Дистанционное электронное голосование

РусКрипто 2022

Что такое ДЭГ

Реализация активного избирательного права (права на участие в референдуме)

на специальном портале, размещенном в сети Интернет

с использованием находящихся во владении (пользовании) абонентских устройств

в случаях и порядке, которые установлены федеральным законом 67-ФЗ*

** – Федеральный закон от 14 марта 2022 года № 60-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» вступил в силу со дня его официального опубликования, то есть с 14 марта 2022 года.*

Нормативное регулирование ДЭГ

ДО ВСТУПЛЕНИЯ В СИЛУ 60-ФЗ	ПОСЛЕ ВСТУПЛЕНИЯ В СИЛУ 60-ФЗ
в Федеральном законе № 67-ФЗ содержались: определение ДЭГ, норма, предусматривающая возможность проведения ДЭГ, а также положение о том, что порядок проведения ДЭГ утверждается ЦИК России;	в Федеральный закон № 67-ФЗ введена **новая статья 64[1]**, устанавливающая основные принципы и параметры проведения ДЭГ, единые для всех выборов и референдумов на территории Российской Федерации;
порядок проведения ДЭГ в городе Москве регулировался Федеральным законом «О проведении эксперимента по организации и осуществлению дистанционного электронного голосования в городе федерального значения Москве», законами города Москвы, актами ЦИК России и МГИК	ДЭГ проводится с использованием ГАС «Выборы», а также иных государственных информационных систем, прошедших сертификацию и соответствующих требованиям, установленным ЦИК России;
	обязательная идентификация, аутентификация и подтверждение личности;
	анонимизация результатов волеизъявления, их зашифрование при проведении голосования и расшифрование после его завершения;

Портал ДЭГ

п. 15 статьи 64.1 Федерального закона 67-ФЗ

Дистанционная идентификация
и аутентификация участников ДЭГ

✓ в том числе с использованием специального мобильного приложения

! как обеспечить доверие браузерам/мобильным устройствам
как обеспечить распространение мобильных приложений?

Критичные свойства безопасности системы

СВОЙСТВО	МЕРЫ ЗАЩИТЫ ОТ НАРУШИТЕЛЯ
Подлинность выборов	Аутентификация избирателей через ЕСИА Подпись вслепую открытых ключей избирателей Подпись бюллетеня Доказательство корректности содержимого бюллетеня Доказательство корректности использования правильного ключа расшифрования
Анонимность избирателей	Подпись вслепую открытых ключей избирателей Гомоморфное шифрование бюллетеней Разделение ключа шифрования Доказательство корректности содержимого бюллетеня (с нулевым разглашением)
Конфиденциальность промежуточных результатов	Шифрование бюллетеней Разделение ключа шифрования Доказательство корректности содержимого бюллетеня (с нулевым разглашением) Доказательство корректности использования правильного ключа расшифрования (с нулевым разглашением)

Протокол тайного голосования и МУиН

Письмо ФСБ России о Концепции федеральной системы ДЭГ,
Исследования КриптоПро и Криптонит

ТЕХНОЛОГИИ	СТАНДАРТЫ И АЛГОРИТМЫ
Анонимизация избирателя	«Слепая» подпись регистратора. Поддерживаемые алгоритмы и стандарты 1) RSA 4096 2) алгоритмы с эллиптическими кривыми, определенные в Р 50.1.114-2016
Распределение ключа и генерация ключа шифрования	ГОСТ Р 34.12-2015 Распределение ключа между держателями по схеме Шамира
Шифрование бюллетеня на стороне избирателя	Зашифрование данных по схеме Эль-Гамаля (на эллиптических кривых) Неинтерактивные доказательства с нулевым разглашением (NIZK)
Подпись бюллетеня на стороне избирателя	ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012
Проверка корректности данных в зашифрованных бюллетенях	Неинтерактивные доказательства с нулевым разглашением (NIZK)
Сложение зашифрованных бюллетеней	Зашифрование данных по схеме Эль-Гамаля (на эллиптических кривых) со свойствами аддитивного гомоморфизма
Распределенное расшифрование результатов голосования	Неинтерактивные доказательства с нулевым разглашением (NIZK)

