballot			Описатель бюллетеня
65.	Questions			Список вопросов референдума
66.	question			Вопрос референдума
67.	answer			Ответ на вопрос референдума
68.	id	Обязательный	string	Идентификатор ответа на вопрос референдума
69.	num	Обязательный	integer	Номер ответа на вопрос референдума
70.	text	Обязательный	string	Текст ответа на вопрос референдума
71.	id	Обязательный	string	Идентификатор вопроса референдума
72.	num	Обязательный	integer	Номер вопроса референдума
73.	shortText	Обязательный	string	Краткий текст вопроса референдума

№	Атрибут/ Комплексный тип	Обязательность	Тип данных	Описание
74.	fullText	Обязательный	string	Полный текст вопроса референдума
75.	ElectionLevelEnum			Справочник уровня кампании по волеизъявлению

Приложение 2

Структура транзакций в ПТК ДЭГ

В данном разделе представлено описание параметров БЧ транзакций, обрабатываемых в ПТК ДЭГ. Транзакции можно условно разделить на четыре группы:

1) Транзакции подготовки голосования:
   - initiateVoting;
   - updateServerLis;
   - addMainKey;
   - startVoting.
2) Транзакции для работы со списком избирателей:
   - addVotersList;
   - removeFromVotersList;
   - addToVotersList.
3) Транзакции выдачи бюллетеня и приема голоса:
   - blindSigIssue;
   - vote.
4) Транзакции подведения итогов:
   - finishVoting;
   - decryption;
   - commissionDecryption;
   - results.

Транзакции подготовки голосования

initiateVoting – транзакция создания смарт-контракта голосования

Транзакция initiateVoting создает смарт-контракт голосования, который будет обрабатывать все последующие транзакции, относящиеся к голосованию. В параметрах транзакции содержатся публичные ключи компонент ПТК ДЭГ, для проверки отправляемых ими транзакций. Полный перечень параметров транзакции представлен в таблице 1.

Таблица 1 – Параметры транзакции initiateVoting

Параметр	Описание	Тип	Пример, примечание
bulletinHash	Хэш бюллетеня	string	5ec3f6a79frgwqgrgeetqgd339d4d135f3dba

Параметр	Описание	Тип	Пример, примечание
dimension	Размерность бюллетеня	string	[[1,1,3],[1,5,8]]
blindSigModulo	Модуль протокола выдачи слепой подписи	string	base64:lRTl6mS6ql16vNPY3Z...
blindSigExponent	Публичная экспонента протокола выдачи слепой подписи	string	base64:AQAB
dateStart	Дата и время начала приема бюллетеней (UTC по часам контракта)	DateTime	Поле опциональное
servers	Список публичных ключей серверов, от которых могут быть обработаны транзакции addMainKey, updateServerList, startVoting, finishVoting, decryption, commissionDecryption, results	string	["pubkey1", "pubkey2"]
votersListRegistrators	Участник, уполномоченный отправить транзакции addVotersList, removeFromVotersList, addToVotersList	string	"pubkey1"
blindSigIssueRegistrator	Участник, уполномоченный отправить транзакцию blindSigIssue	string	"pubkey1"
issueBallotsRegistrator	Участник, уполномоченный отправить транзакции startIssueBallots, stopIssueBallots	string	"pubkey1"
pollId	Id голосования в системах Ростелекома	string	uid

Параметр	Описание	Тип	Пример, примечание
isRevoteBlocked	Опциональный признак, отвечающий за возможность переголосований. isRevoteBlocked = false - переголосование разрешено, isRevoteBlocked = true или признак отсутствует - переголосование запрещено	Boolean	True
jwtTokenRegistrator	Сертификат системы идентификации.	string	Сертификат в base64

updateServerList – транзакция обновления публичных ключей серверов

Транзакция updateServerList обновляет публичные ключи компонент ПТК ДЭГ, для проверки отправляемых ими транзакций. Полный перечень параметров транзакции представлен в таблице 2.

Таблица 2 – Параметры транзакции updateServerList

Параметр	Описание	Тип	Пример, примечание
servers	Список публичных ключей серверов, от которых могут быть обработаны транзакции addMainKey, updateServerList, startVoting, finishVoting, decryption, commissionDecryption, results	string	["pubkey1", "pubkey2"]

addMainKey – транзакция записи в БЧ ключа зашифрования бюллетеней

Транзакция addMainKey публикует ключ, который будет применяться для зашифрования бюллетеней, а также публичный ключ ТИК ДЭГ и публичный ключ ЦИК, из которых он собирается. Полный перечень параметров транзакции представлен в таблице 3.

Таблица 3 – Параметры транзакции addMainKey

Параметр	Описание	Тип	Пример, примечание
mainKey	Ключ шифрования бюллетеней	string	
commissionKey	Ключ комиссии	string	
dkgKey	Ключ декрипта (ЦИК в целевом решении)	string	

startVoting – транзакция перевода голосования в режим приема голосов

Транзакция startVoting переводит голосование в режим приема голосов. Транзакция содержит ключ operation со значением startVoting.

Транзакции для работы со списком избирателей

addVotersList – транзакция записи в БЧ списка избирателей

Транзакция addVotersList публикует часть списка избирателей, допущенных к голосованию. Весь список избирателей публикуется несколькими транзакциями. Полный перечень параметров транзакции представлен в таблице 4.

Таблица 4 – Параметры транзакции addVotersList

Параметр	Описание	Тип	Пример, примечание
votersCount	Кол-во избирателей в списке	Integer	2
userIdHashes	Массив хешей userId избирателей	String	[\"123123123\", \"123123123\"]

removeFromVotersList – транзакция исключения избирателей из списка

Транзакция removeFromVotersList исключает избирателя/избирателей из списка избирателей. Полный перечень параметров транзакции представлен в таблице 5.

Таблица 5 – Параметры транзакции removeFromVotersList

Параметр	Описание	Тип	Пример, примечание
userIdHashes	Массив хешей userId избирателей	String	[\"123123123\", \"123123123\"]

addToVotersList – транзакция добавления избирателей в список

Транзакция addToVotersList восстанавливает избирателя/избирателей в списке избирателей. Полный перечень параметров транзакции представлен в таблице 6.

Таблица 6 – Параметры транзакции addToVotersList

Параметр	Описание	Тип	Пример, примечание
userIdHashes	Массив хешей userId избирателей	String	[\"123123123\", \"123123123\"]

Транзакции выдачи бюллетеня и приема голоса

blindSigIssue - транзакция записи факта формирования подписи вслепую

Транзакция blindSigIssue публикует значения подписей вслепую маскированных публичных ключей избирателей, что свидетельствует о фактах успешной авторизации избирателей и получения ими бюллетеней. Полный перечень параметров транзакции представлен в таблице 7.

Таблица 7 – Параметры транзакции blindSigIssue

Параметр	Описание	Тип	Пример, примечание
data	Факт формирования подписи вслепую	String	[{ /"userId/": /"userId1/", /"maskedSig/": /"maskedSig1/"}, { /"userId/": /"userId2/", /"maskedSig/": /"maskedSig2/"}] где userId - внутренний ID избирателя в авторизованной зоне maskedSig - значение подписи вслепую маскированного публичного ключа избирателя

vote – транзакция записи зашифрованного голоса

Транзакция vote записывает зашифрованный голос избирателя. Транзакция также содержит значение подписи вслепую публичного ключа избирателя, с которого снят маскирующий фактор. Полный перечень параметров транзакции представлен в таблице 8.

