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

СибГУТИ

Разработка системы дистанционного электронного голосования

Выполнил: студент гр. АБ-66
Крылосов А.А.
Руководитель: доц. каф. БиУТ
Попков Г.В.

Новосибирск, 2022

Актуальность темы

Преимущества

- Доступность
- Ускорение голосования
- Сокращение организационных затрат
- Минимизация ошибок
- Облегчение труда
- Экономия бумаги
- Многоязычные интерфейсы
- Сохранение здоровья участников

Недостатки

- Технические неисправности
- Сомнения в истинности результатов
- Сложнее авторизовать избирателя
- Сложнее удостовериться, что никто не влиял на ход голосования

Актуальность темы

Представленные системы имеют недостатки:

- Нет возможности удостовериться, что голоса не были изменены
- Нет уверенности в тайне голосования
- Один сервис, которому избиратели должны доверять
- Отсутствует или плохо работает система наблюдателей

Другие электронные системы имеют еще больше недостатков, или вообще не являются дистанционными

Цель и задачи работы

Цель:

Разработка системы дистанционного электронного голосования, которая бы отвечала необходимым требованиям и позволяла проводить прозрачные и честные выборы

Задачи:

1. определить объект разработки, составить модель угроз и нарушителя;
2. разработать техническое решение, выбрать протокол голосования;
3. написать исходный код системы электронного голосования;
4. рассмотреть вопросы безопасности жизнедеятельности;
5. выполнить технико-экономические расчеты.

Определение объекта разработки

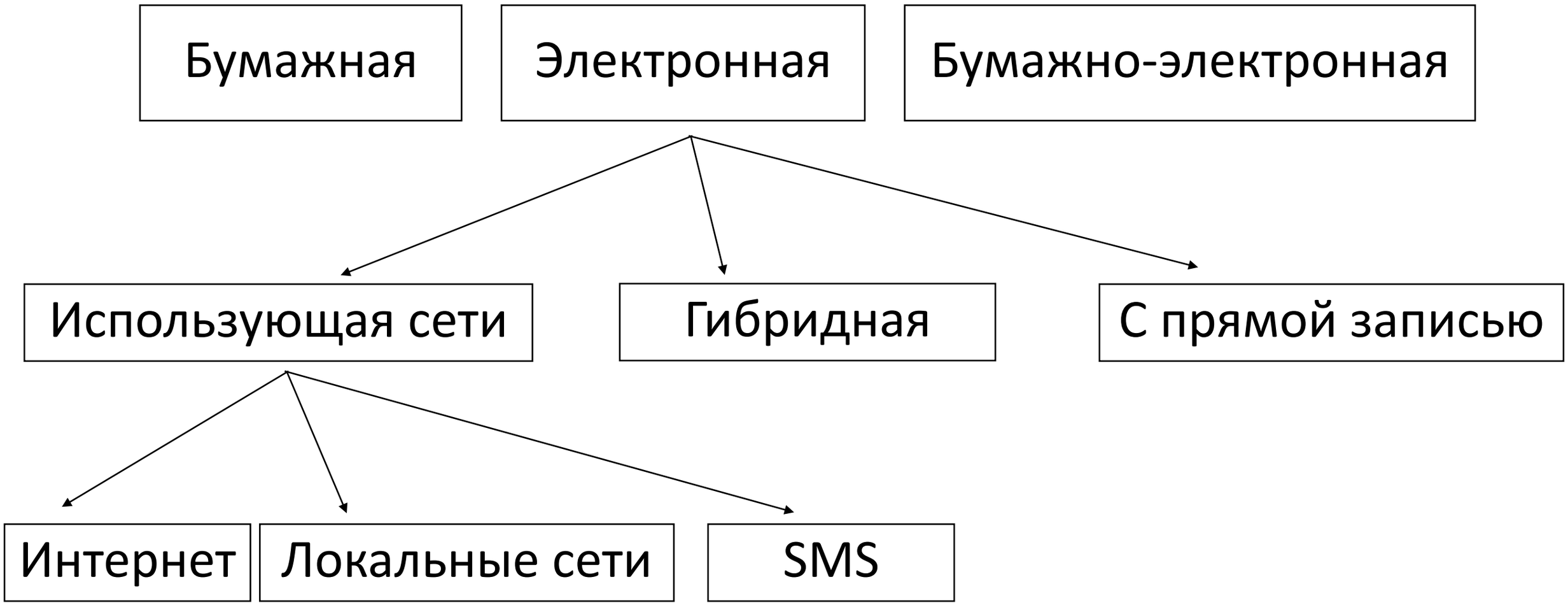
Электронное голосование – голосование без использования бюллетеня, изготовленного на бумажном носителе, с использованием комплекса средств автоматизации.

Анализ требований:

1. голосование только легитимных участников;
2. тайна голосования;
3. аудит списка избирателей;
4. аудит результатов голосования;
5. сокрытие результатов до окончания голосования;
6. решение голосующего не может быть изменено кем-то другим;
7. отказоустойчивость в случае технических неисправностей.

*Постановление ЦИК России от 27 августа 2014 года № 248/1529–6

Определение объекта разработки



* Богдан Ю.И. «Анализ существующих систем голосования» Восточно-Европейский журнал передовых технологий

Разработка модели угроз

Виды риска	Возможные последствия
Ущерб физическому лицу	Нарушение конфиденциальности (утечка) персональных данных «Травля» гражданина в сети «Интернет» Разглашение персональных данных граждан
Риски юридическому лицу, индивидуальному предпринимателю	Нарушение законодательства Российской Федерации. Нарушение штатного режима функционирования автоматизированной системы Потеря клиентов, поставщиков. Потеря конкурентного преимущества.
Ущерб государству в области обеспечения обороны страны, безопасности правопорядка, социальной, политической, сферах деятельности	Нарушение выборного процесса. Отсутствие доступа к государственной услуге. Публикация недостоверной социально значимой информации приводящая к социальной напряженности, панике среди населения и др. Доступ к системам и сетям с целью незаконного использования вычислительных мощностей. Использование веб-ресурсов государственных органов для распространения и управления вредоносным программным обеспечением. Утечка информации ограниченного доступа.