Механизмы защиты от внешнего нарушителя

1. Защита каналов связи

✓ ГОСТ TLS в браузере
ГОСТ TLS в мобильном приложении

! Низкий охват среди пользователей
Нет браузеров для мобильных устройств

2. Использование стойких алгоритмов, стандартизированных в РФ

✓ ГОСТ TLS Подпись ГОСТ Р 34.10-2012
Эллиптические кривые
Схема разделения ключа Шамира

! Схема подписи вслепую (в процессе)
Схема гомоморфного шифрования Эль-Гамаля
Доказательства с нулевым разглашением

3. Защита от агитации - ZKP до записи в блокчейн

Основные подходы к защите от внутреннего нарушителя

1

Разделение на логические и физические сегменты

2

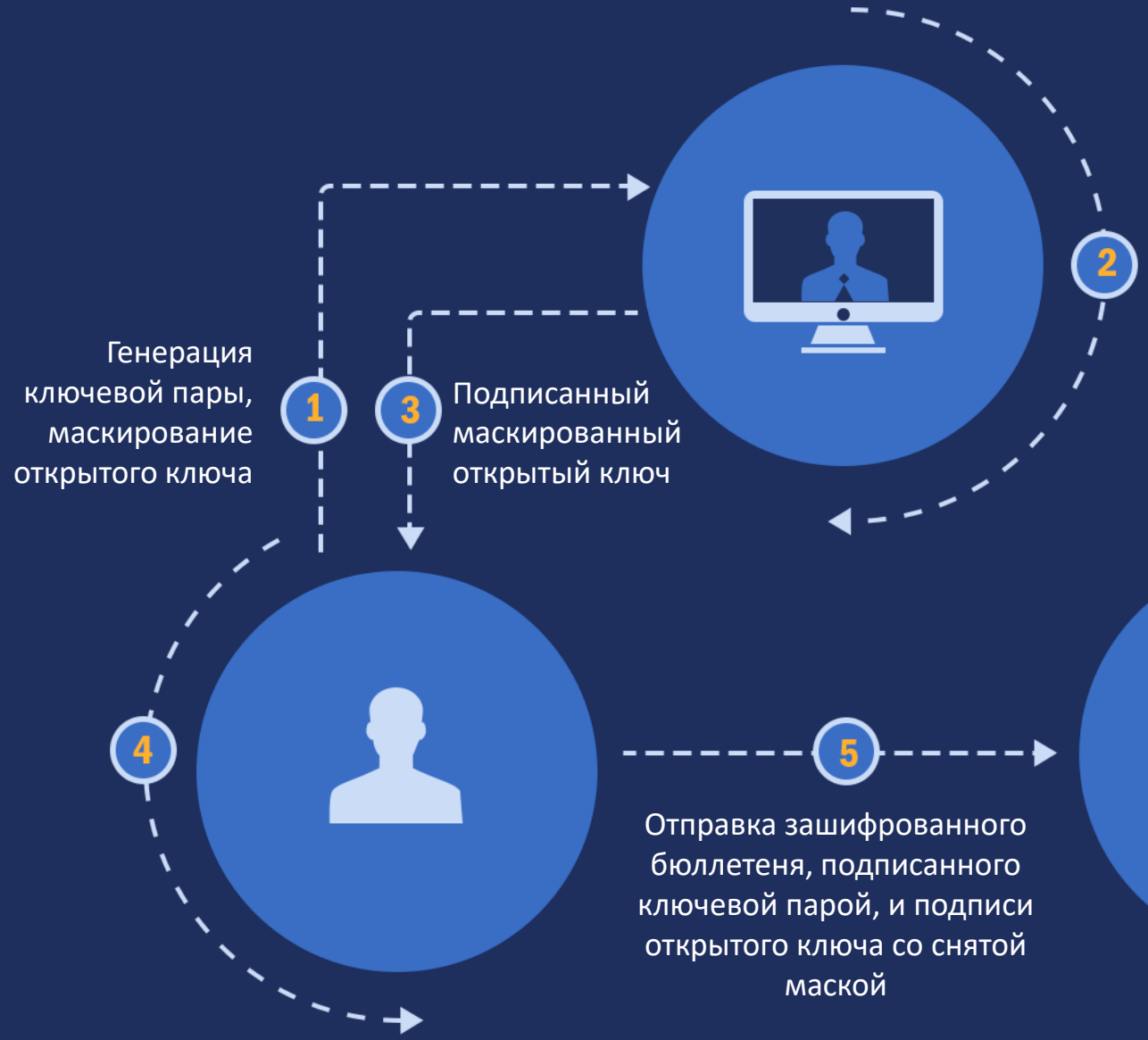
Анонимизация по алгоритму подпись «вслепую» для каждого бюллетеня