Таблица 8 – Параметры транзакции vote

Параметр	Описание	Тип	Пример, примечание
vote	Зашифрованный голос	binary	Байтовое представление
blindSig	Слепая подпись избирателя	binary	Байтовое представление

Транзакции подведения итогов

finishVoting – транзакция перевода голосования в режим завершения приема голосов

Транзакция finishVoting переводит голосование в режим завершения приема голосов. Транзакция содержит ключ operation со значением finishVoting.

decryption – транзакция записи результата частичной расшифровки ключом ЦИК

Транзакция decryption публикует результат частичной расшифровки итогов голосования, полученный с применением ключа расшифровки ЦИК. Полный перечень параметров транзакции представлен в таблице 9.

Таблица 9 – Параметры транзакции decryption

Параметр	Описание	Тип	Пример, примечание
decryptions	Результат частичной расшифровки результата подсчета голосов ключом ЦИК	binary	Байтовое представление

commissionDecryption – транзакция записи результата частичной расшифровки ключом организующей комиссии

Транзакция commissionDecryption публикует ключ расшифровки ТИК ДЭГ и результат частичной расшифровки итогов голосования, полученный с применением этого ключа. Полный перечень параметров транзакции представлен в таблице 10.

Таблица 10 – Параметры транзакции commissionDecryption

Параметр	Описание	Тип	Пример, примечание
decryptions	Результат расшифровки ключом комиссии	binary	Байтовое представление
commisionSecretKey	Приватный ключ комиссии	string	Необязательное поле. hex

results – транзакция записи результатов голосования

Транзакция results публикует итоги голосования, посчитанные на основе частичной расшифровки на ключе ЦИК и частичной расшифровки на ключе ТИК ДЭГ. Полный перечень параметров транзакции представлен в таблице 11.

Таблица 11 – Параметры транзакции results

Параметр	Описание	Тип	Пример, примечание
results	Результаты подсчетов в расшифрованном виде	string	[[25,23,11,11,6,3,1,0]]

Приложение 3

Инструкция по утилите для скачивания файлов

! *Утилита массовой выгрузки файлов транзакций БЧ разработана сторонним разработчиком. Выгрузить файлы, содержащие транзакции, можно стандартными инструментами Портала Наблюдения, без использования указанной утилиты. Для этого необходимо перейти на страницу округа/территории и нажать на название файла. Файл будет сохранён на вашем ПК.*

Пользователю для загрузки и использования утилиты для скачивания файлов необходимо произвести следующие действия:

1) Нажать на раздел «Экосистема» в верхней части страницы Портала наблюдения.
2) Перейти по ссылке «Утилита для скачивания файлов».
3) Загрузить файл с названием «VotingFilesDownloader-2022-08-31-1-win-x86.zip» (рис.24).

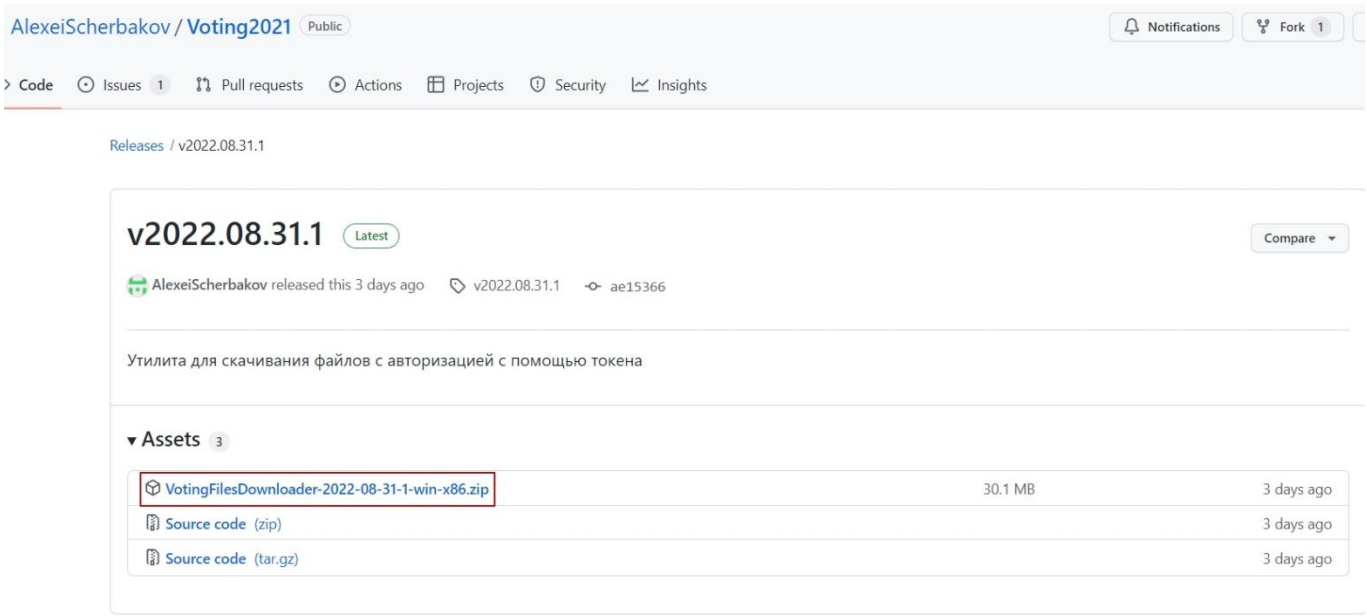

Рисунок 24 – Файл для скачивания на ресурсе GitHub

4) Разархивировать загруженную папку.
5) Запустить ПО Windows PowerShell.
6) В Windows PowerShell запустить директорию по команде «*cd <указать путь папки, где находится разархивированная папка>*.» и нажать на клавишу Enter.

   Для удобства указания пути, где располагается разархивированная папка, в Windows PowerShell рекомендуется вводить несколько начальных

символов папки и нажимать на клавишу Tab для переключения между предлагаемыми вариантами папок. Альтернативным способом является ввод пути к папке вручную. При успешном выполнении команды в Windows PowerShell осуществится переход к этой папке. (рис.25).

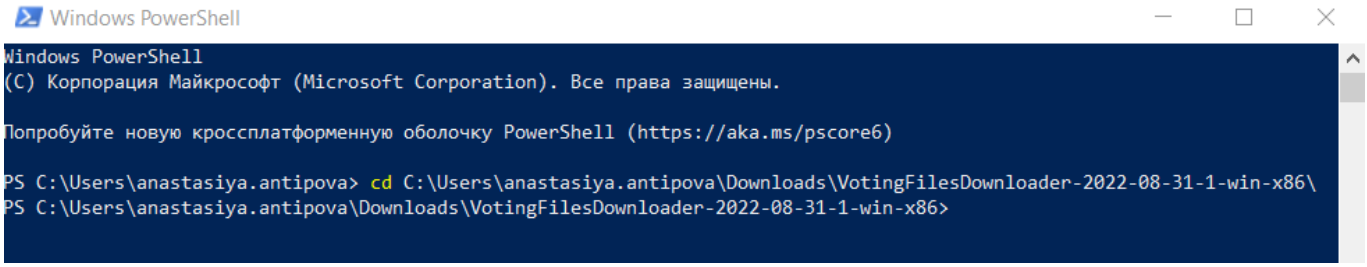

Рисунок 25 – Пример указания пути к папке в ПО Windows PowerShell

7) После символа >, которым оканчивается путь папки, ввести символ пробела, и далее название установочного файла *.\VotingFilesDownloader.exe* (рис.26).