Разработка модели угроз

Рассматриваются угрозы:

1. угроза внедрения кода или данных (УБИ. 006);
2. угроза восстановления и/или повторного использования аутентификационной информации (УБИ. 008);
3. угроза использования информации идентификации/аутентификации, заданной по умолчанию (УБИ. 030);
4. угроза несанкционированного доступа к аутентификационной информации (УБИ. 074);
5. угроза несанкционированного изменения аутентификационной информации (УБИ. 086);
6. угроза обхода некорректно настроенных механизмов аутентификации (УБИ. 100);
7. угроза перехвата данных, передаваемых по вычислительной сети (УБИ. 116);
8. угроза удаления аутентификационной информации (УБИ. 152).

Разработка модели угроз

Специфичные для голосования угрозы:

1. возможность со стороны нарушителя, извлечь сведения о выборе избирателя, группы избирателей, всех избирателей, а также идентифицировать избирателя по выбору;
2. возможность реализации голосования более одного раза;
3. подмена голосов избирателей;
4. некорректная запись голоса избирателя;
5. досрочное прекращение голосования;
6. деанонимизация избирателя;
7. установление промежуточных итогов голосования до его завершения.

Разработка модели нарушителя

Виды нарушителя	Возможные цели реализации угроз безопасности информации
Специальные службы иностранных государств	Нанесение ущерба государству в области обеспечения обороны, безопасности и правопорядка, и иных областях его деятельности. Дискредитация или дестабилизация деятельности органов государственной власти, организаций, получение конкурентных преимуществ на уровне государства, срыв заключения международных договоров, создание внутриполитического кризиса.
Террористические, экстремистские группировки	Нанесение ущерба отдельным сферам деятельности или секторам экономики государства. Дестабилизация общества. Дестабилизация деятельности органов государственной власти, организаций
Преступные группы (криминальные структуры) Отдельные физические лица	Получение финансовой или иной материальной выгоды. Желание самореализации
Разработчики программных, программно-аппаратных средств	Внедрение функциональных программные аппаратные средства на этапе разработки. Получение конкурентных преимуществ. Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия

