

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Сибирский государственный университет телекоммуникаций и информатики»
Кафедра Безопасность и управление в телекоммуникациях

Разработка системы дистанционного электронного голосования

Выполнил: студент гр. АБ-66

Крылосов А.А.

Руководитель: доц. каф. БиУТ

Попков Г.В.

Новосибирск, 2021

Актуальность темы

Преимущества электронного голосования:

- Ускорение голосования
- Минимизация ошибок
- облегчение труда избирательных комиссий
- экономия бумаги и возможность оперативного изменения списков без перепечатывания всего тиража бюллетеней;
- использование многоязычных интерфейсов.

Однако, при этом возникает ряд специфических проблем:

- сомнения в истинности результатов, полученных с помощью машин;
- сложнее авторизовать избирателя;
- сложнее удостовериться, что на ход голосования никто не повлиял.

Цель выпускной квалификационной работы

Целью является разработка системы дистанционного электронного голосования, которая бы отвечала необходимым требованиям и позволяла проводить прозрачные и честные выборы.

Требования к электронному голосованию

- голосование только легитимных участников и при том, только один раз;
- тайну голосования, никто, кроме голосующего, не должен знать его выбор;
- аудит списка избирателей;
- аудит результатов голосования;
- сокрытие результатов до окончания голосования;
- решение голосующего не может быть тайно.

Виды систем голосования



Сравнение существующих систем голосования

Параметр	Бумажное	Бумажно- электронное	Электронное с прямой записью	Электронное через публ. сети
Соответствует требованиям эл. голосования	+	+	+	+
Автоматизированный подсчет голосов	-	+	+	+
Автоматизированный сбор голосов	-	-	+	+
Возможно проголосовать дистанционно	-	-	-	+

Требования к обеспечению безопасности

- В составе ПТК ДЭГ необходимо использовать сертифицированные по требованиям безопасности информации средства защиты информации средства защиты информации не ниже 4 класса и соответствующие 4 уровню доверия.
- Для ПТК ДЭГ необходимо обеспечить выполнения требований, предъявляемых к 1 (первому) классу защищенности информационных систем.
- В ПТК ДЭГ необходимо обеспечить третий уровень защищенности персональных данных при их обработке в ПТК ДЭГ (УЗ-3).

Протокол тайного голосования

Р - Сервис регистратор
У - Сервис учета голосов
Г - Голосующий
С - Сообщение

1

Р утверждает список
голосующих

2

Р утверждает список
голосующих

3

Р утверждает список
голосующих

4

Р утверждает список
голосующих

5

Р утверждает список
голосующих

6

Р утверждает список
голосующих

7

Р утверждает список
голосующих

8

Р утверждает список
голосующих

9

Р утверждает список
голосующих

Протокол тайного голосования

Сервис регистратор (Р)

Голосующий (Г)

Сервис учета голосов (У)

Протокол тайного голосования

Сервис регистратор (Р)

Голосующий (Г)

Сервис учета голосов (У)

Шаг 1. Утверждает список
голосующих

Протокол тайного голосования

Сервис регистратор (Р)

Голосующий (Г)

Сервис учета голосов (У)

Шаг 1. Утверждает список
голосующих



Шаг 2. В создает ключи $K_{Гзак}$,
 $K_{Готк}$, $K_{Гсек}$ и выкладывает
 $K_{Готк}$

Протокол тайного голосования

Сервис регистратор (Р)

Голосующий (Г)

Сервис учета голосов (У)

Шаг 1. Утверждает список
голосующих



Шаг 2. В создает ключи $K_{Г\text{зак}}$,
 $K_{Г\text{отк}}$, $K_{Г\text{сек}}$ и выкладывает
 $K_{Г\text{отк}}$



Шаг 3. Формирует сообщение
(С), шифрует его $K_{Г\text{сек}}$,
маскирует, подписывает $K_{Г\text{зак}}$,
отправляет

Протокол тайного голосования

Сервис регистратор (Р)

Голосующий (Г)

Сервис учета голосов (У)

Шаг 1. Утверждает список голосующих



Шаг 2. В создает ключи $K_{Гзак}$, $K_{Готк}$, $K_{Гсек}$ и выкладывает $K_{Готк}$



Шаг 3. Формирует сообщение (С), шифрует его $K_{Гсек}$, маскирует, подписывает $K_{Гзак}$, отправляет



Шаг 4. V создает ключи $K_{Рзак}$, $K_{Ротк}$ выкладывает $K_{Vотк}$.

Протокол тайного голосования

Сервис регистратор (Р)

Голосующий (Г)

Сервис учета голосов (У)

Шаг 1. Утверждает список голосующих

Шаг 2. В создает ключи $K_{Гзак}$, $K_{Готк}$, $K_{Гсек}$ и выкладывает $K_{Готк}$

Шаг 4. V создает ключи $K_{Рзак}$, $K_{Ротк}$ выкладывает $K_{Vотк}$.

Шаг 3. Формирует сообщение (С), шифрует его $K_{Гсек}$, маскирует, подписывает $K_{Гзак}$, отправляет

Шаг 5. Удостоверяется, что С принадлежит Г, который еще не голосовал, подписывает $K_{Vзак}$, отправляет.

Протокол тайного голосования

Сервис регистратор (Р)

Голосующий (Г)

Сервис учета голосов (У)

Шаг 1. Утверждает список голосующих

Шаг 2. В создает ключи $K_{Гзак}$, $K_{Готк}$, $K_{Гсек}$ и выкладывает $K_{Готк}$

Шаг 4. V создает ключи $K_{Рзак}$, $K_{Ротк}$ выкладывает $K_{Vотк}$.

Шаг 3. Формирует сообщение (С), шифрует его $K_{Гсек}$, маскирует, подписывает $K_{Гзак}$, отправляет

Шаг 5. Удостоверяется, что С принадлежит Г, который еще не голосовал, подписывает $K_{Vзак}$, отправляет.