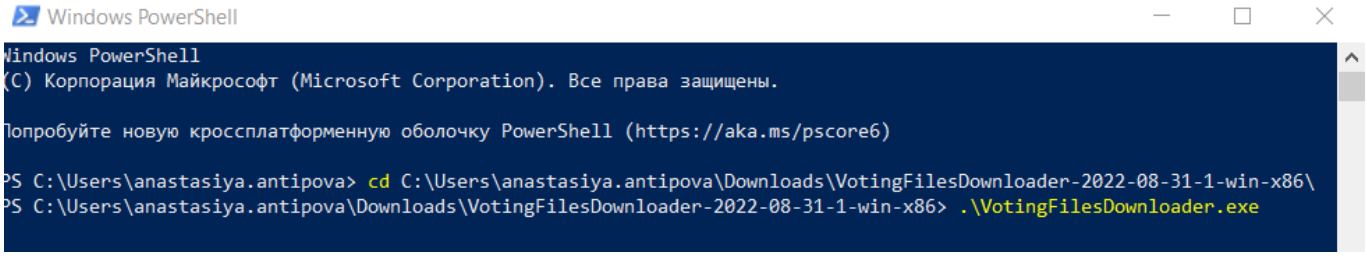

Рисунок 26 – Пример указания пути к файлу в ПО Windows PowerShell

8) Авторизоваться на Портале наблюдения с помощью учетной записи Госуслуг по ссылке https://stat.vybory.gov.ru/.
9) Открыть инструменты разработчика на странице Портала наблюдения.
10) В инструментах разработчика перейти к вкладке «Application», развернуть раздел «Local Storage», выбрать ссылку https://stat.vybory.gov.ru/.
11) В рабочей области выбрать строку «Token» и скопировать ее значение (рис.27).

! Для массовой выгрузки файлов требуются свежие данные из строки «Token». Для получения обновленной информации рекомендуется выйти из профиля на Портале наблюдения и вновь войти с помощью авторизации по учетной записи Госуслуг.

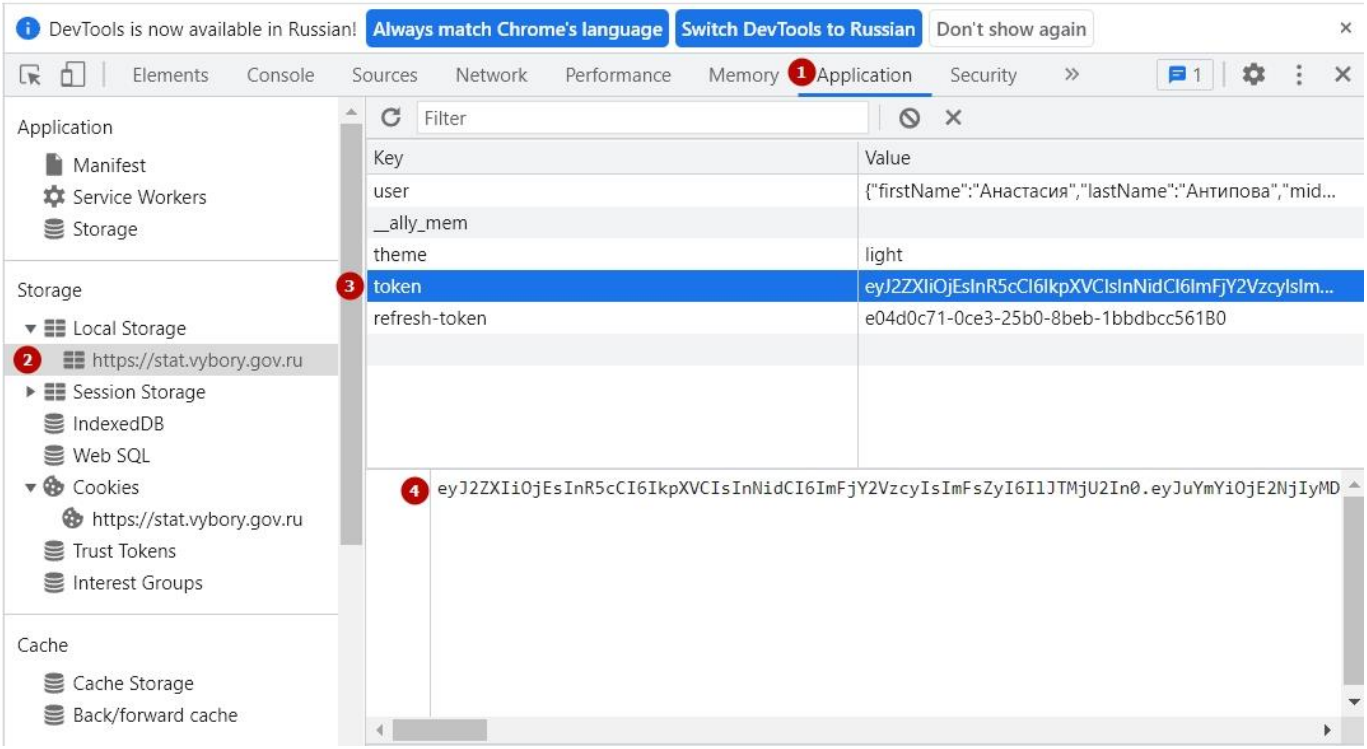

Рисунок 27 – Копирование значение Token из инструмента разработчика

12) Вернуться в Windows PowerShell и после указания названия установочного файла ввести символ пробела и далее *«--token=<скопированное значение «Token»* из инструмента разработчика >, после чего нажать на клавишу Enter (рис.28)

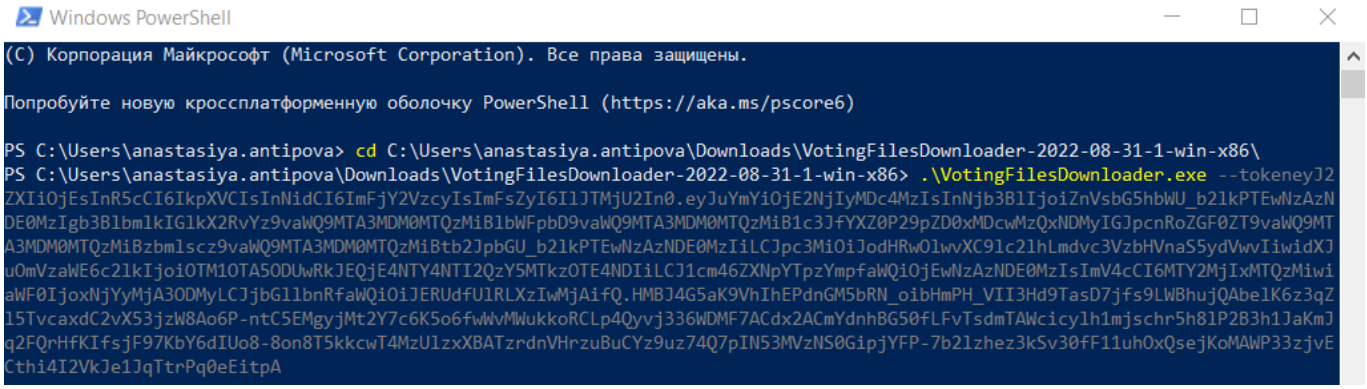

Рисунок 28 – Пример ввода значения из строки Token в ПО Windows PowerShell

В ПО Windows PowerShell отобразиться прогресс загрузки файлов на ПК. Перед загрузкой по указанному в п.6 пути появится папка «data», в которую будет вложена папка «files» и файл с базой данных формата «db3».

В папку «data» загрузятся папки, которые будут именованы по названию смарт-контракта голосования (рис.29).