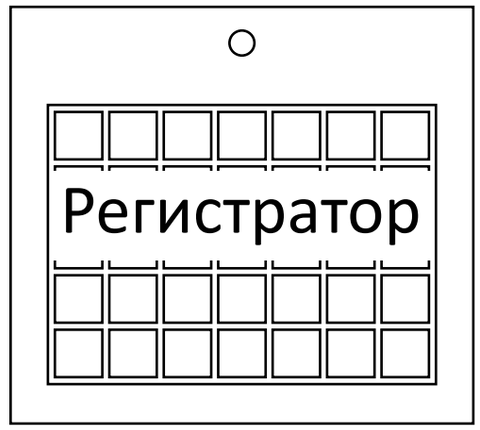
Разработка технического решения

Разработка технического решения

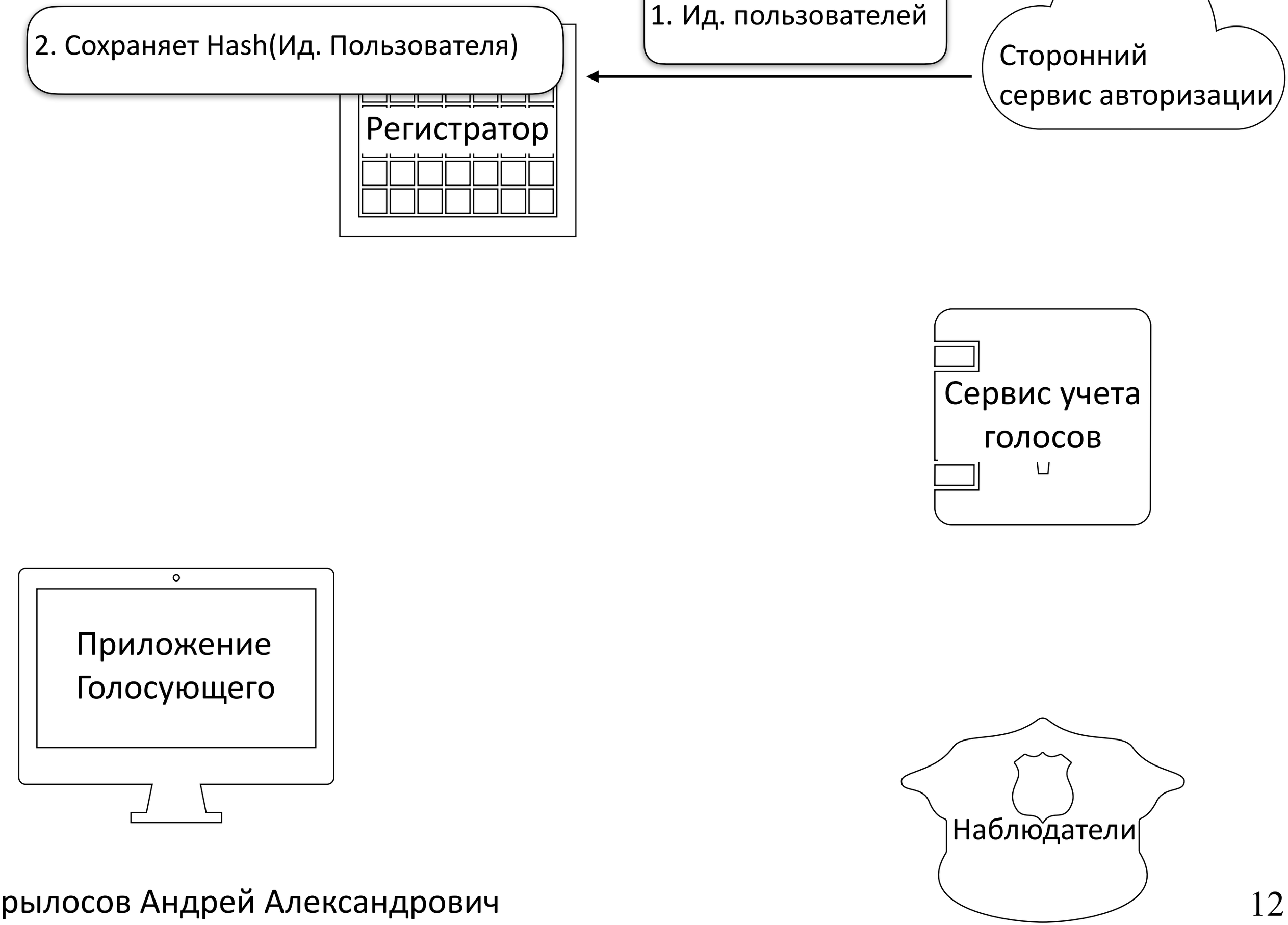
Разработка технического решения

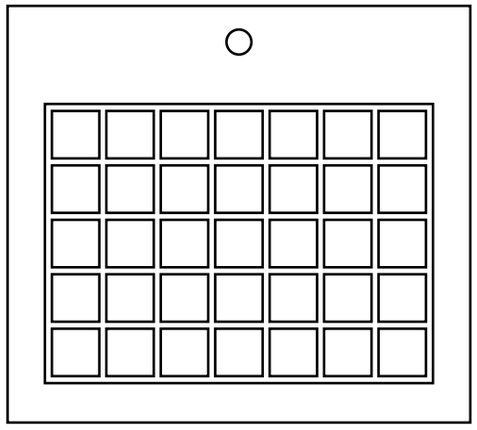
Разработка технического решения

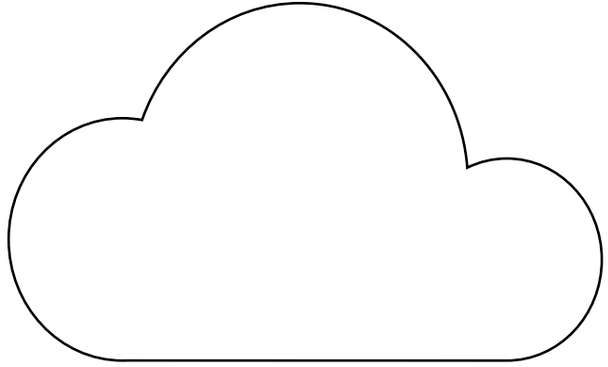
Разработка технического решения

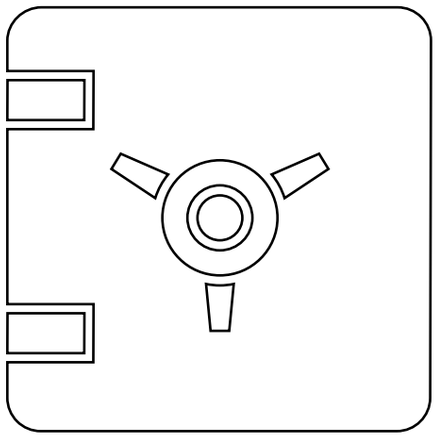


1. Ид. пользователей


2. Сохраняет Hash(Ид. Пользователя)
1. Ид. пользователей
Сторонний сервис авторизации
Регистратор
Сервис учета голосов
Приложение Голосующего
Наблюдатели

