Дистанционное электронное голосование

Основные архитектурные подходы

Как принять участие в ДЭГ

1

Сопоставление пользователей портала Госуслуг с регистром избирателей, участников референдума

2

Подача заявлений для участия в дистанционном электронном голосовании на портале Госуслуг со 2 августа 2021 года до 23:59 13 сентября 2021

3

Обработка заявлений для участия в дистанционном электронном голосовании и рассылка результатов обработки

4

Дистанционное электронное голосование на портале ДЭГ с 08:00 17 сентября до 20:00 19 сентября 2021 года

Портал ДЭГ

Портал голосования vybory.gov.ru – основная точка контакта с участниками ДЭГ

Дистанционная идентификация и аутентификация участников ДЭГ

Информация о доступных голосованиях и порядке проведения дистанционного голосования

Основные подходы ПТК ДЭГ

1

Разделение на логические и физические сегменты

2

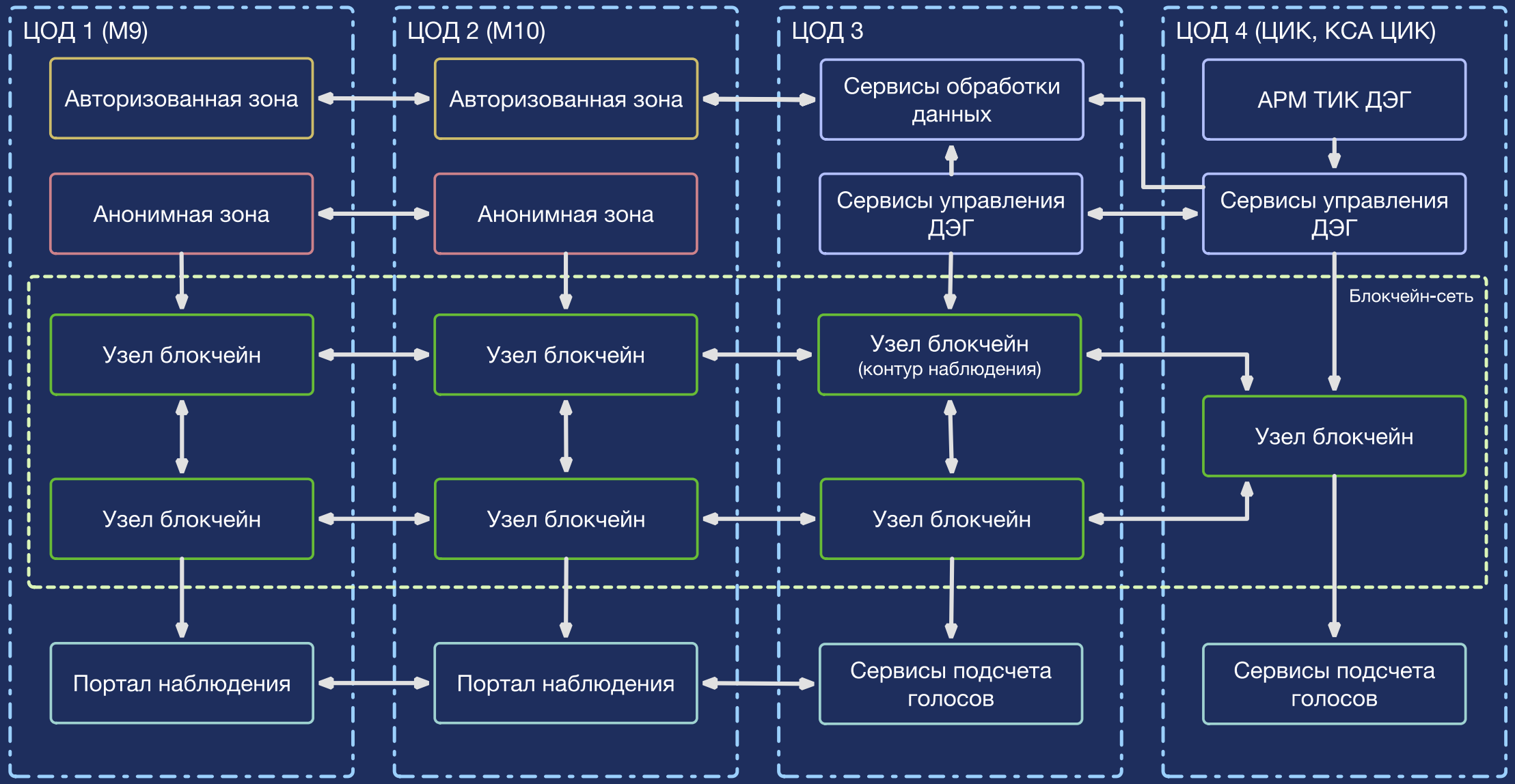
Анонимизация по алгоритму подпись «вслепую» для каждого бюллетеня