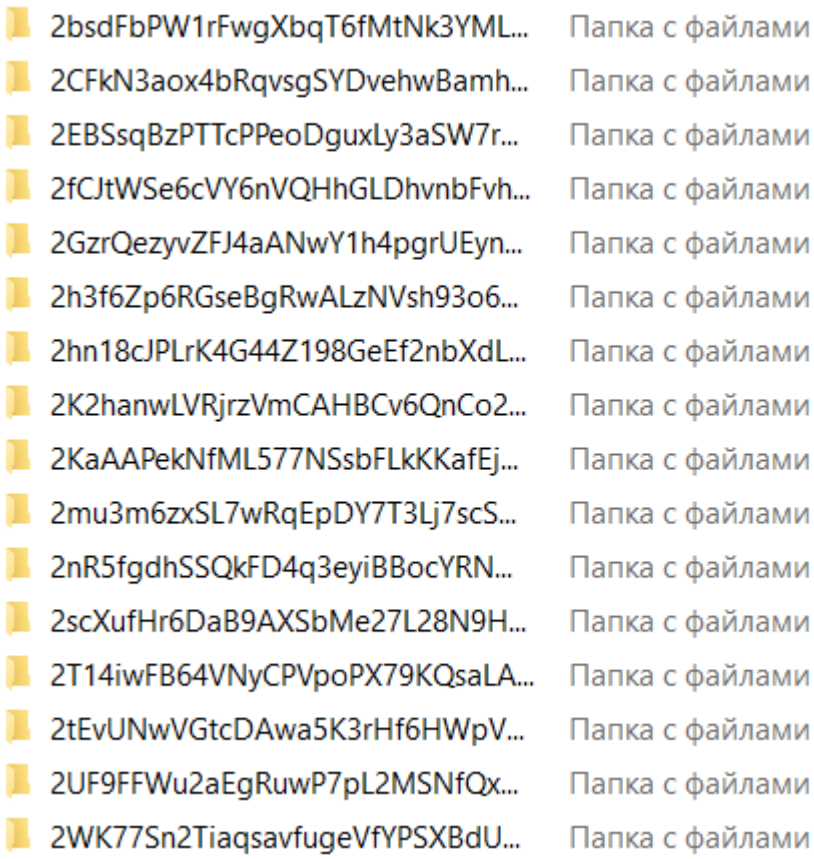

Рисунок 29 – Пример папки files, внутри которой находятся папки, именованные смарт-контрактом голосования

Внутри каждой такой папки будут архивированные папки с транзакциями, относящимися к конкретному голосованию, которые существуют на Портале наблюдения на момент выгрузки.

В случае повторного запуска массовой файловой выгрузки на ПК в течение голосования, осуществляется дополнение уже существующих папок новыми данными без обновления ранее выгруженных файлов (рис.30).

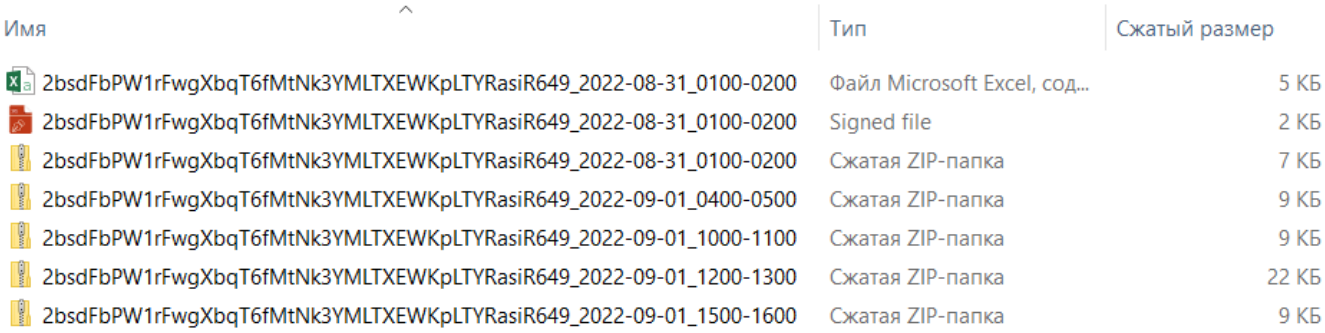

Рисунок 30 – Папка смарт-контракта голосования с архивами транзакций

Выгруженные файлы необходимы для дальнейшей работы с утилитой наблюдателя, а также для исследования и сравнения полученных данных с результатами голосования. Подробная информация о способах анализа данных

описана сторонним разработчиком и находится в общем доступе сети Интернет по ссылке habr.com/ru/post/585448/.

Приложение 4

1. Техническое описание утилиты наблюдателя

Утилита используется для выполнения криптографических проверок корректности учета бюллетеней и подведения итогов голосования. По файловым выгрузкам из БЧ восстанавливает историю проведения голосования, проверяет корректность учтенных бюллетеней, основываясь на сохраненных в транзакциях доказательствах корректности зашифрованной информации, суммирует бюллетени (без расшифрования) с применением техники гомоморфного сложения, проверяет и выдает заключение о корректности записанных в БЧ расшифрованных результатах голосования.

Корректность бюллетеня означает:

- Присутствие в нем всех необходимых ячеек с шифртекстами голосов за каждого отдельного кандидата из бюллетеня.
- Корректность подписи ГОСТ Р 34.10-2012 транзакции бюллетеня (проверяется при помощи открытого ключа ГОСТ Р 34.10-2012 голосующего).
- Корректность слепой подписи открытого ключа голосующего (который соответствует подписи транзакции). Эта подпись выдается регистратором и подтверждает, что голосующий имеет право голосовать, т.к. его открытый ключ был подписан вслепую Регистратором (т.е. Регистратор не видел, какой открытый ключ он подписывал, но был уведомлен, что голосующий имеет на это право).
- Корректность каждого доказательства с нулевым разглашением range proof (в диапазоне от [0,1]) в каждой ячейке бюллетени. Голосующий может положить в ячейку за каждого кандидата либо 0, либо 1 и зашифровать их. Внесение других чисел в ячейку не предусмотрено, в этом случае доказательство будет некорректным.
- Корректность каждого доказательства с нулевым разглашением range proof для суммы ячеек [1,N]. Число N устанавливается избирательной комиссией для каждого голосования. Голосующий может проголосовать за любое количество кандидатов строго в диапазоне от 1 до N включительно. Число кандидатов и отданное предпочтение за кандидатов, за которых избиратель проголосовал, остается известным только самому голосующему.

Утилита проверяет опубликованные результаты в следующем порядке:

1) Загружает закрытый ключ комиссии commissionPrivKey.

2) Загружает результаты работы сервера подсчета, который частично расшифровал суммарный бюллетень. Это {privDecryptServicesum(R_1_i), zkp_1}, {privDecryptServicesum(R_2_i), zkp_2}, ... , {privDecryptServicesum(R_M_i), zkp_M}
где zkp_j - доказательство корректности расшифровки, т.е доказательство того, что точка privDecryptServicesum(R_j_i), представляет собой именно скалярное умножение точки sum(R_j_i) и закрытого ключа privDecryptService в виде его произведения на точки sum(R_1_i), ... , sum(R_M_i) и zkp, которые это подтверждают.

3) Проверяет все M доказательств zkp_j для M ячеек суммарной бюллетени и в случае хотя-бы одного некорректного доказательства выдает ошибку.

4) В случае корректности всех M zkp производится полная расшифровка суммарного бюллетеня:
V_1 = sum(C_1_i) - k1privDecryptServicesum(R_1_i) - k2commissionPrivKeysum(R_1_i), V_2 = sum(C_2_i) - k1privDecryptServicesum(R_2_i) - k2commissionPrivKeysum(R_2_i), . . . V_M = sum(C_M_i) - k1privDecryptServicesum(R_M_i) - k2commissionPrivKeysum(R_M_i),
где k1 = Hash(PubDecryptService || commissionPubKey), k2 = Hash(commissionPubKey || PubDecryptService), т.е. коэффициенты, с помощью которых вычислялся PubMain, на котором шифровались все бюллетени в данном голосовании.