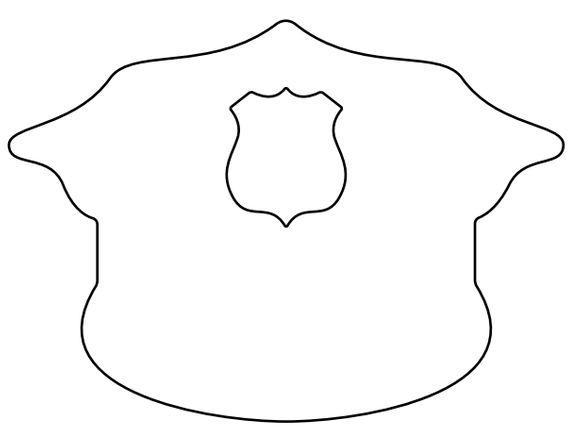


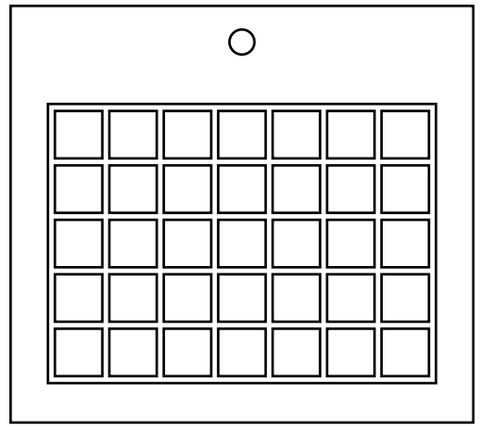


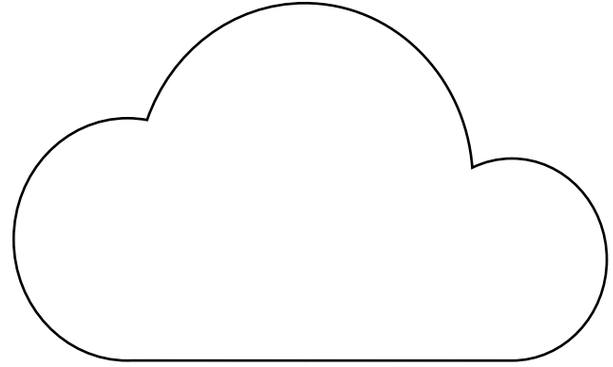


3. Создает ключи
- открытый
- закрытый
- секретный

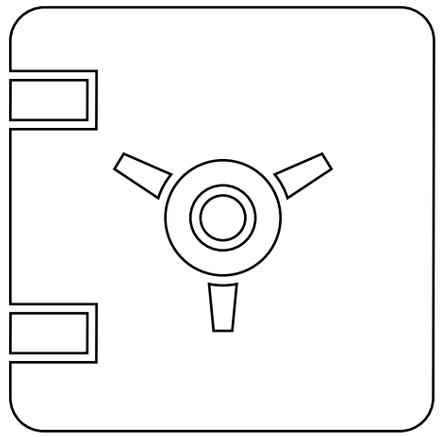
Маскирует открытый ключ

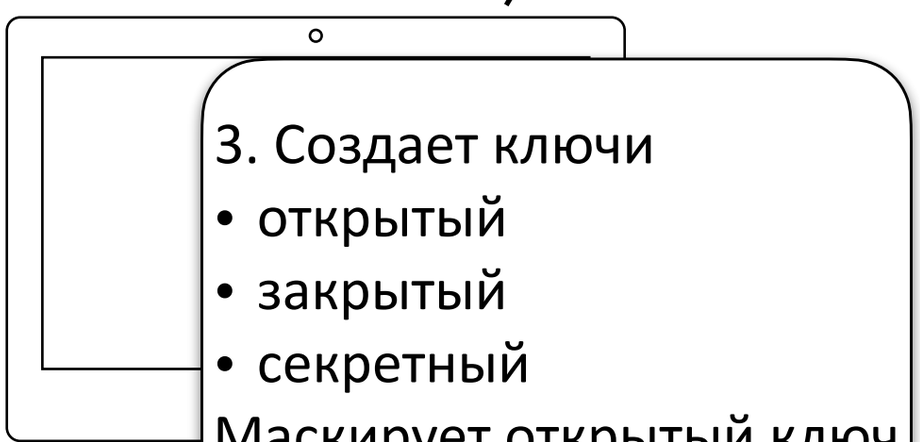






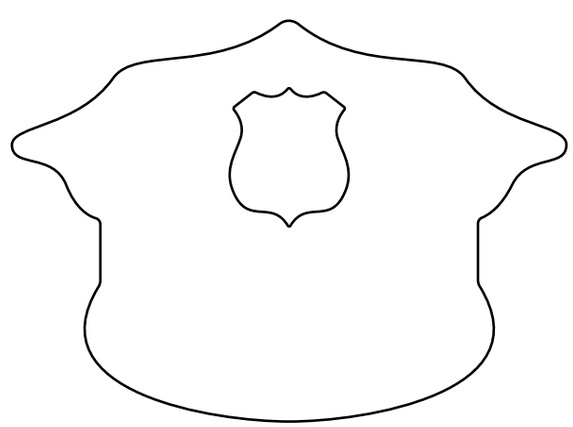
4. Данные авторизации
Маскированный открытый ключ

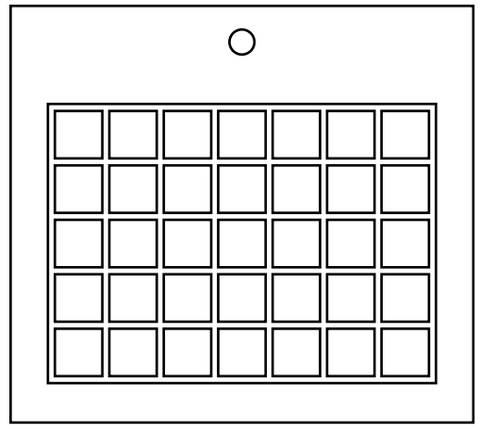


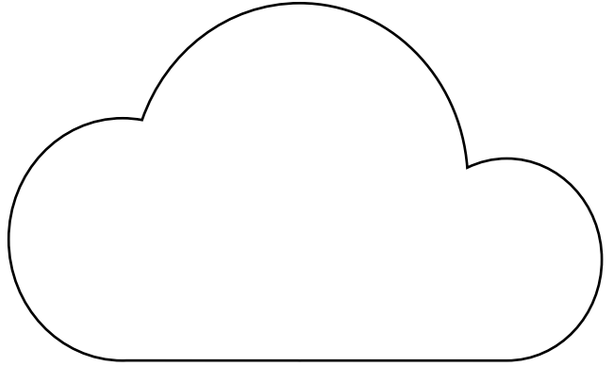


3. Создает ключи
- открытый
- закрытый
- секретный

Маскирует открытый ключ

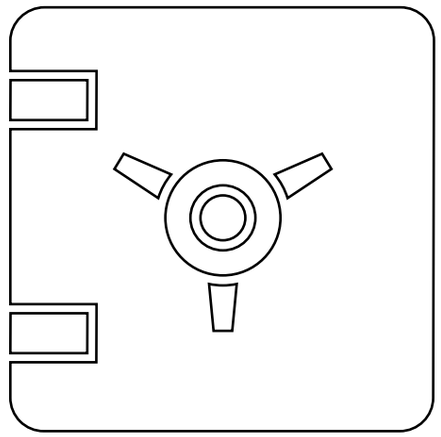


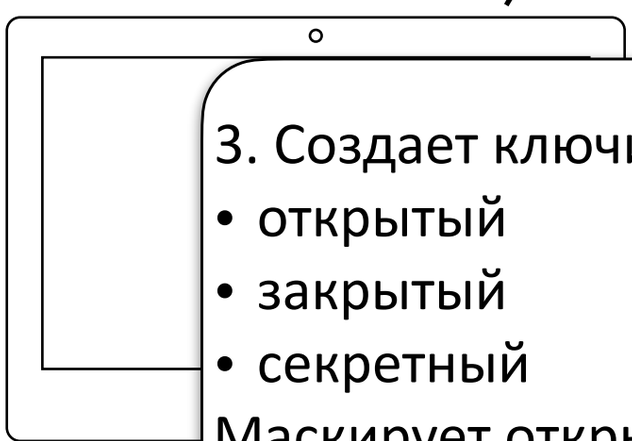




5. Данные авторизации

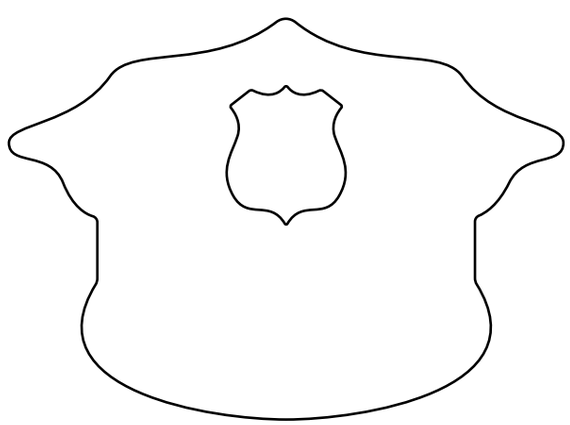
4. Данные авторизации
Маскированный открытый ключ



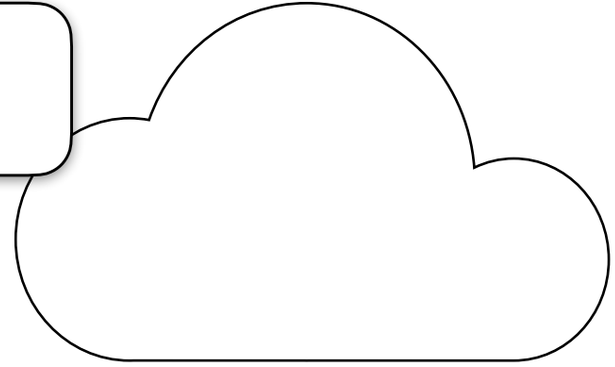


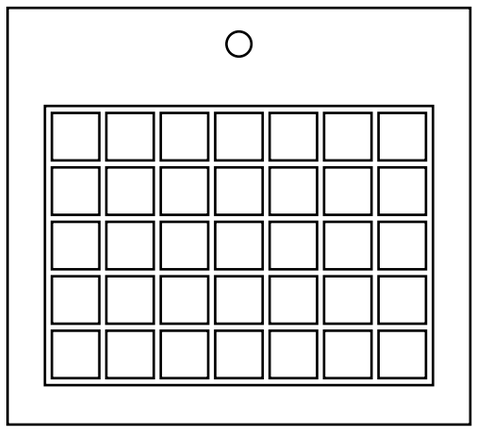
3. Создает ключи
- открытый
- закрытый
- секретный