3

Операции над зашифрованными данными

Расшифровка суммированных данных

Инфраструктурная схема ПТК ДЭГ



Компоненты программно-технического комплекса ДЭГ

1

Портал ДЭГ

Позволяет пользователям получить информацию о доступных для них голосованиях и о завершенных голосованиях с их участием, а также информацию о порядке проведения дистанционного голосования. Интеграция с внешними системами ЕСИА, Единой биометрической системой и СМС-шлюзом мобильных операторов обеспечивает дистанционную идентификацию и аутентификацию участников ДЭГ

2

Анонимная зона Портала ДЭГ

Предназначена для проверки прав доступа к бюллетеню анонимного пользователя, отображения бюллетеня в анонимной зоне, фиксации волеизъявления участника ДЭГ и отправки зашифрованного и подписанного на устройстве пользователя бюллетеня в блокчейн-платформу

3

Портал наблюдения

Отображает статистические сведения о ходе дистанционного электронного голосования на определенные моменты времени, демонстрирует неизменность хранения результатов волеизъявления участников ДЭГ, транзакции, записываемые в блокчейн

4

Список участников ДЭГ

Обеспечивает возможность загрузки и хранения списков избирателей, обладающих правом на участие в общероссийской тренировке системы дистанционного электронного голосования, а также данные участников ДЭГ, необходимые для сопоставления при идентификации и аутентификации.
Проверка всех идентификационных данных и подписание «слепой подписью» открытого ключа участника ДЭГ, которая будет проверяться сервисом голосования при приеме бюллетеня, а также перевод участника ДЭГ в анонимную зону портала ДЭГ для осуществления волеизъявления