Все эти M точек содержат сумму голосов за каждого из M кандидатов, закодированную в следующем виде:

V_j = voted_for_j*BasePoint,

где voted_for_j – число голосов за j-го кандидата, BasePoint – базовая точка используемой элиптической кривой.

Для решения этих уравнений и получения всех voted_for_j можно использовать метод полного перебора возможных значений voted_for_j (очевидно, что он лежит в диапазоне от 0 (никто не проголосовал за кандидата) до числа всех проголосовавших с валидными бюллетенями).

Итого в результате должен получиться результат голосования:

voted_for_1, voted_for_2, ... , voted_for_M

2. Инструкция по сборке и запуску утилиты наблюдателя

Предварительная подготовка к пользованию утилитой наблюдателя

При необходимости установить утилиту наблюдателя на операционную систему Windows требуется дополнительная установка программного обеспечения Docker Desktop и git.

Ниже представлены инструкции по установке программ.

Инструкция по установке программного обеспечения Docker на операционную систему Windows

1) Загрузить с официального сайта https://www.docker.com/ установщик Docker Desktop на Windows по кнопке «Download Docker Desktop Windows».
2) Дважды нажать левой кнопкой мыши по файлу «Docker Desktop Installer» для запуска процесса установки.
3) Следовать инструкциям мастера установки, дать установщику разрешение на использование прав администратора.
4) Дождаться окончания установки.

Инструкция по установке программного обеспечения git на операционную систему Windows

1) Загрузить с официального сайта https://gitforwindows.org/ установщик git for Windows по кнопке «Download».
2) Дважды нажать левой кнопкой мыши по файлу «Git-<номер версии>.exe» для запуска процесса установки.
3) Следовать инструкциям мастера установки, дать установщику разрешение на использование прав администратора.
4) Дождаться окончания установки.

После завершения предварительных работ по установке дополнительного программного обеспечения пользователю для сборки и запуска утилиты наблюдения необходимо произвести следующие действия:

1) Нажать на раздел «Экосистема» в верхней части страницы Портала наблюдения.

2) Перейти по ссылке «Скачать утилиту».
3) На странице ресурса Github по ссылке https://github.com/cikrf/deg2022 нажать на кнопку «Code» и скопировать ссылку для клонирования репозитория (рис.31).

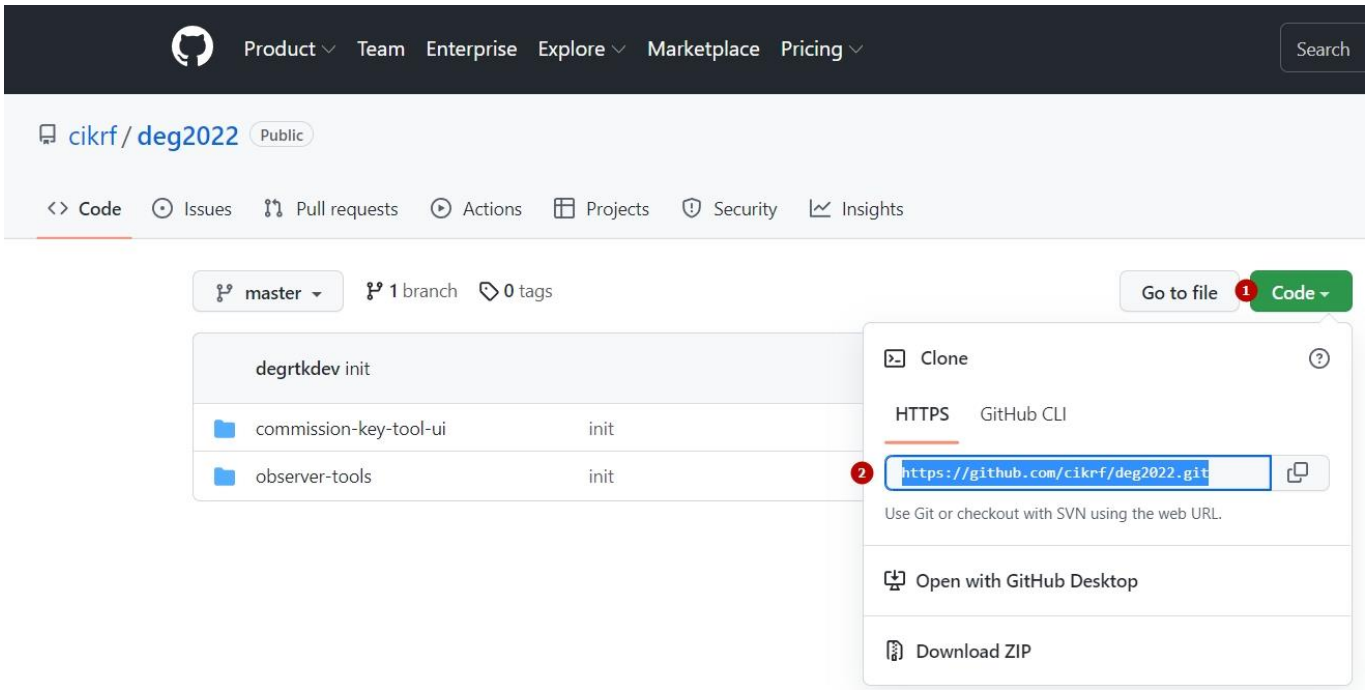

Рисунок 31 – Копирование ссылки из ресурса Github

4) Открыть программу Git Bash и ввести команду: *git clone https://github.com/cikrf/deg2022.git* и нажать Enter. На экране отобразится результат клонирования репозитория. В верхней части окна указана папка, куда производится запись файлов репозитория. (рис.32).
5) Закрыть ПО Git Bash.

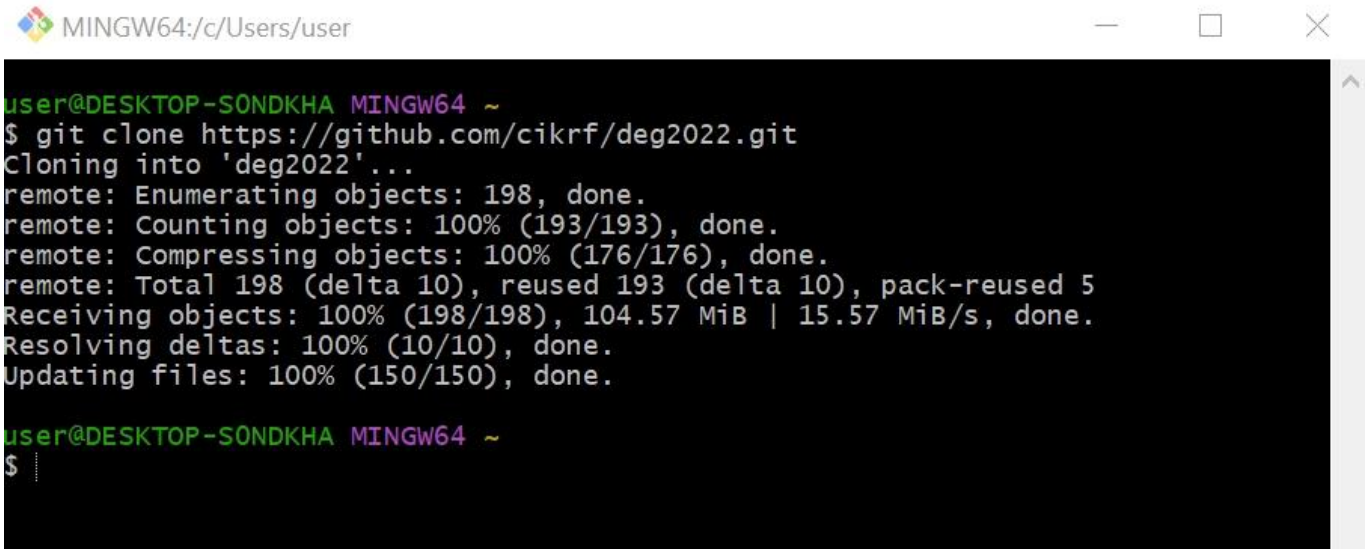

Рисунок 32 – Отображение успешной операции по клонированию репозитория на локальный компьютер

6) Открыть браузер и перейдите на сайт КриптоПро по ссылке https://www.cryptopro.ru/.
7) Перейти к загрузке установщика файла КриптоПро CSP 5.0 для Linux (x64, deb) (рис.33).