Маскирует открытый ключ



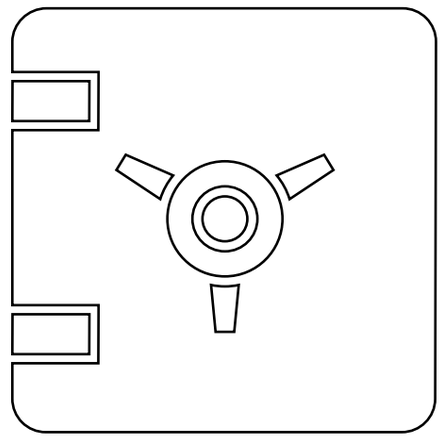
6. Ид. пользователя

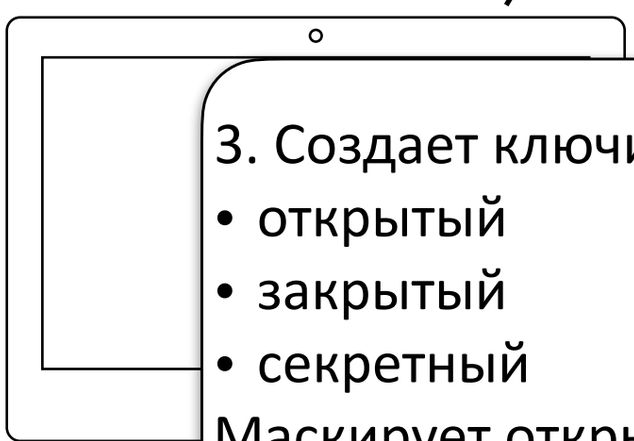




5. Данные авторизации

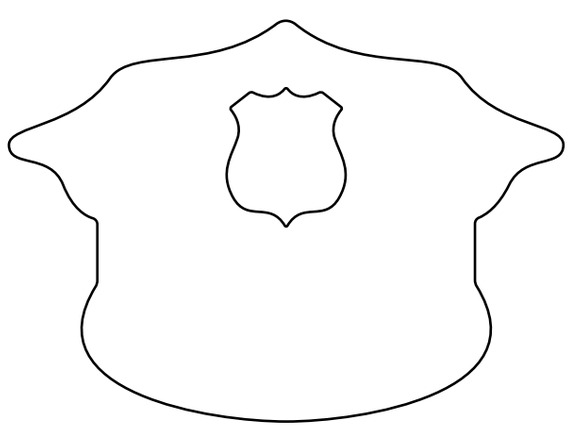
4. Данные авторизации
Маскированный открытый ключ





3. Создает ключи
- открытый
- закрытый
- секретный

Маскирует открытый ключ

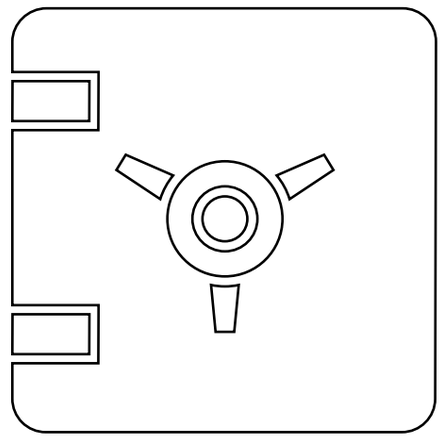


6. Ид. пользователя

7. Проверяет, что пользователь ранее не подписывал ключ
Отмечает, что пользователь уже получил подпись

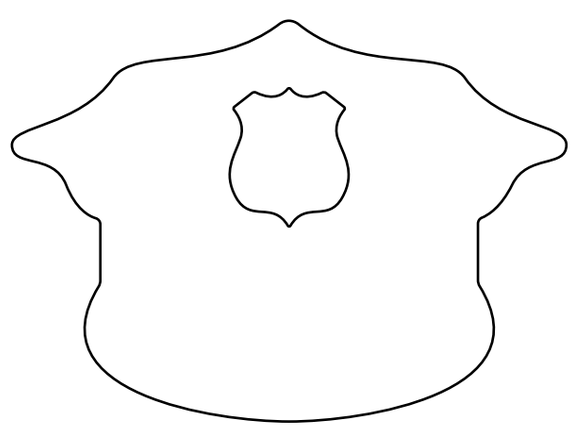
5. Данные авторизации

4. Данные авторизации
Маскированный открытый ключ



3. Создает ключи
- открытый
- закрытый
- секретный

Маскирует открытый ключ



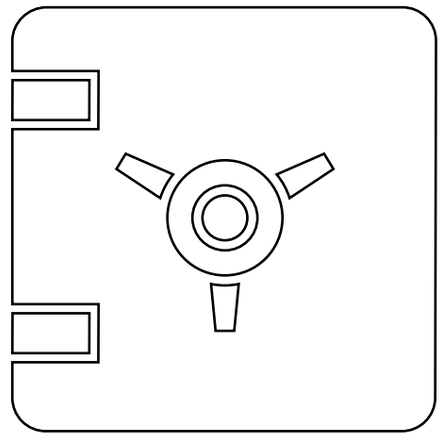
6. Ид. пользователя

7. Проверяет, что пользователь ранее не подписывал ключ
Отмечает, что пользователь уже получил подпись

5. Данные авторизации

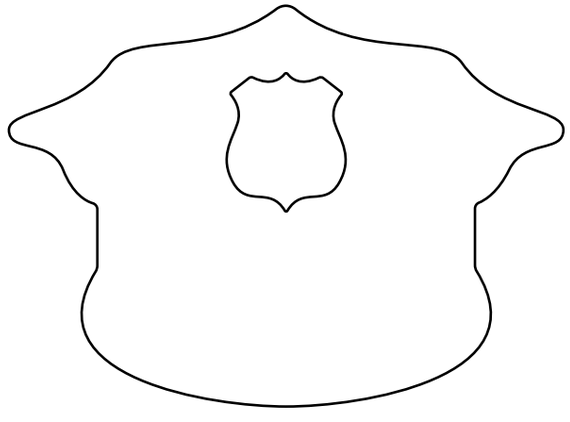
8. Подписанный маскированный ключ

4. Данные авторизации
Маскированный открытый ключ



3. Создает ключи
- открытый
- закрытый
- секретный

Маскирует открытый ключ



6. Ид. пользователя

7. Проверяет, что пользователь ранее не подписывал ключ
Отмечает, что пользователь уже получил подпись