Шаг 6. Удаляет слой маскирующего шифрования и отправляет

Протокол тайного голосования

Сервис регистратор (Р)

Голосующий (Г)

Сервис учета голосов (У)

Шаг 1. Утверждает список голосующих

Шаг 2. В создает ключи $K_{Гзак}$, $K_{Готк}$, $K_{Гсек}$ и выкладывает $K_{Готк}$

Шаг 4. V создает ключи $K_{Рзак}$, $K_{Ротк}$ выкладывает $K_{Vотк}$.

Шаг 3. Формирует сообщение (С), шифрует его $K_{Гсек}$, маскирует, подписывает $K_{Гзак}$, отправляет

Шаг 5. Удостоверяется, что С принадлежит Г, который еще не голосовал, подписывает $K_{Vзак}$, отправляет.

Шаг 6. Удаляет слой маскирующего шифрования и отправляет

Шаг 7. Проверяет подписи Р и Г и помещает зашифрованный С в специальный список

Протокол тайного голосования

Сервис регистратор (Р)

Голосующий (Г)

Сервис учета голосов (У)

Шаг 1. Утверждает список голосующих

Шаг 2. В создает ключи $K_{Гзак}$, $K_{Готк}$, $K_{Гсек}$ и выкладывает $K_{Готк}$

Шаг 4. V создает ключи $K_{Рзак}$, $K_{Ротк}$ выкладывает $K_{Vотк}$.

Шаг 3. Формирует сообщение (С), шифрует его $K_{Гсек}$, маскирует, подписывает $K_{Гзак}$, отправляет

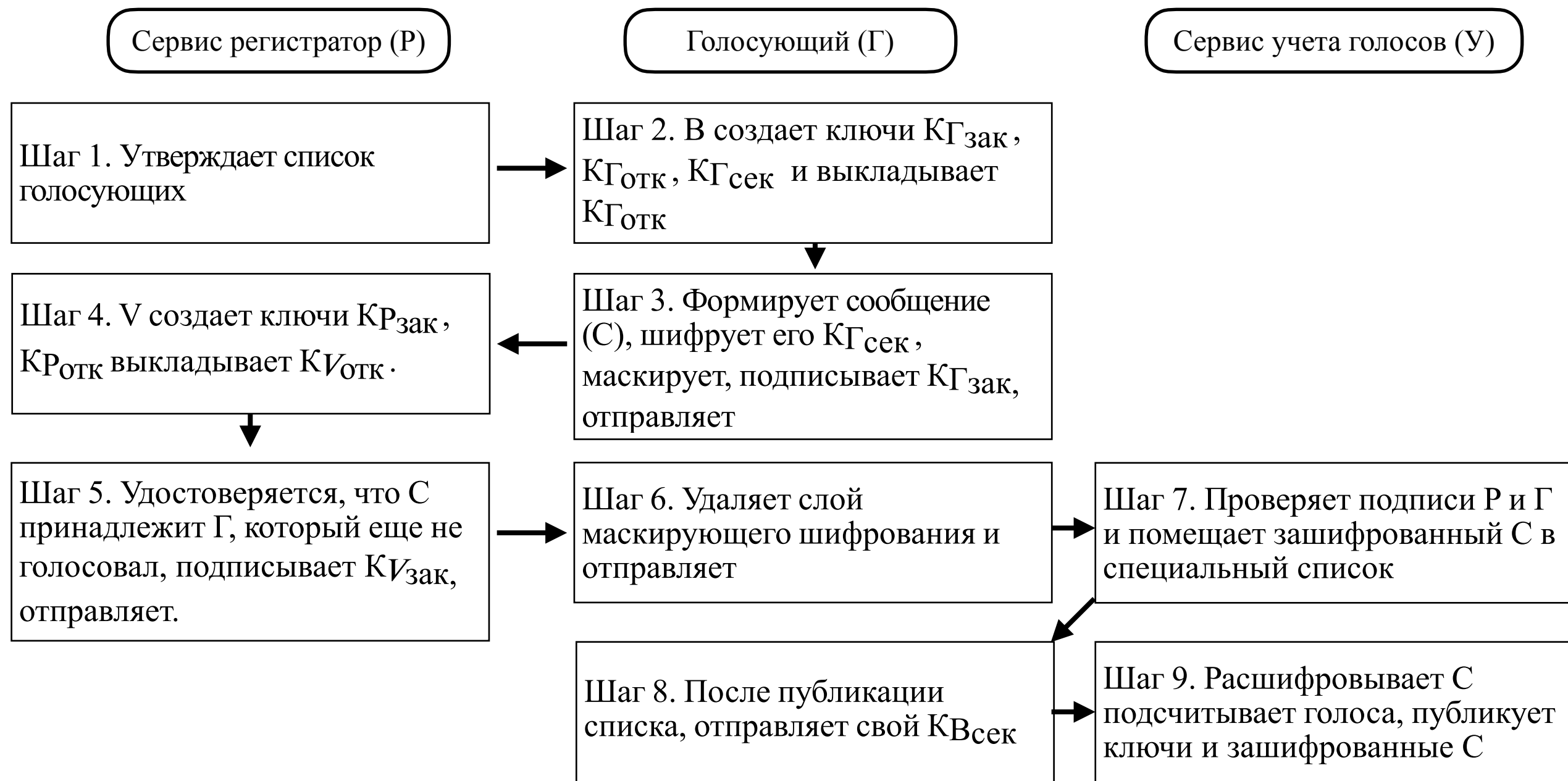
Шаг 5. Удостоверяется, что С принадлежит Г, который еще не голосовал, подписывает $K_{Vзак}$, отправляет.