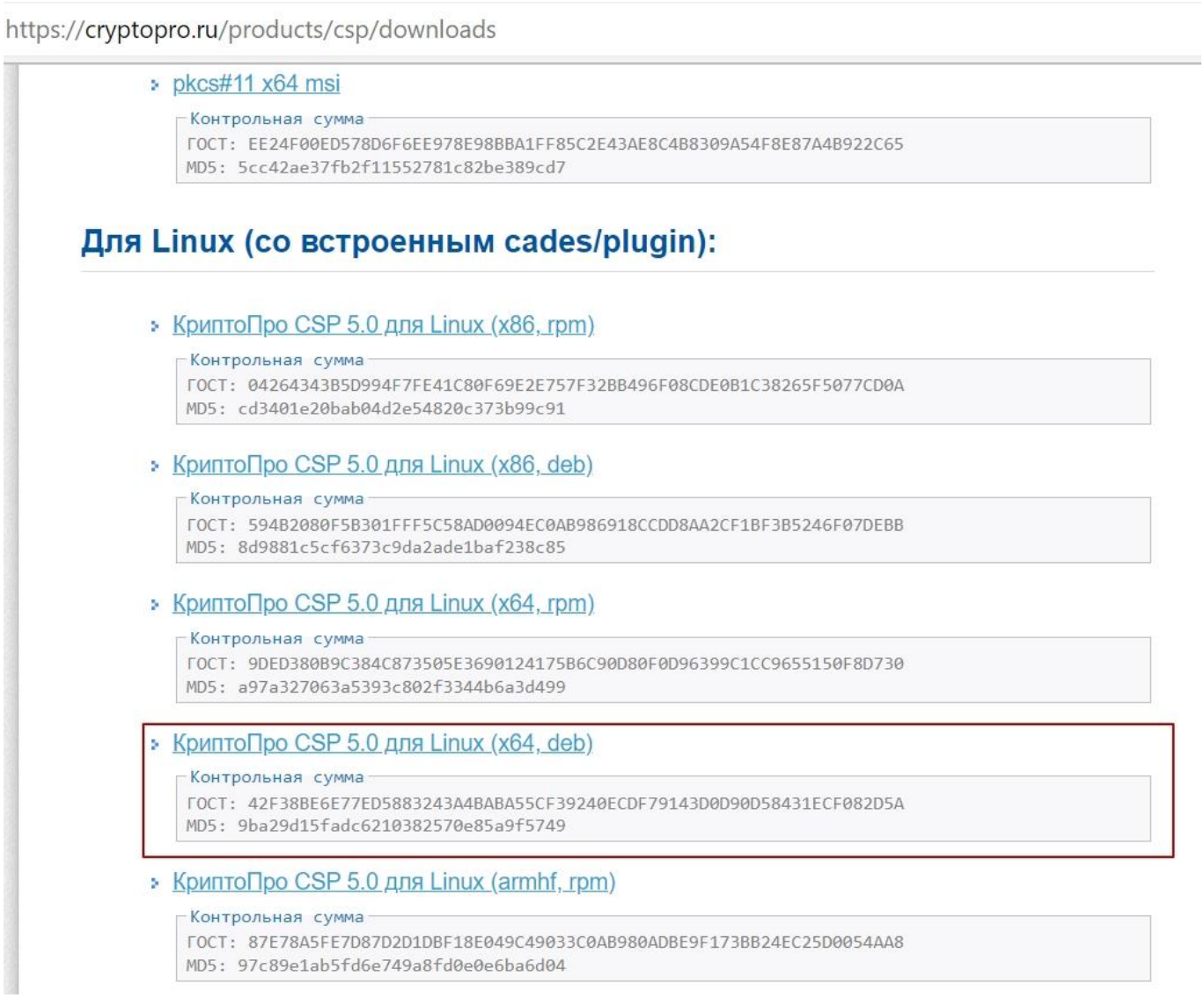

Рисунок 33 – Ссылка для загрузки КриптоПро для Linux

8) Загруженный файл linux-amd64_deb.tgz скопировать в папку репозитория deg2022/observer-tools (рис.34).

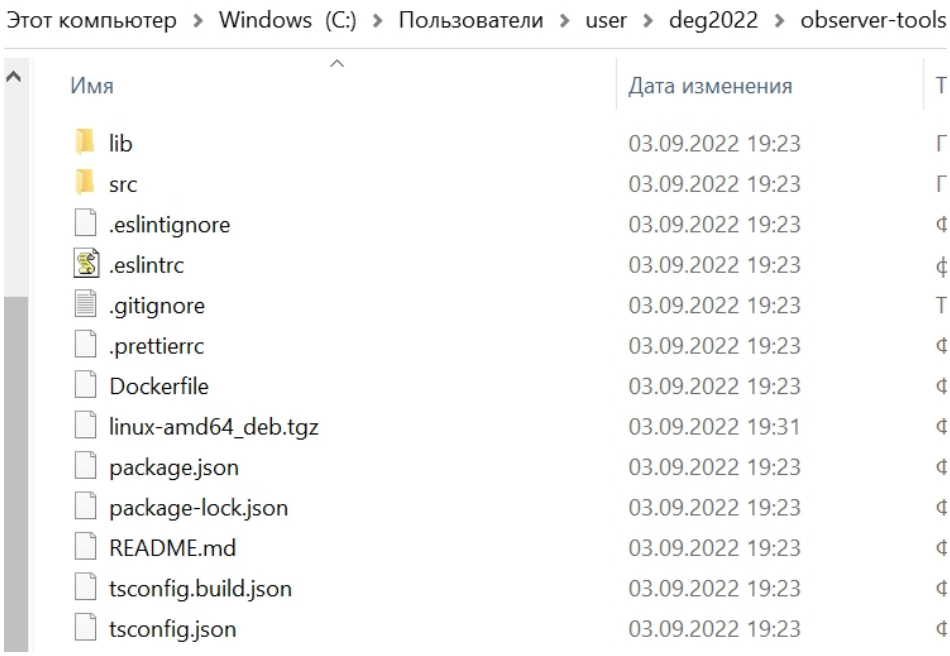

Рисунок 34 – Перечень файлов в директории при копировании установщика КриптоПро для Linux

13) Запустить ПО Windows PowerShell, изменить директорию по команде «*cd <указать путь папки, где находится утилита наблюдателя>*» и нажать на клавишу Enter.

Для удобства указания пути, где располагается склонированная папка из ПО Git Bash, в ПО Windows PowerShell рекомендуется вводить несколько начальных символов папки и нажимать на клавишу Tab для переключения между предлагаемыми вариантами папок. Альтернативным способом является ввод пути к папке вручную. При успешном выполнении команды в ПО Windows PowerShell осуществится переход папке. (рис.35).