3

Операции над зашифрованными данными

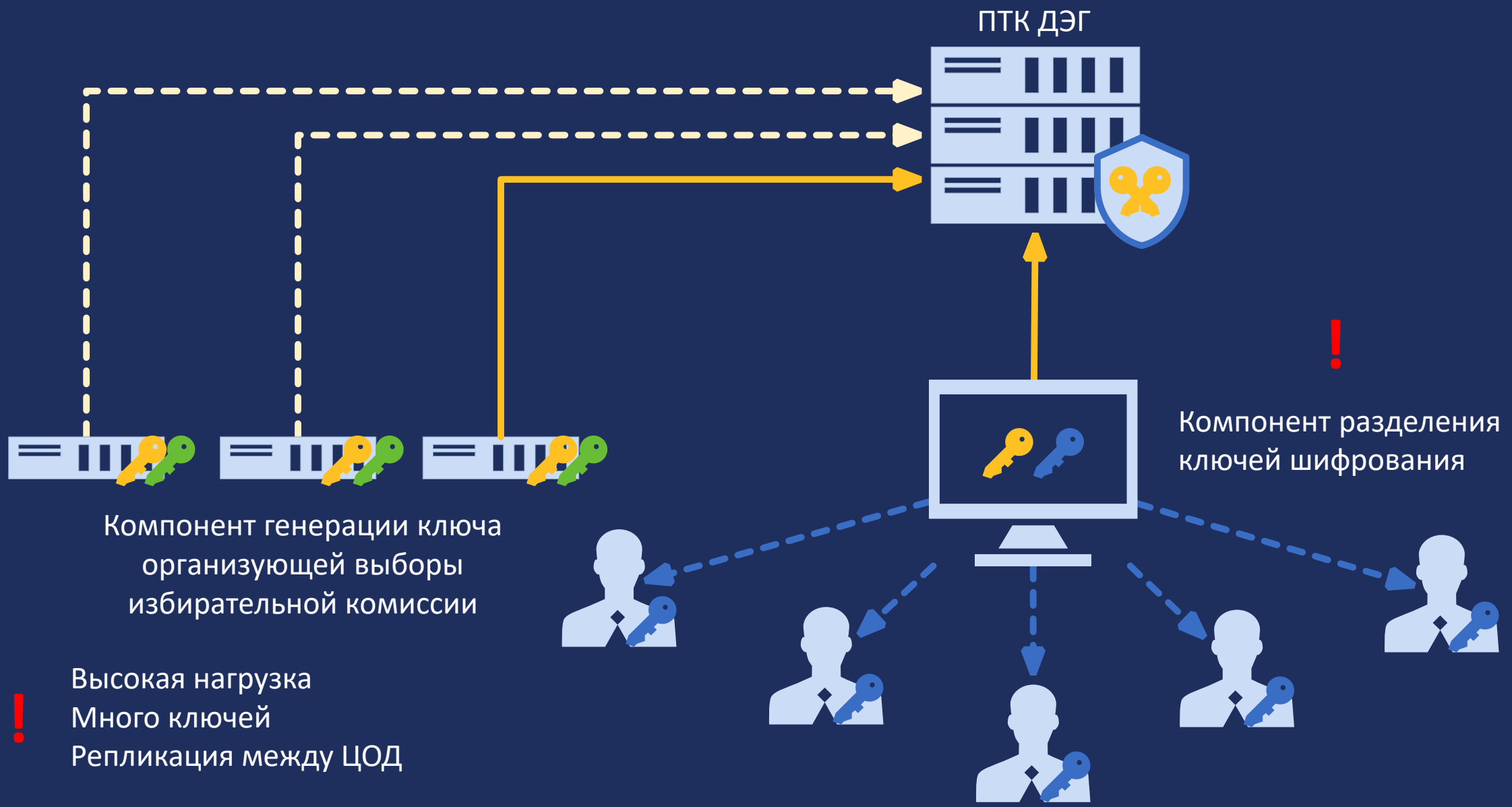
Расшифровка суммированных данных

Анонимизация и подпись «вслепую»