5

Организация и проведение ДЭГ

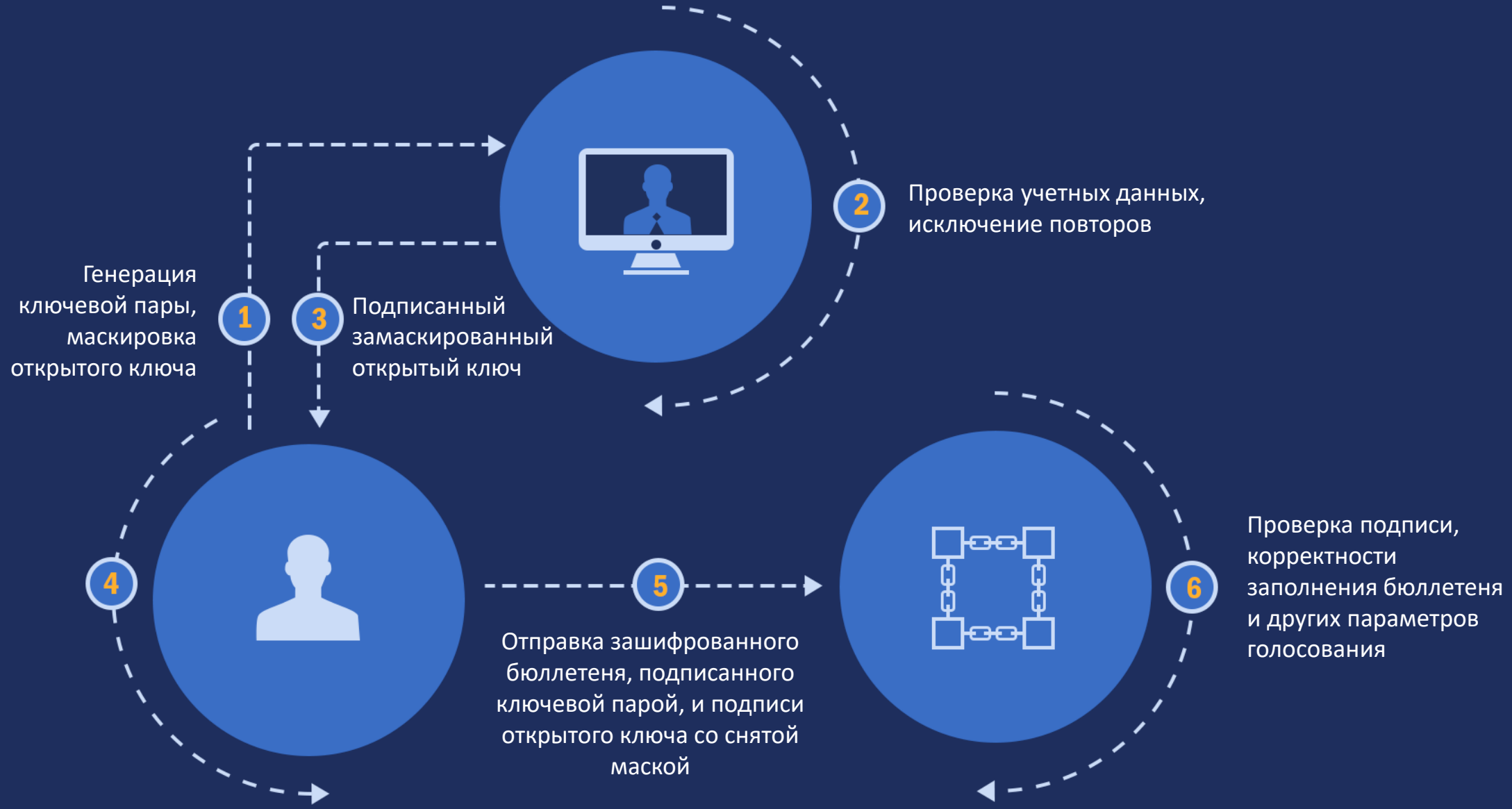
Обеспечивает автоматизацию:
– процессов работы с голосованием (открытие/закрытие/подсчет результатов голосования/формирование протоколов);
– процессов работы со списком участников ДЭГ;
– процессов, связанных с получением статистических отчётов в ходе дистанционного электронного голосования