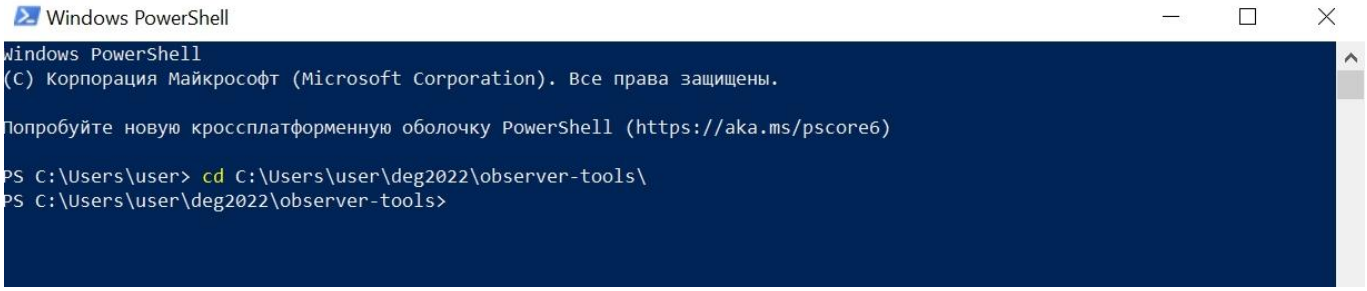

Рисунок 35 – Пример указания пути к папке в ПО Windows PowerShell

14) Задать команду *git init* для создания пустого репозитория Git (рис.36)

Рисунок 36 – Инициация создания репозитория Git

15) После символа >, которым оканчивается путь папки, ввести команду для сбора docker-образа: *docker build -t <название образа на усмотрение пользователя> -f Dockerfile .* (рис.37)/

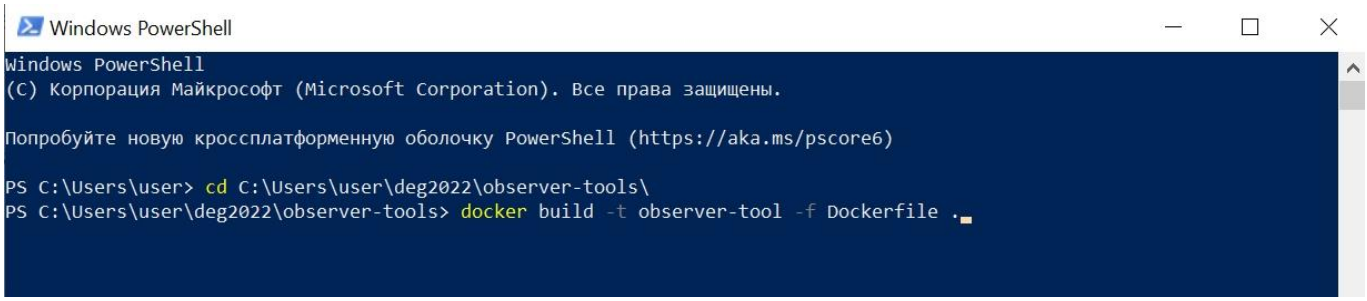

Рисунок 37 – Пример ввода команды для создания образа в ПО Docker Desktop

16) Нажать на клавишу Enter для запуска создания образа.
17) По завершении команды создания образа перейти в ПО Docker Desktop для проверки создания образа (рис.38).

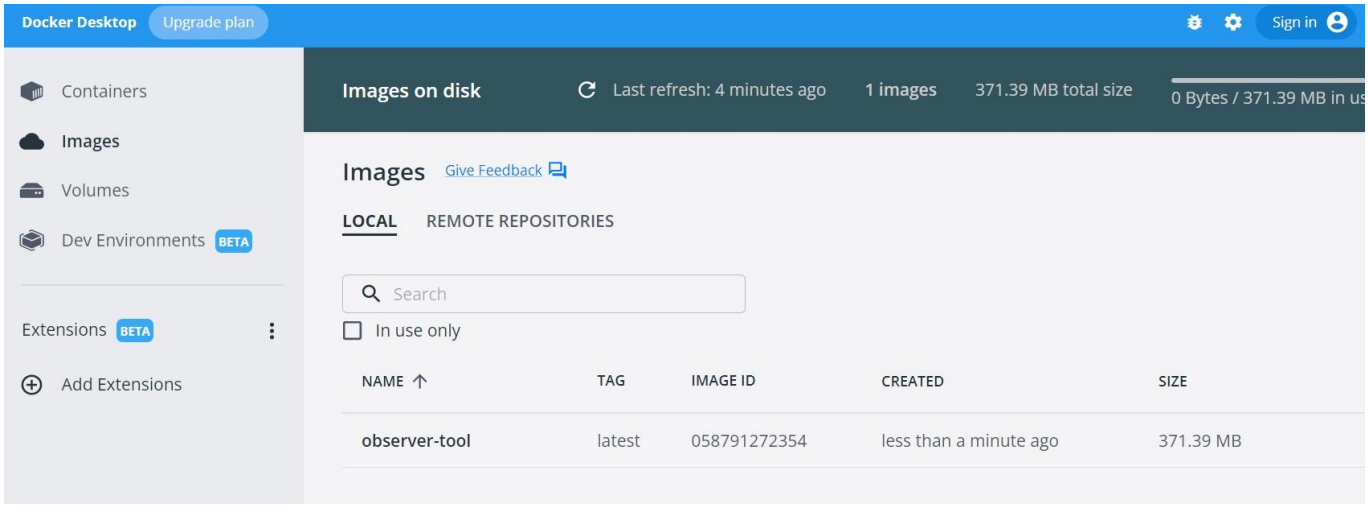

Рисунок 38 – Созданный образ в ПО Docker Desktop

! Для увеличения производительности проверки рекомендуется увеличить количество используемых ядер в Docker Desktop.

18) Разархивировать папку «files», которая была создана при массовой выгрузке транзакций.
19) Вернуться в ПО Windows PowerShell для запуска проверки корректности учета бюллетеней и подведения итогов голосования.
20) Изменить директорию по команде «*cd <указать путь папки, где хранится архив с голосованием, которое надо проверить>*» и нажать на клавишу Enter (рис.39).

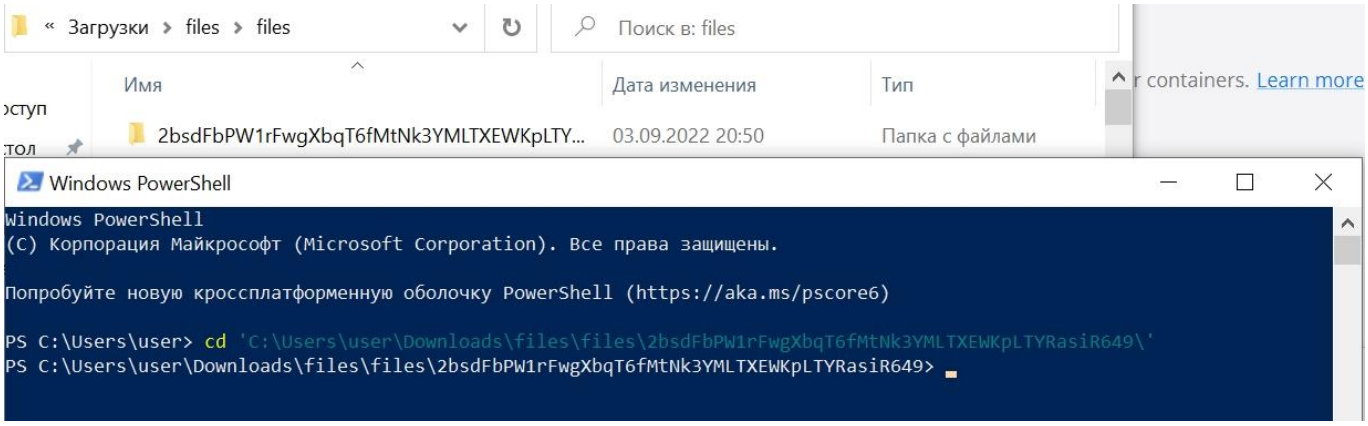

Рисунок 39 – Пример команды указания директории для обращения к конкретному голосованию в ПО Windows PowerShell