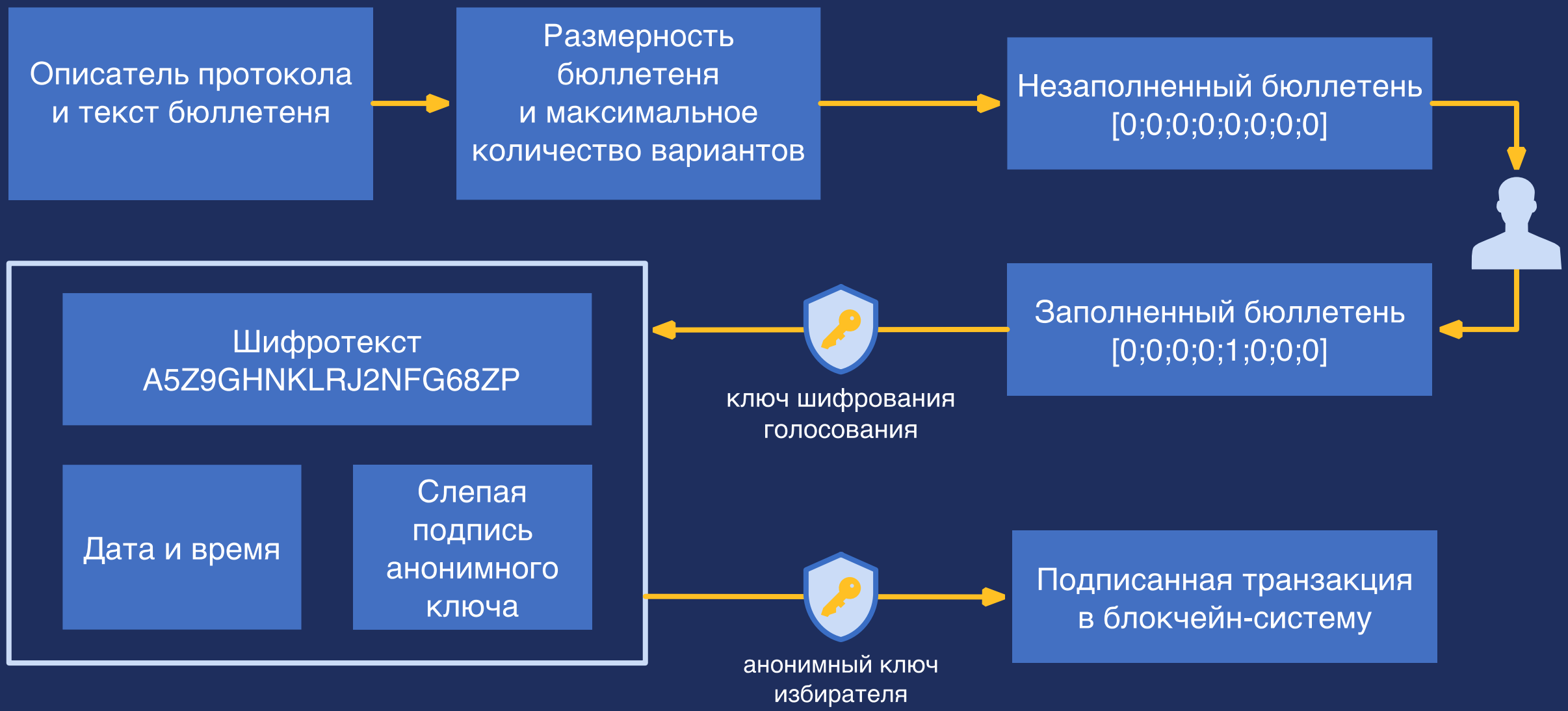
! Публикация в блокчейн факта выдачи с HMAC для аудита