Шаг 6. Удаляет слой маскирующего шифрования и отправляет

Шаг 7. Проверяет подписи Р и Г и помещает зашифрованный С в специальный список

Шаг 8. После публикации списка, отправляет свой $K_{Всек}$

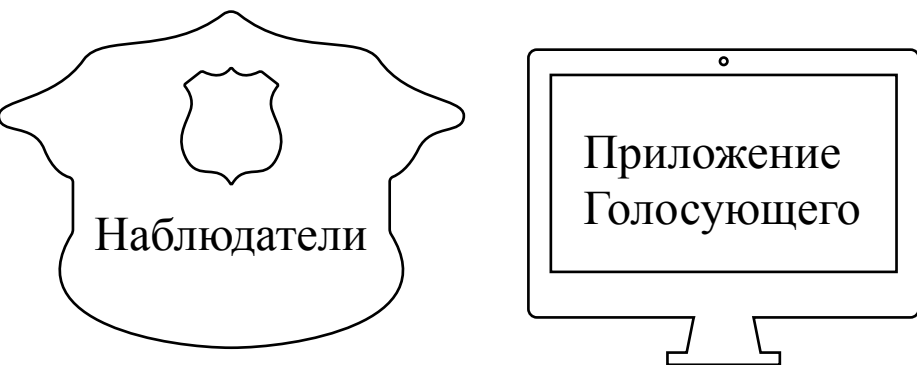
Протокол тайного голосования



Концепция модулей системы голосования



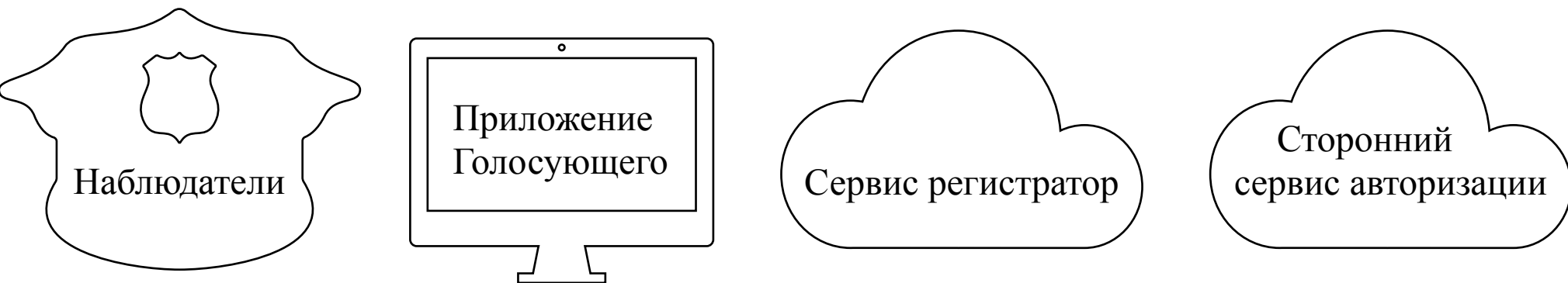
Концепция модулей системы голосования



Концепция модулей системы голосования



Концепция модулей системы голосования



Концепция модулей системы голосования



Концепция модулей системы голосования

Этап: авторизация



Концепция модулей системы голосования