21) Выполнить команду, указанную ниже, после чего нажать на клавишу Enter:

- Для проверки одного голосования: *docker run --rm -t -i --mount type=bind,source="$(pwd)",target=/app/files,readonly <указать имя образа, созданного в Docker Desktop на шаге 16> run validate <указать имя папки голосования, которую необходимо проверить>* (рис.40, 41)

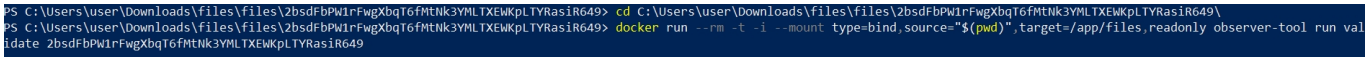

Рисунок 40 – Пример команды для проверки одного голосования

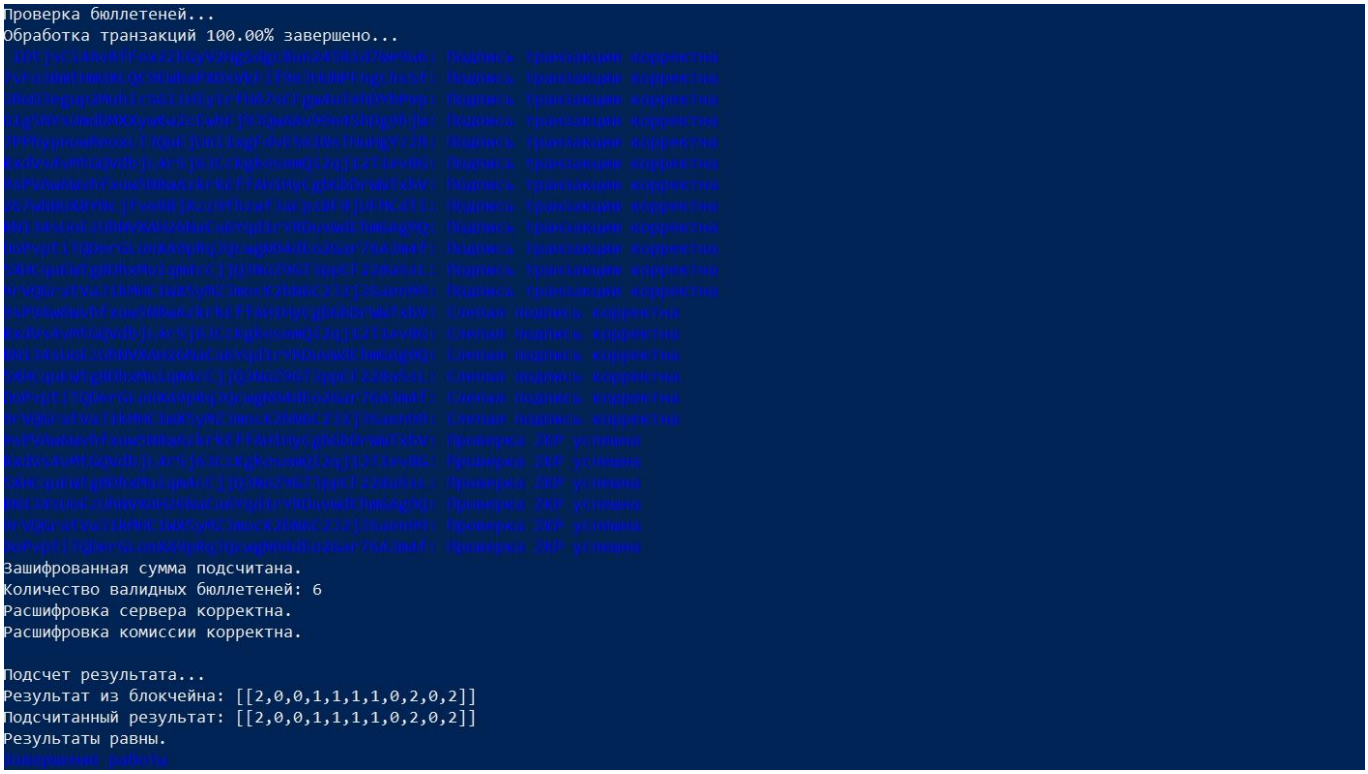

Рисунок 41 – Пример проверки транзакций по выбранному голосованию

- Для всех голосований в папке «files»: *docker run --rm -t -i --mount type=bind,source=//c/git/rtk/<указать имя образа, созданного в Docker Desktop на шаге 16>/temp,target=/app/files,readonly observer-tool run validate -> log.txt*

Результаты проверки всех голосований результаты будут сохранены в файле «log». При необходимости остановки проверки голосований требуется нажать сочетание клавиш CTRL+C .

- ! Необходимо учесть, что при указании команды вывода текущей рабочей директории *$(pwd)* команды в ПО Windows PowerShell для Linux автоматически выбирается текущая папка, для Windows необходимо вместо *$(pwd)* указать путь к текущей папке.

Приложение 5

Инструкция по настройке и установке утилиты для генерации и разделения ключей

Предварительная подготовка к пользованию утилитой по разделению ключей для программного обеспечения Astra Linux 1.7.1 Воронеж

Настройка Astra Linux для работы с Рутокеном

Перед установкой библиотек необходимо подключить установочный диск с отметкой «*OS Astra Linux 1.7.1 1.7_x86-64 DVD*», после чего выполнить установку дополнительных библиотек для работы с Рутокен:

1) Запустить ПО Windows PowerShell
2) Выполнить команды: *sudo apt install libccid pcscd libpcsclite1 pcsc-tools opens.*
3) Для проверки видимости Рутокена выполнить команду: *pcsc_scan*

Настройка окружения для запуска AppImage в Astra Linux 1.7.1 Воронеж

Чтобы система могла запускать приложения appimage, в параметры ядра нужно добавить опцию *parsec.enable_exec_on_fuse=1*:

1) В файле */etc/default/grub* добавить параметр в содержимое следующей переменной:
   GRUB_CMDLINE_LINUX_DEFAULT="parsec.max_ilev=63 parsec.enable_exec_on_fuse=1 quiet net.ifnames=0"
2) Далее необходимо обновить конфигурацию загрузчика GRUB и перезагрузить систему: *sudo update-grub sudo reboot*

Установка утилиты и настройка ярлыка на рабочем столе

1) Создать папку *'~/CommissionKeyTool/'* и скопировать *CommissionKeyTool-x.x.x.AppImage*, где x.x.x - версия утилиты.
2) Выполнить команду: # chmod +x ./CommissionKeyTool-x.x.x.AppImage
3) Выполнить команду: # ./CommissionKeyTool-x.x.x.AppImage --appimage-extract
4) В папке «*~/CommissionKeyTool/squashfs-root*» удалить все файлы, кроме:
   - *squashfs-root/keytool-ui.png*
   - *squashfs-root/usr/share/icons*

5) Правой кнопкой мыши вызвать меню для файла «*CommissionKeyTool-x.x.x.AppImage*».
6) Выбрать «*Отправить» -> «Рабочий стол (создать ярлык)*».
7) Переименовать ярлык на рабочем столе в «CommissionKeyTool» или в другое презентабельное имя.

Открыть свойства ярлыка и перейти на вкладку «Ярлык». В поле «Значок» указать путь к изображению: «*~/CommissionKeyTool/squashfs-root/keytool-ui.png*».