Создание ключевой пары для шифрования результатов

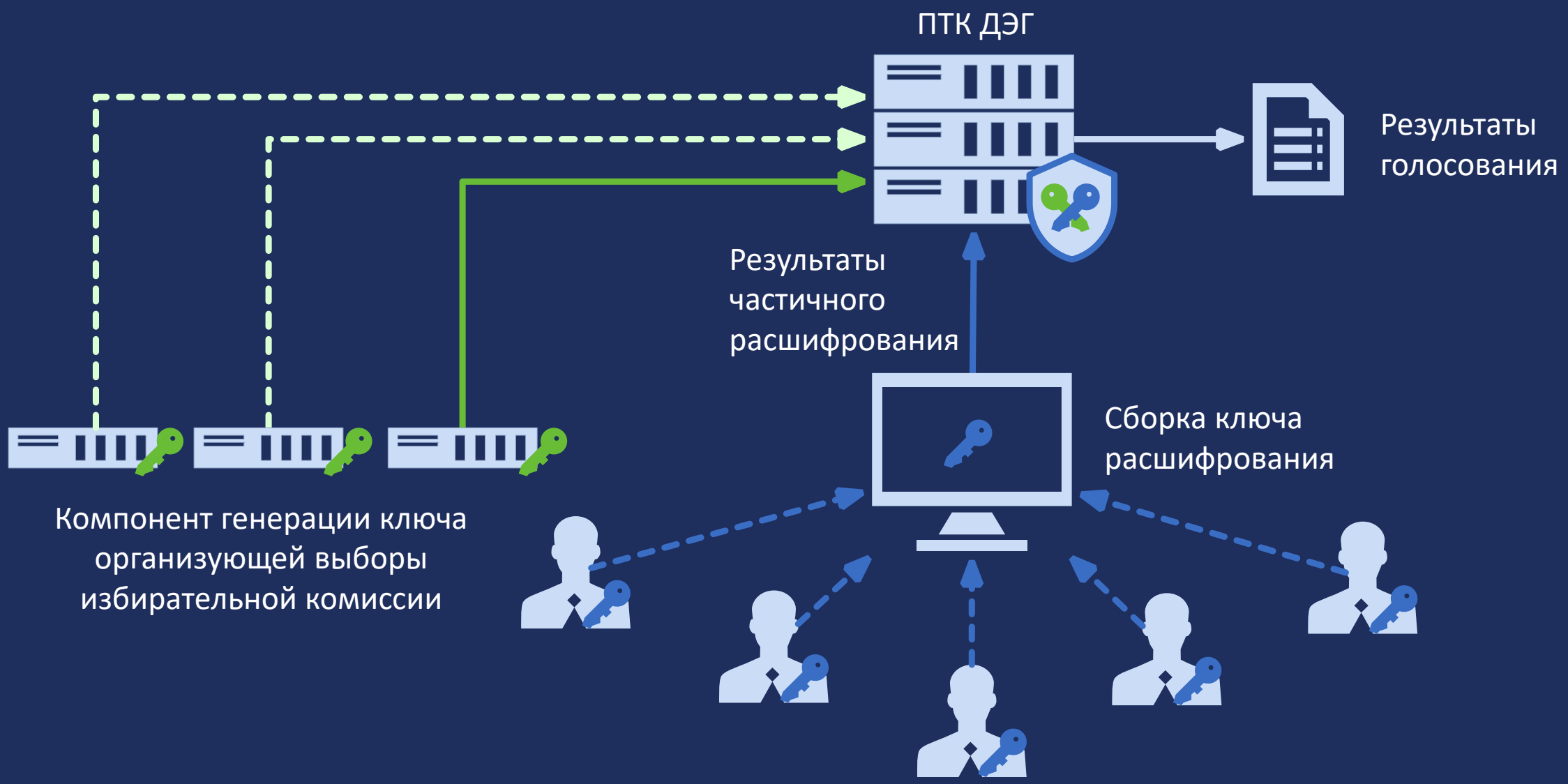


Высокая нагрузка
Много ключей
Репликация между ЦОД

Электронный бюллетень ПТК ДЭГ



Завершение голосования и подсчет результатов голосования



Подсчет результатов