Этап: авторизация



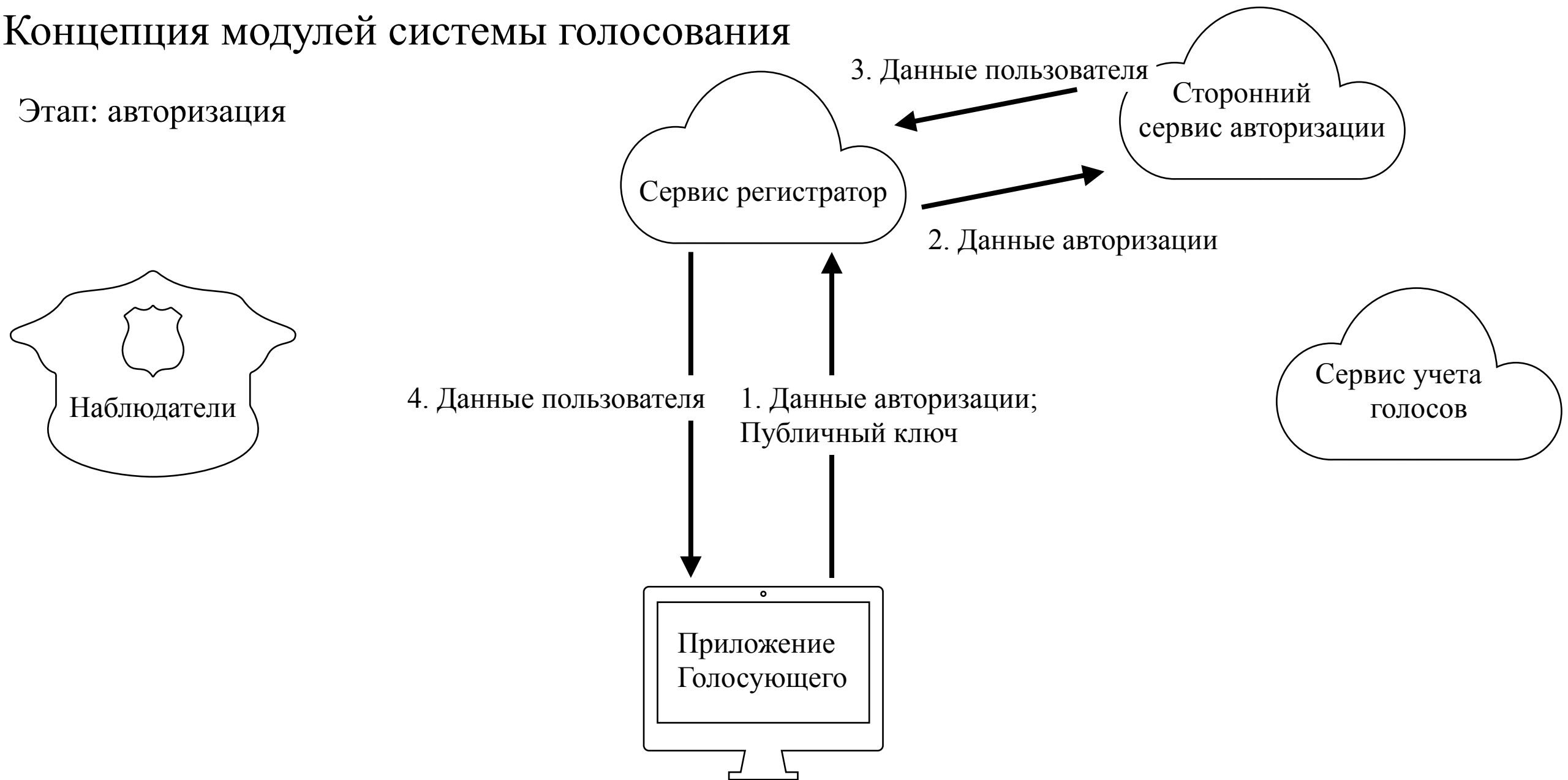
Концепция модулей системы голосования

Этап: авторизация



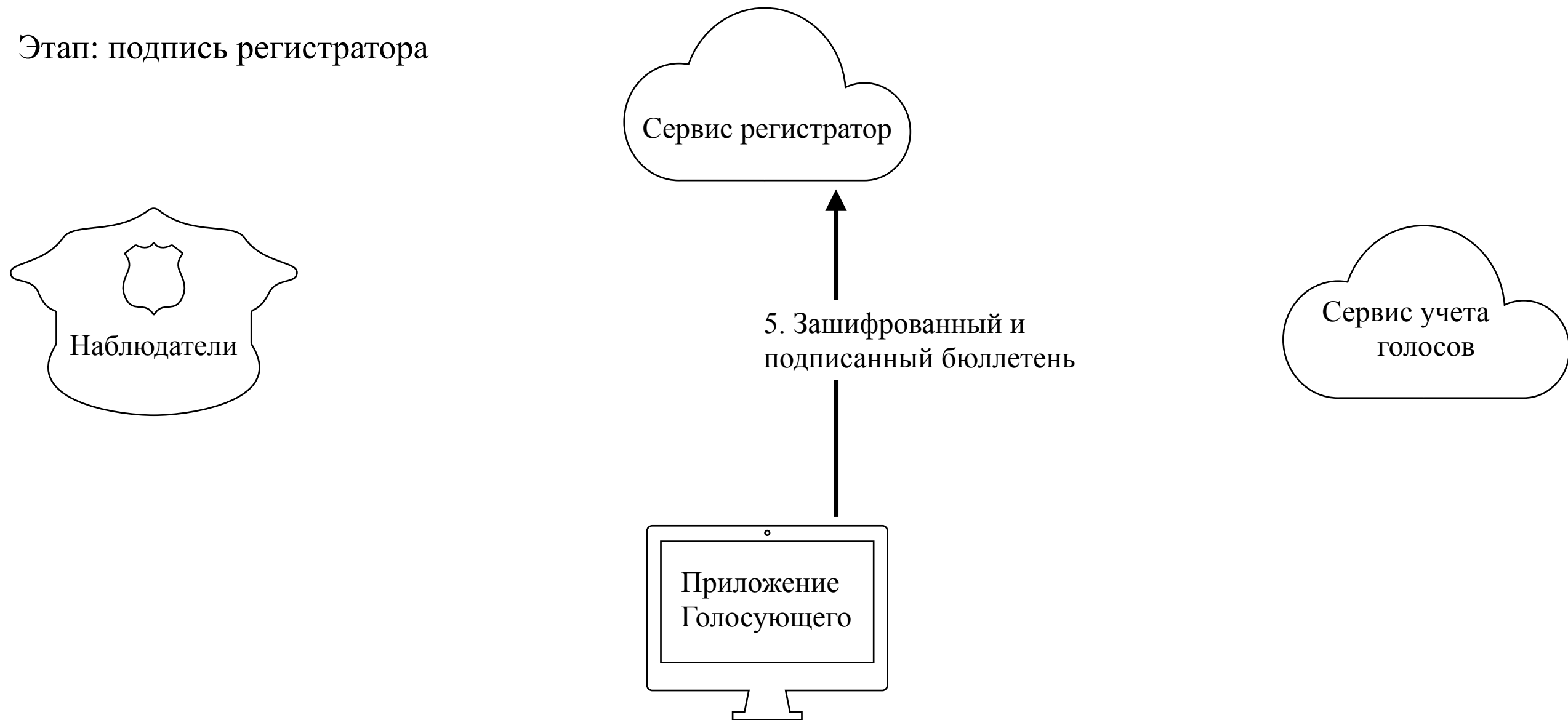
Концепция модулей системы голосования

Этап: авторизация



Концепция модулей системы голосования

Этап: подпись регистратора



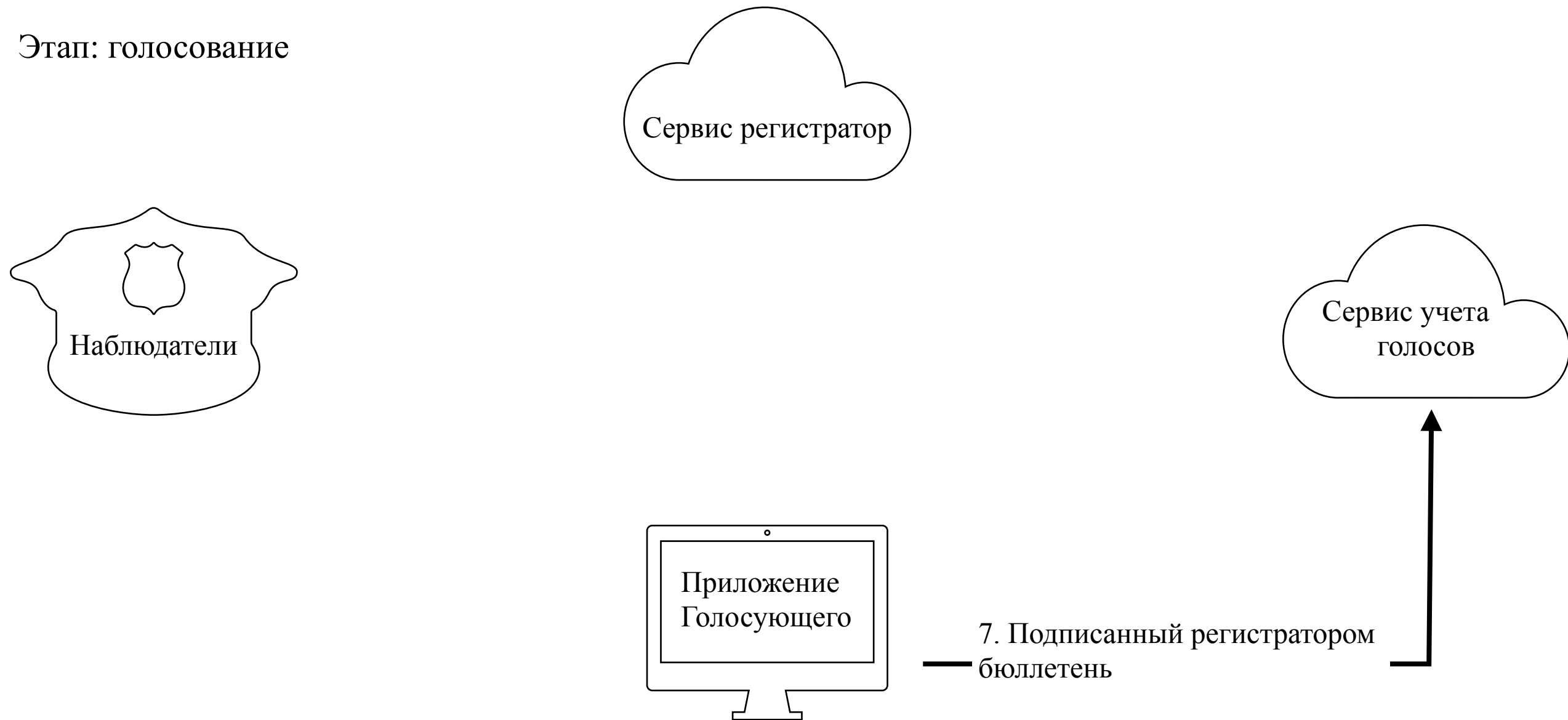
Концепция модулей системы голосования

Этап: подпись регистратора



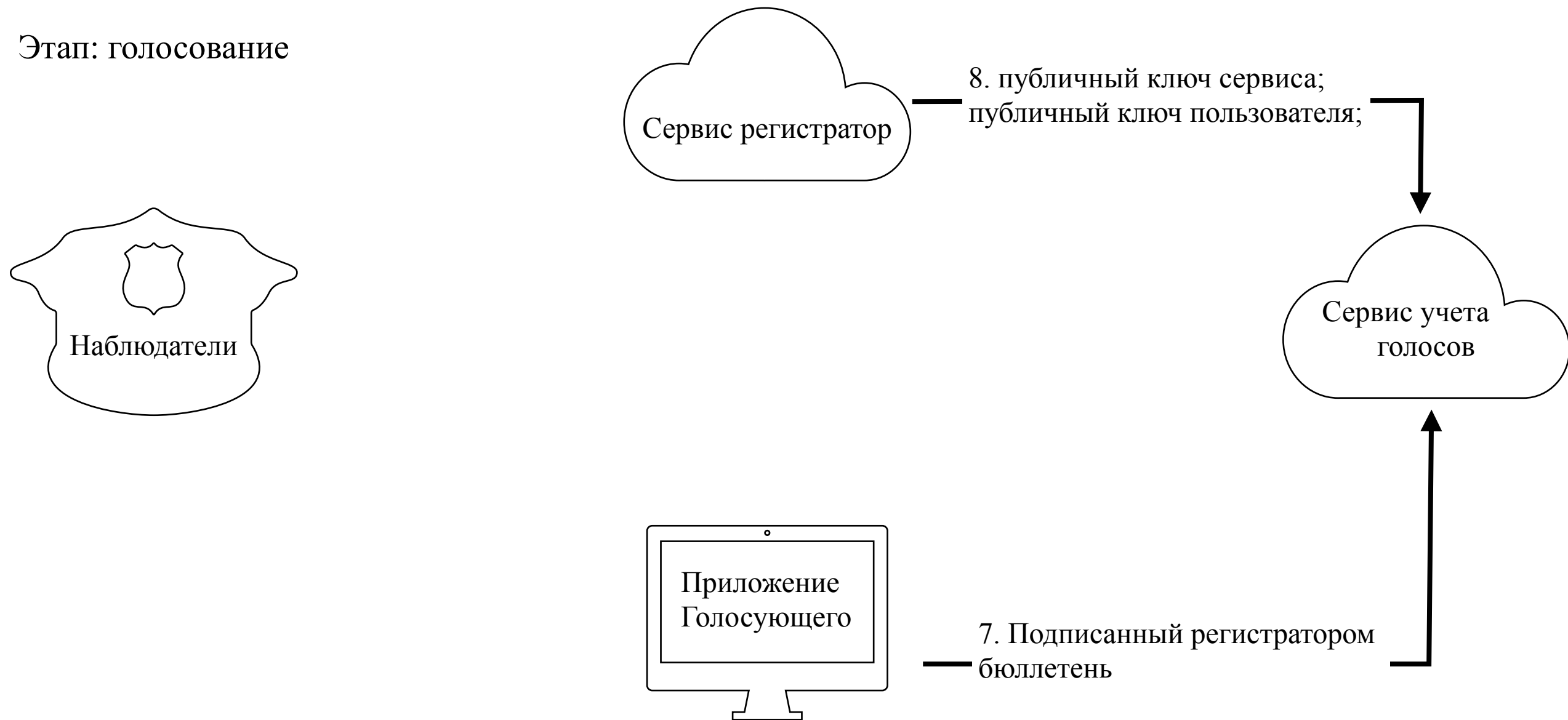
Концепция модулей системы голосования

Этап: голосование



Концепция модулей системы голосования

Этап: голосование



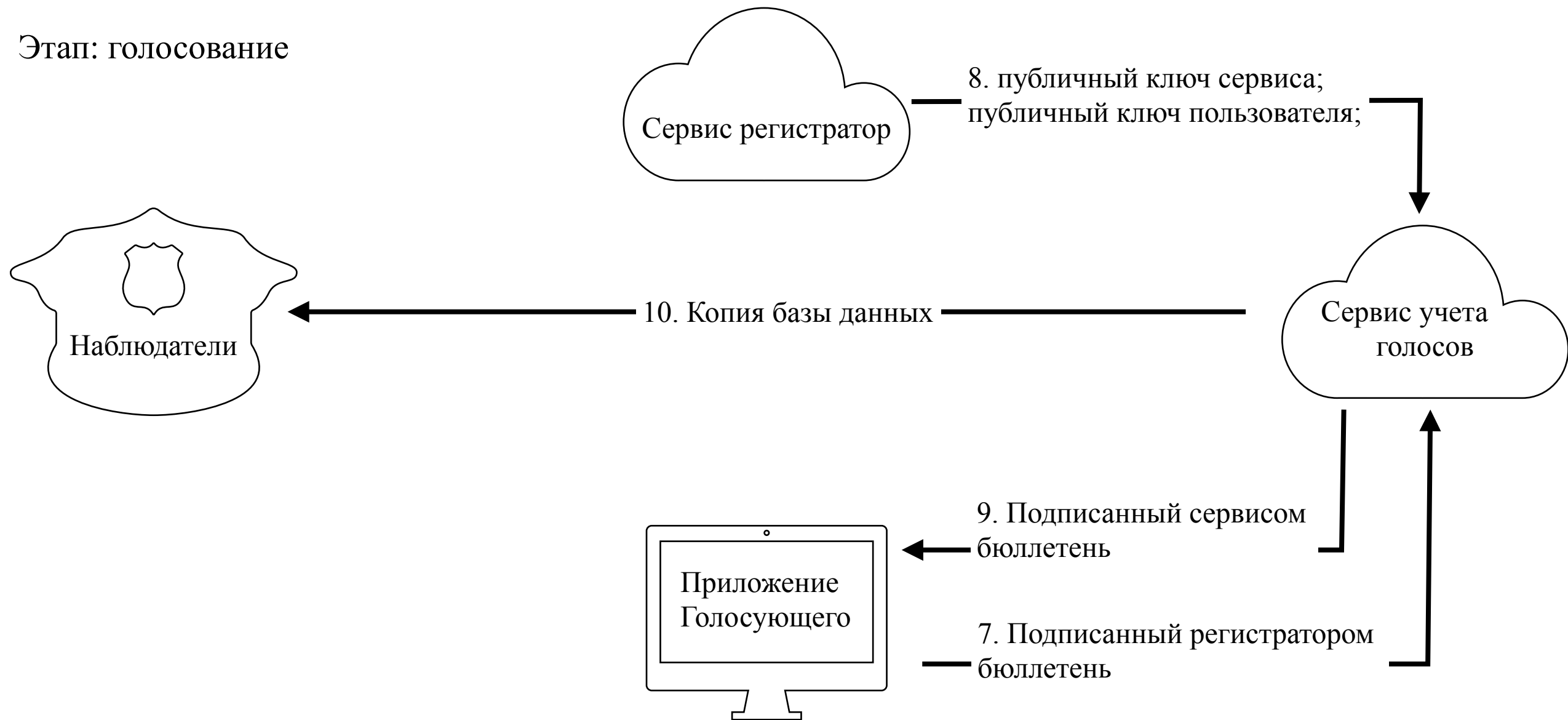