5. Данные авторизации

8. Подписанный маскированный ключ

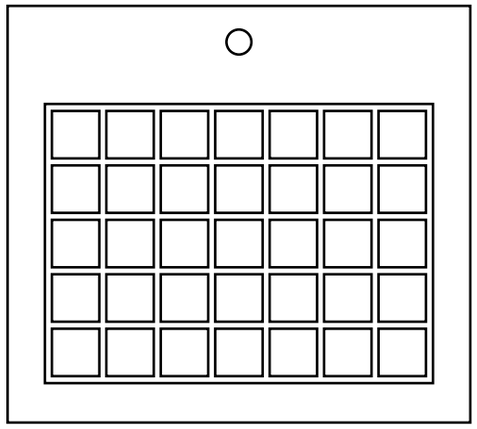
4. Данные авторизации
Маскированный открытый ключ

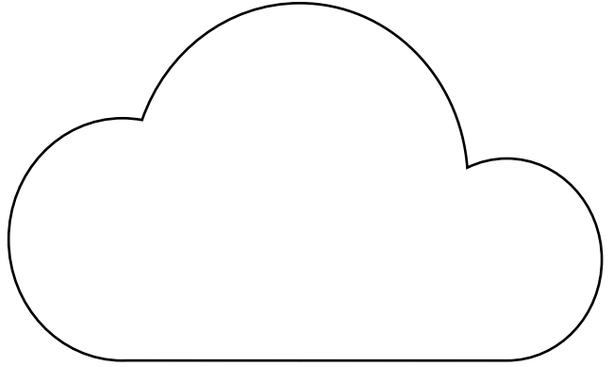
3. Создает ключи
- открытый
- закрытый
- секретный

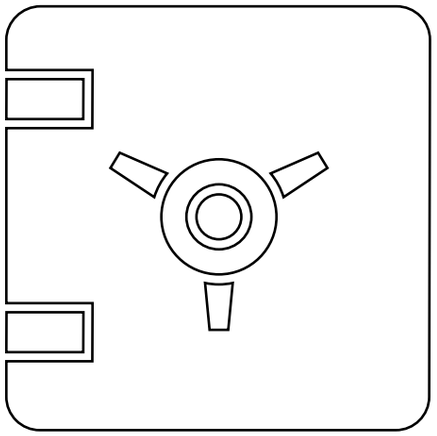
Маскирует открытый ключ

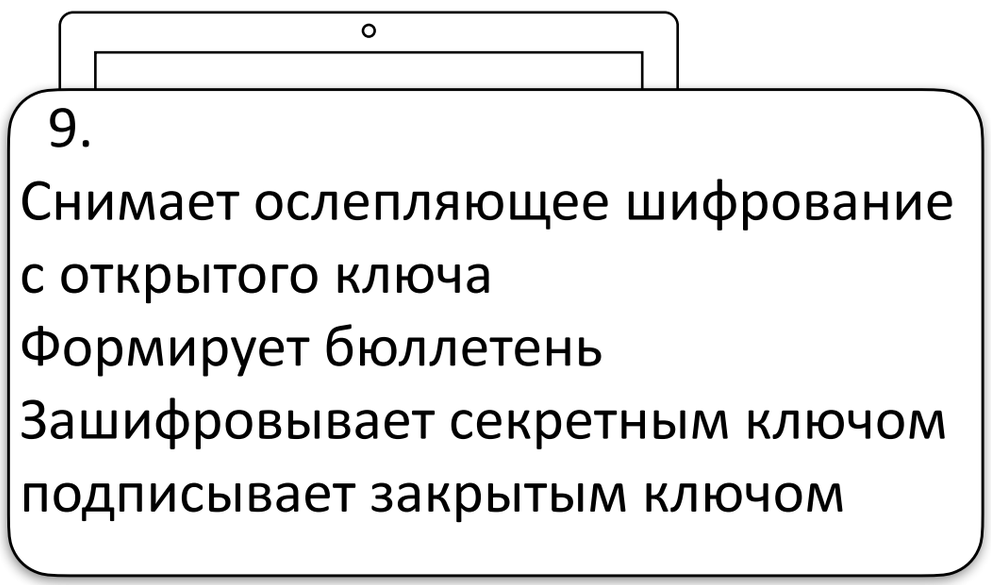
Копия базы данных каждые 10 минут

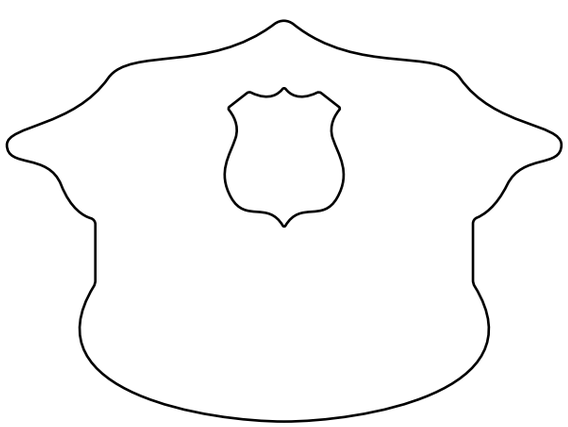
Подсчитывают количество полученных подписей