6

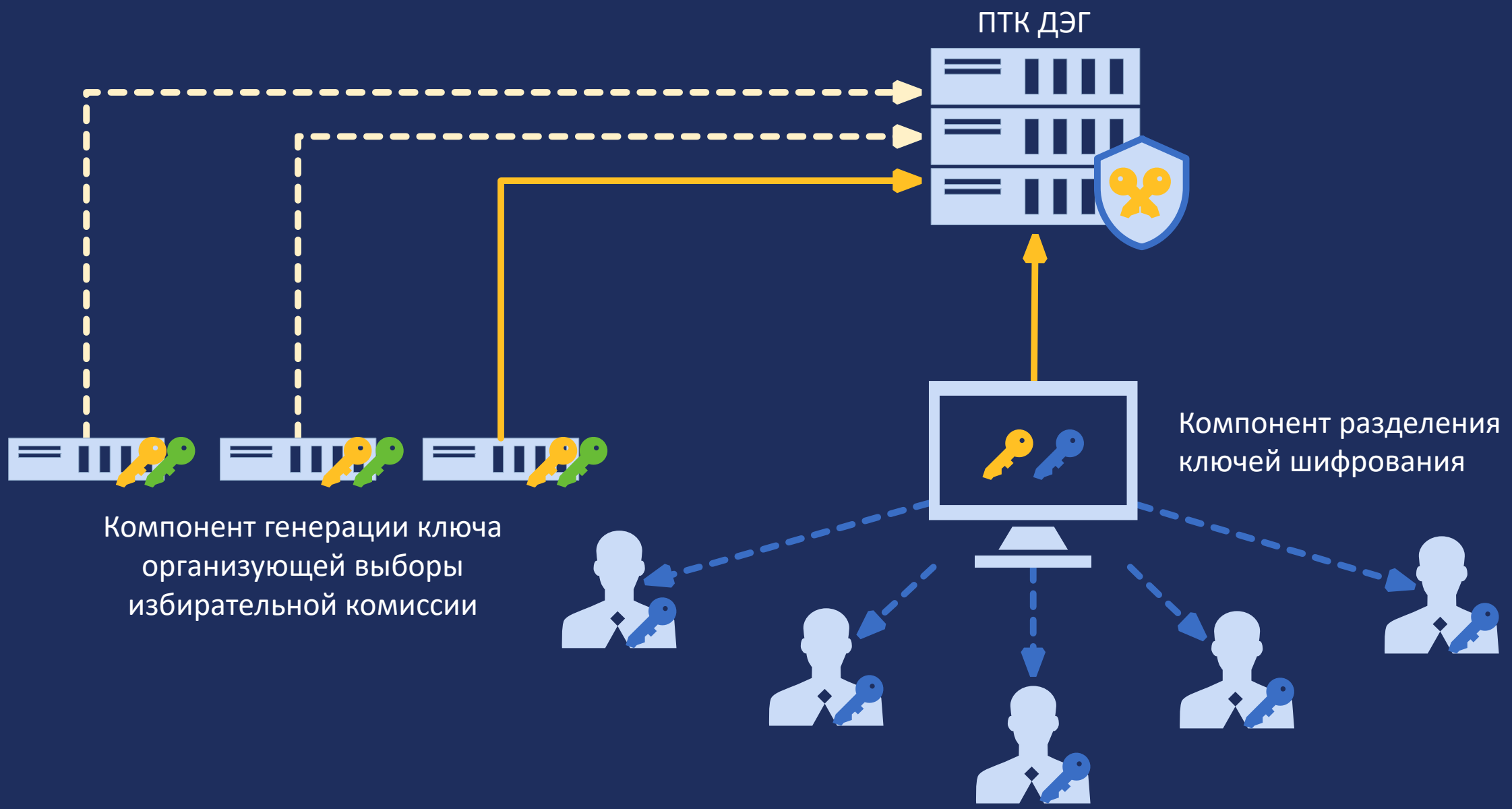
Распределенное хранение данных

Компонент системы, состоящий из набора независимых узлов, обеспечивающий:
– обмен информацией между децентрализованными компонентами ПТК ДЭГ;
– приём, проверку и хранение параметров голосования;
– приём, проверку и хранение транзакций с зашифрованными результатами волеизъявления участников ДЭГ с использованием смарт-контрактов;
– просмотр хранимой информации;
– распределенную выработку ключевой пары шифрования;
– распределенное шифрование результатов волеизъявления