Концепция модулей системы голосования

Этап: голосование



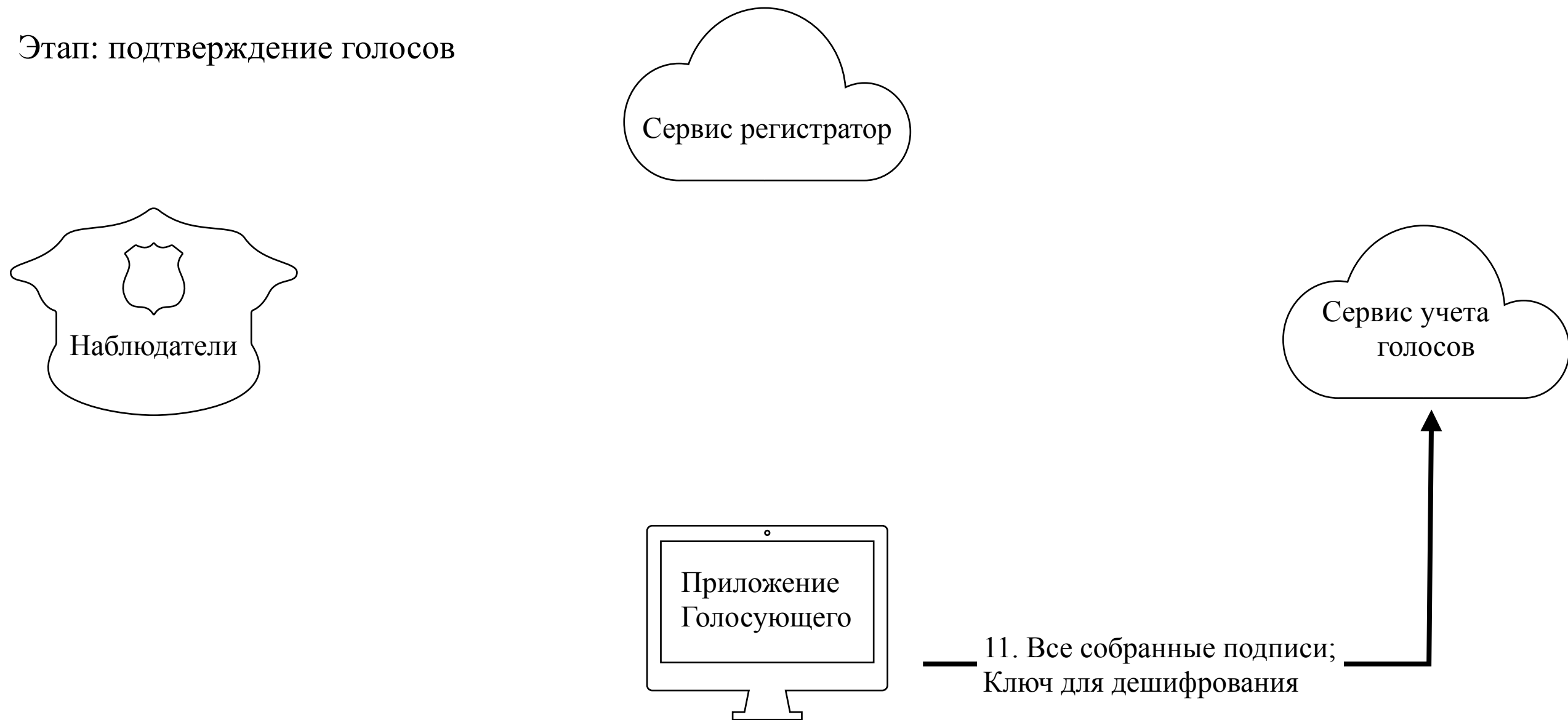
Концепция модулей системы голосования

Этап: голосование



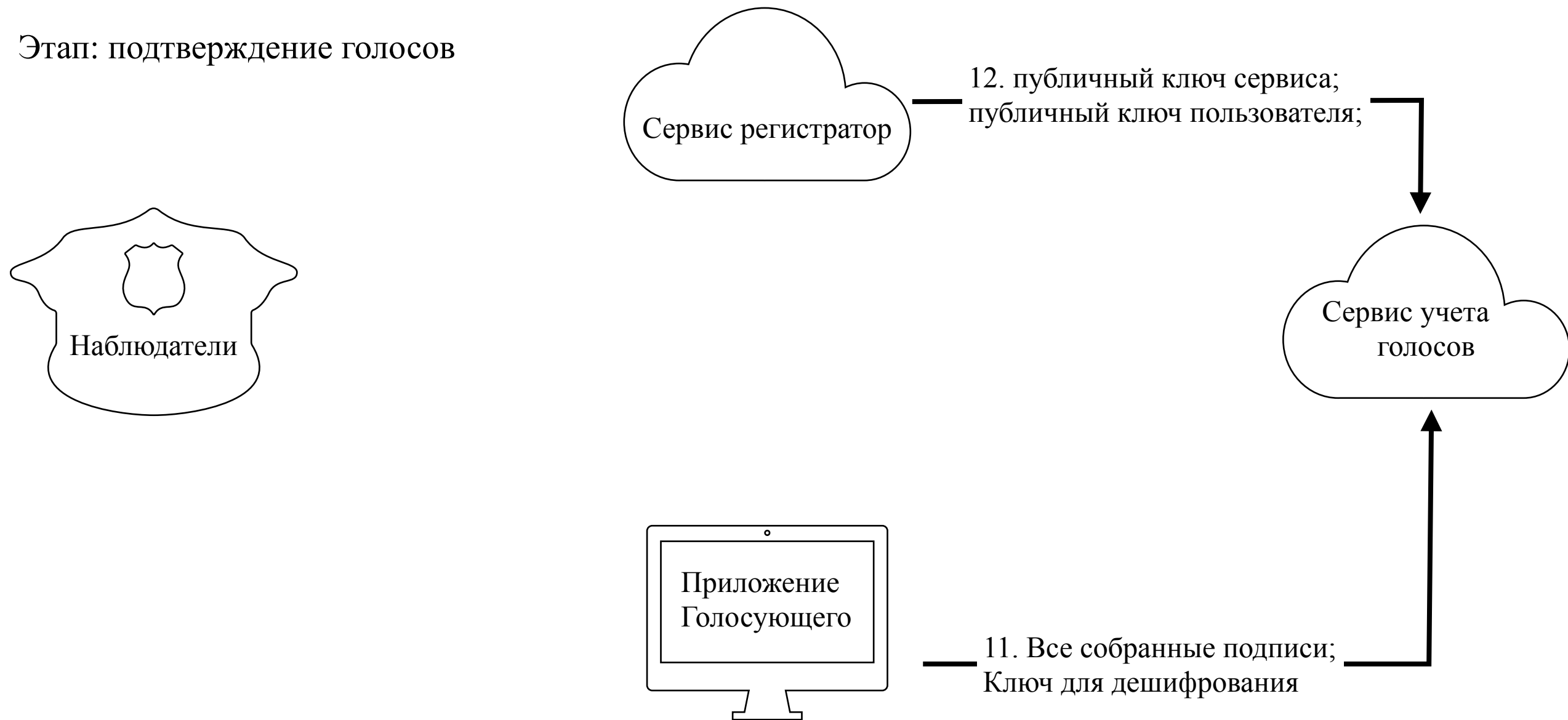
Концепция модулей системы голосования

Этап: подтверждение голосов



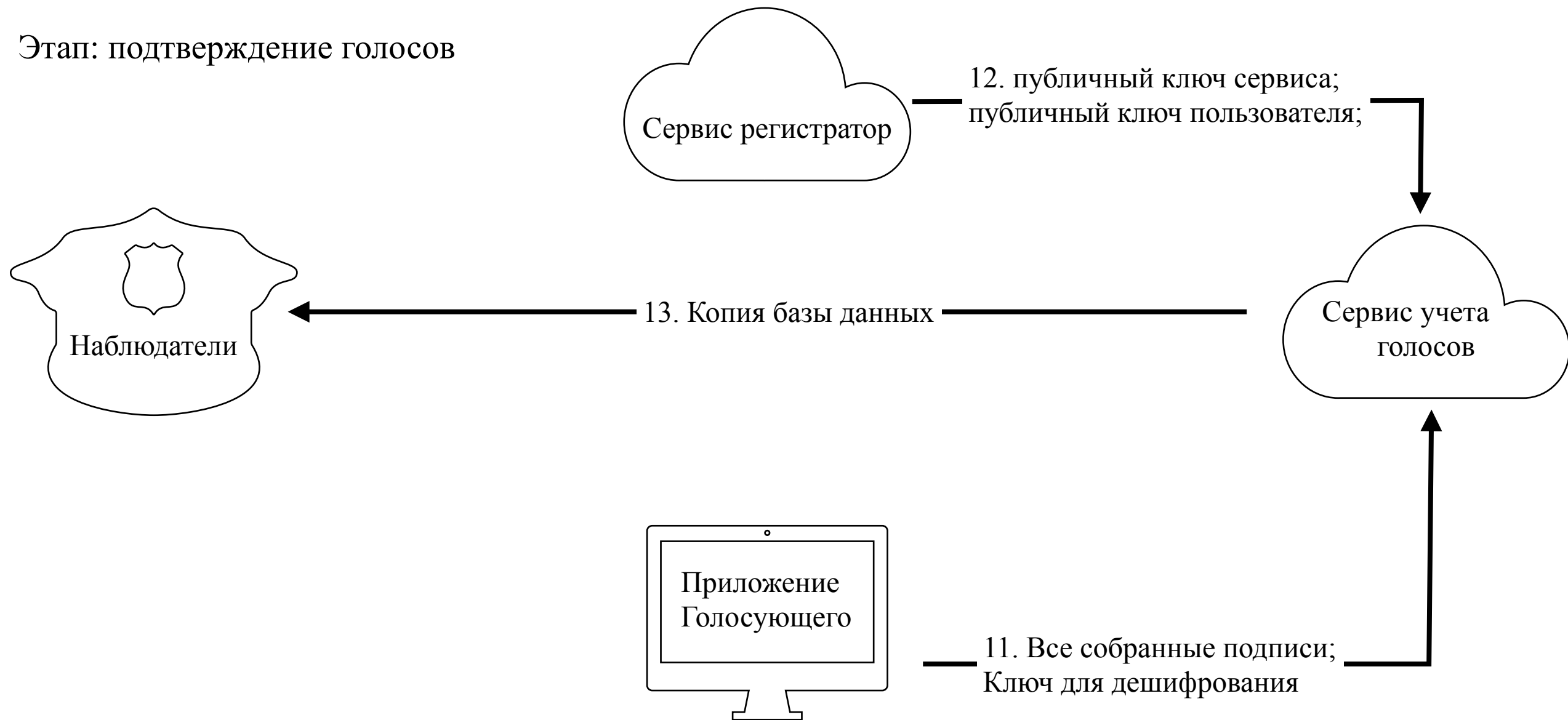
Концепция модулей системы голосования

Этап: подтверждение голосов



Концепция модулей системы голосования

Этап: подтверждение голосов











Концепция модулей системы голосования

Этап: подсчет голосов



Схема базы данных сервиса авторизации

auth			
	id	integer	 
	login	string	 
	hash_pash	string	 