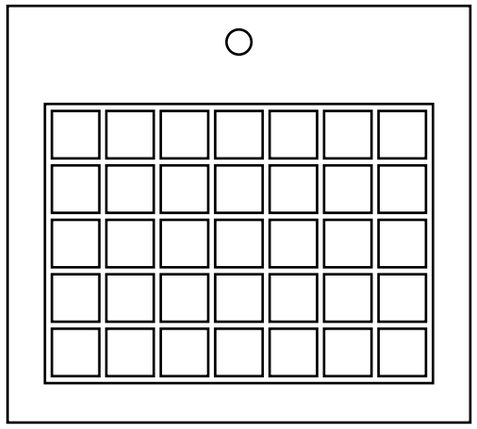


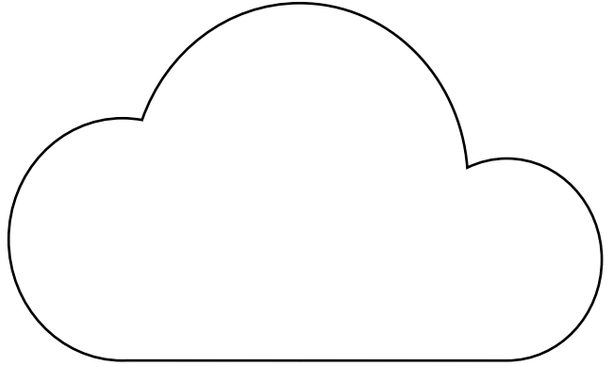


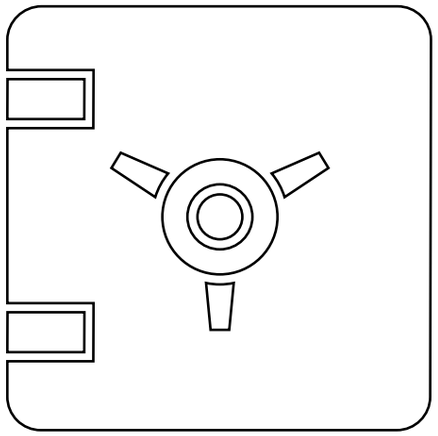



9.
Снимает ослепляющее шифрование
с открытого ключа
Формирует бюллетень
Зашифровывает секретным ключом
подписывает закрытым ключом

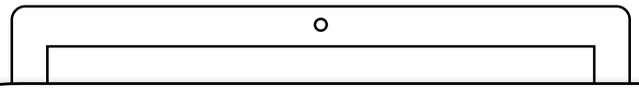




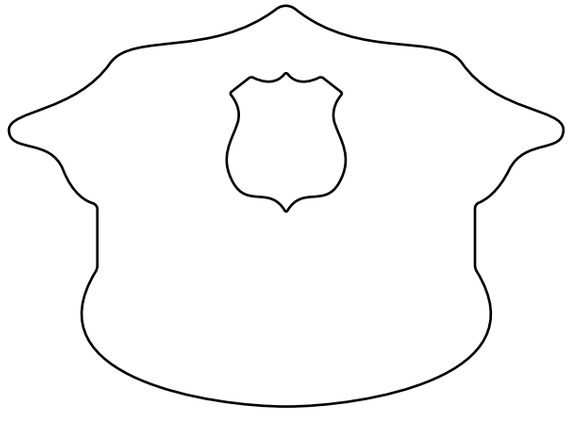


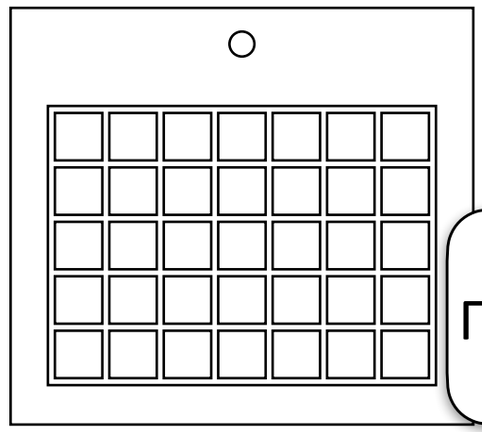


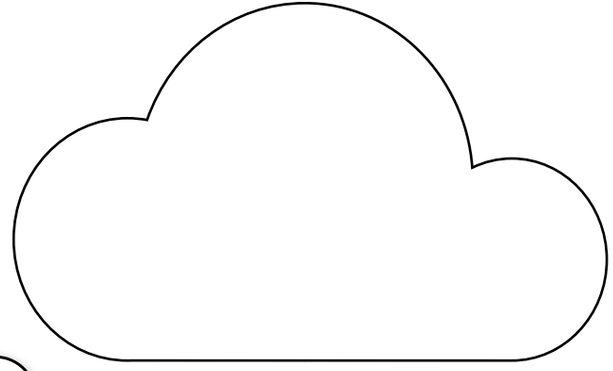
10.
Подготовленный бюллетень
Открытый ключ



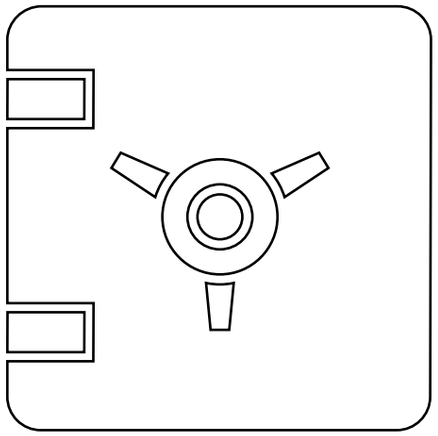
9.
Снимает ослепляющее шифрование
с открытого ключа
Формирует бюллетень
Зашифровывает секретным ключом
подписывает закрытым ключом



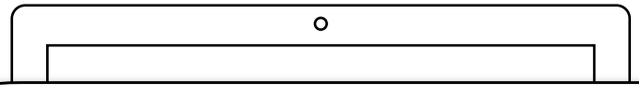




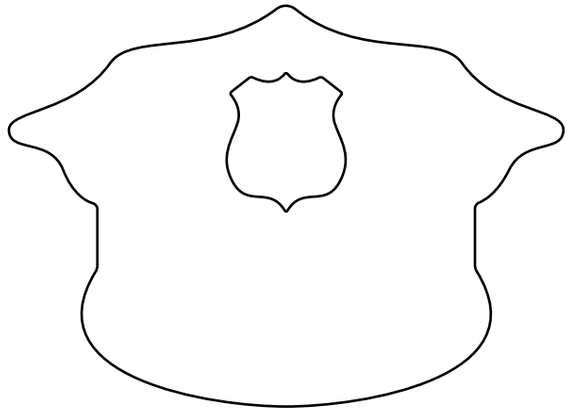
11.
Публичный ключ регистратора

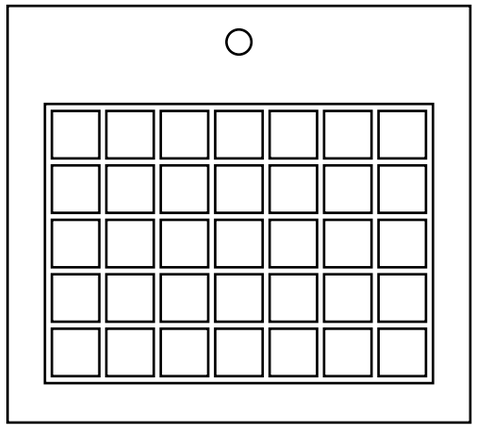


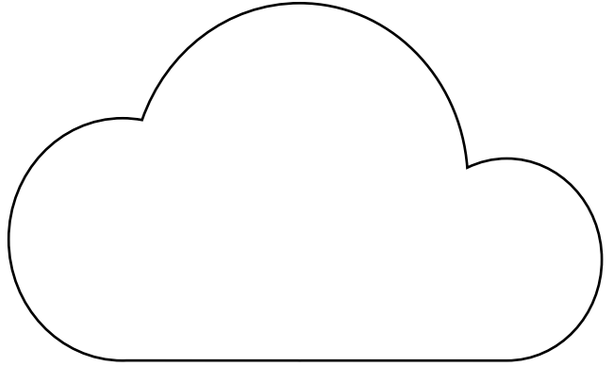
10.
Подготовленный бюллетень
Открытый ключ