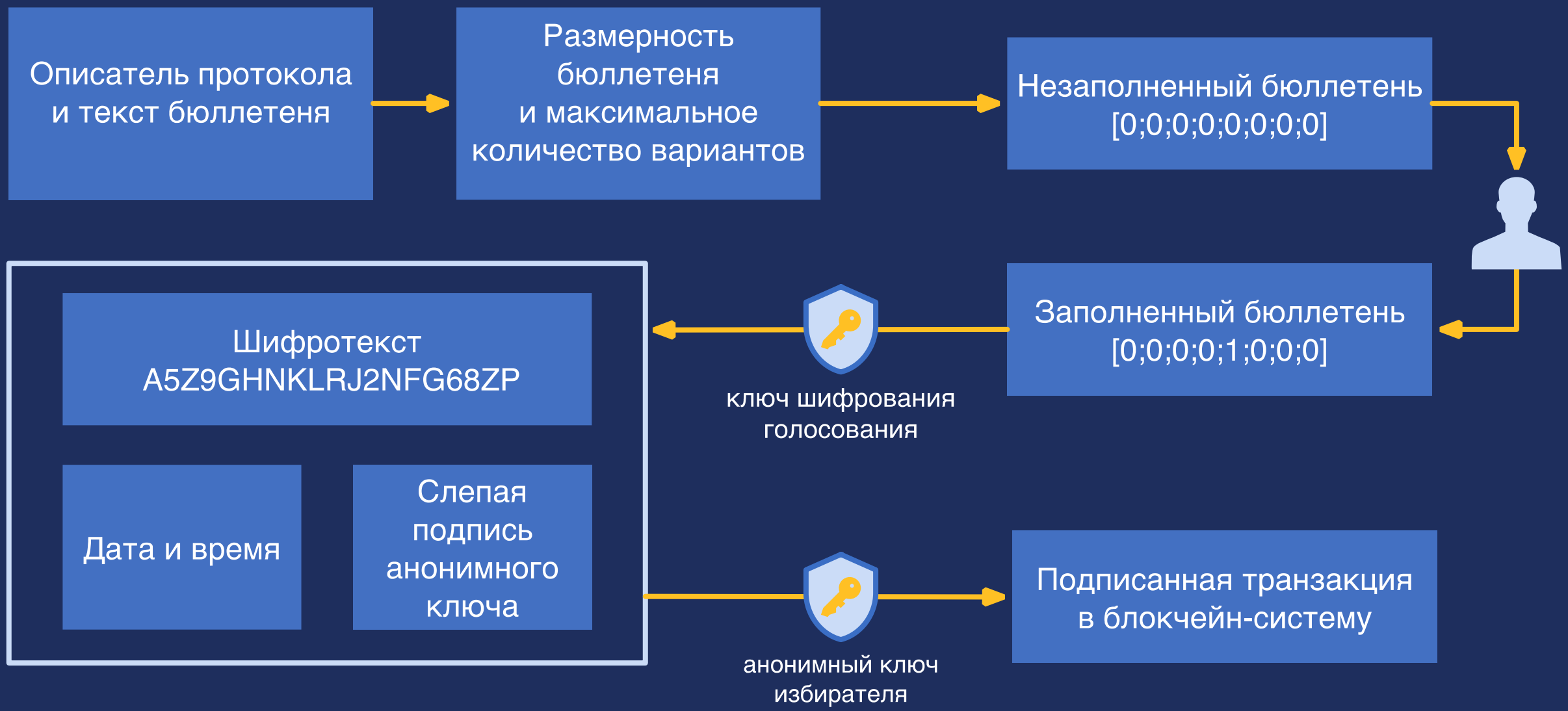
Анонимизация и «слепая подпись»