 Add field			













users			
	id	integer	 
	public_key	string	 
 Add field			

Схема базы данных сервиса учета голосов

bulletins			
	id	integer	 
	secret_key	string	 
 Add field			

Интерфейс клиентского приложения

Дистанционное электронное голосование

Логин

Пароль

Войти

Дистанционное электронное голосование

Привет Андрей, сделай свой выбор!

- ☐ Вариант 1
- ☐ Вариант 2
- ☐ Вариант 3
- ☐ Вариант 4

Голосовать

Дистанционное электронное голосование

Голос за кандидата "Вариант 2" учтен!

Безопасность жизнедеятельности

- Особенности воздействия электронных систем на здоровье пользователей;
- Эргономические требования к системам отображения информации;
- Режимы труда и отдыха при работе с электронными устройствами;
- Экологические проблемы утилизации электронных гаджетов.

Технико-экономическое обоснование работы

- Разработка данного программного продукта займет около 20 дней, по себестоимости 84962,9 руб. С учетом налога на добавленную стоимость цена составит 122346,56 руб.
- При использовании разрабатываемого программного продукта происходит условная экономия денежных средств в размере 1808352 рублей в год.
- Так же выяснили, что продукт конкурентоспособен. Продукт имеет те же параметры, что и у конкурентов, а также обладает параметрами, которых у конкурентов – нет.

Заключение

- Определен объект разработки, определены требования к ДЭГ, спрогнозированы угрозы и уязвимости разрабатываемой системы и рассмотрены способы их предотвращения.
- Проработаны технические решения для разработки системы дистанционного электронного голосования. Для реализации системы дистанционного электронного голосования выберем протокол Sensus
- Разработана система дистанционного электронного голосования. Система голосования представляет собой сервер регистратор, сервер учета голосов, систему аудита и клиентское приложение.

Спасибо за внимание