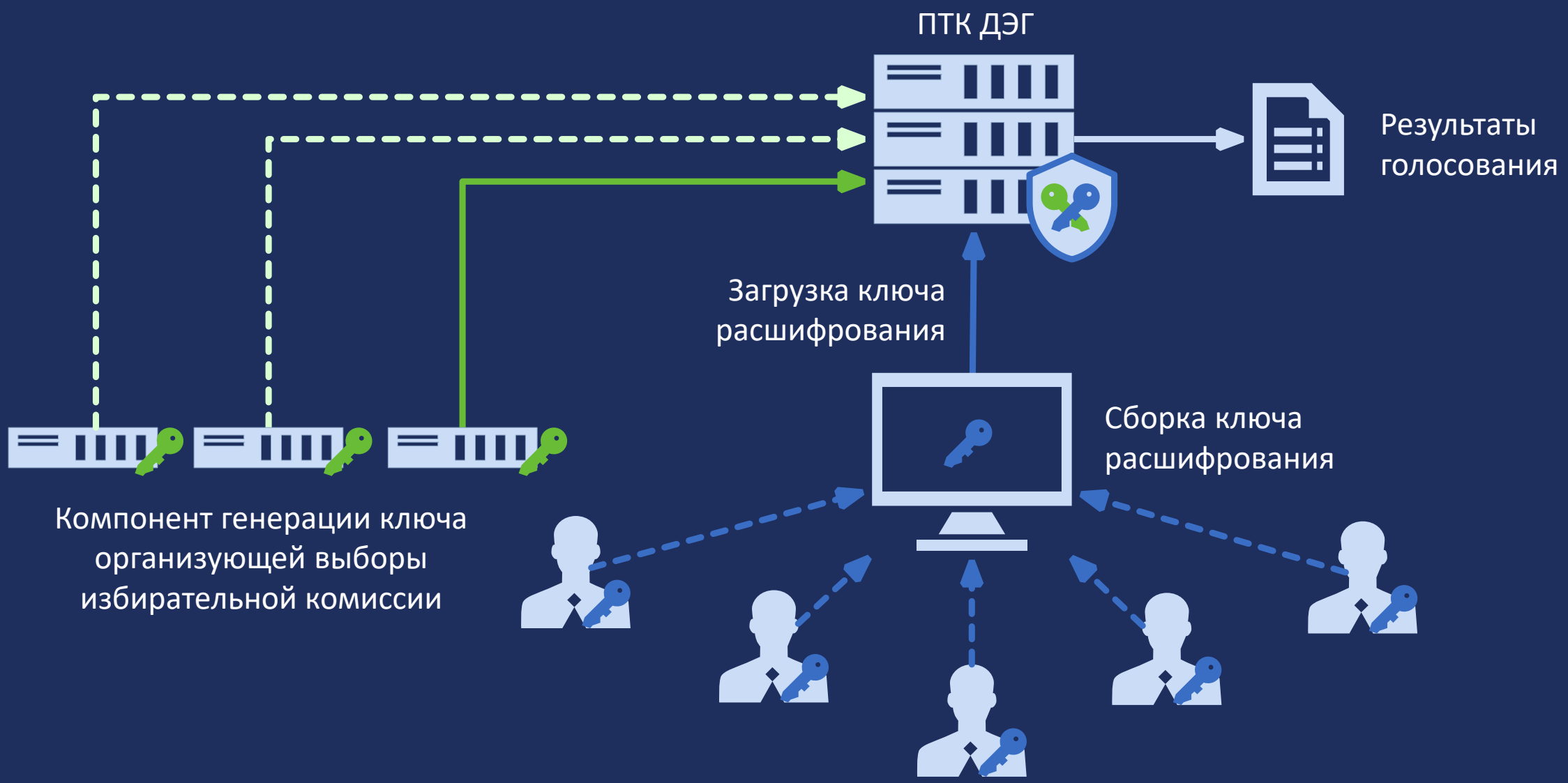
Создание ключевой пары для шифрования результатов



Электронный бюллетень ПТК ДЭГ



Завершение голосования и подсчет результатов голосования



Подсчет результатов

Основные криптографические алгоритмы

ТЕХНОЛОГИИ	СТАНДАРТЫ
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 (опционально DKG Pedersen 91) 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 свойставми аддитивного гомоморфизма
Распределенное расшифрование результатов голосования	Неинтерактивные доказательства с нулевым разглашением (NIZK)