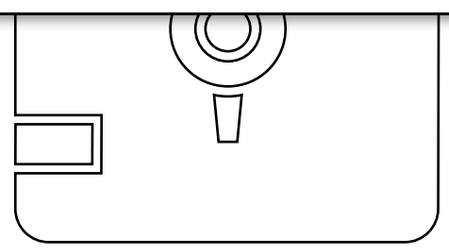
9.
Снимает ослепляющее шифрование
с открытого ключа
Формирует бюллетень
Зашифровывает секретным ключом
подписывает закрытым ключом

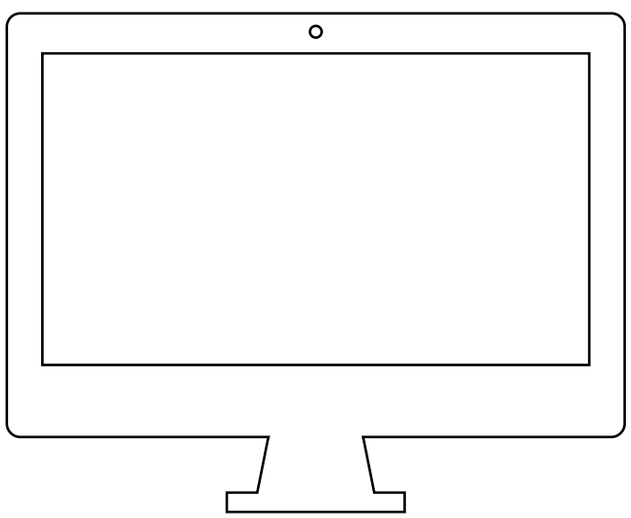


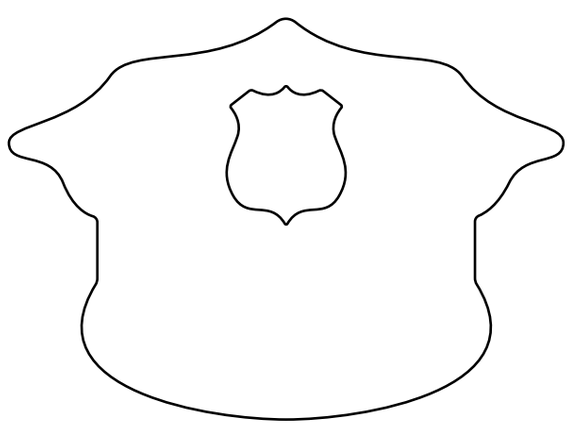


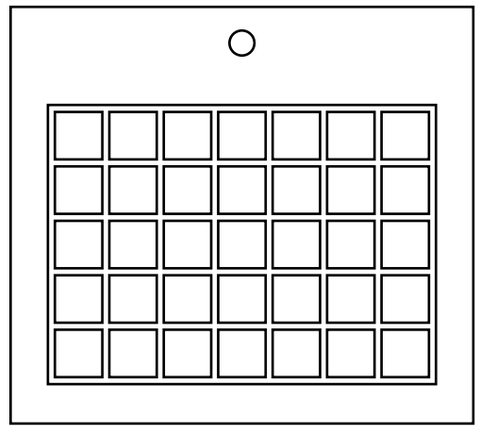


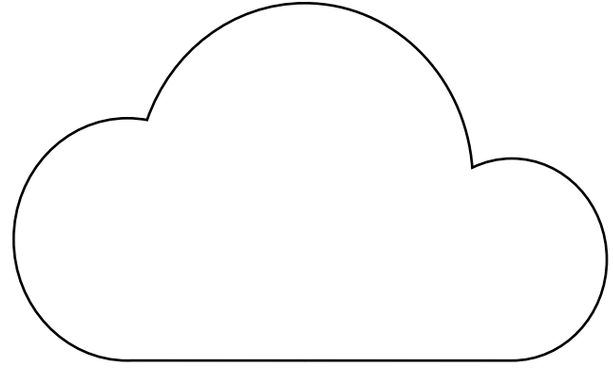
12.
Проверяет подписи
Подписывает бюллетень
Помещает бюллетень в список



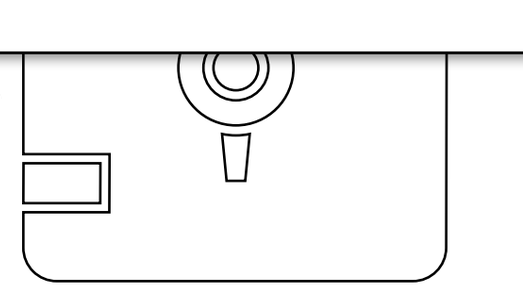




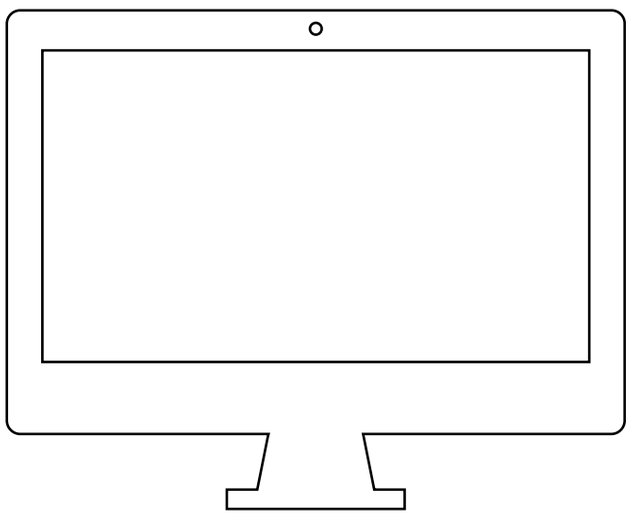


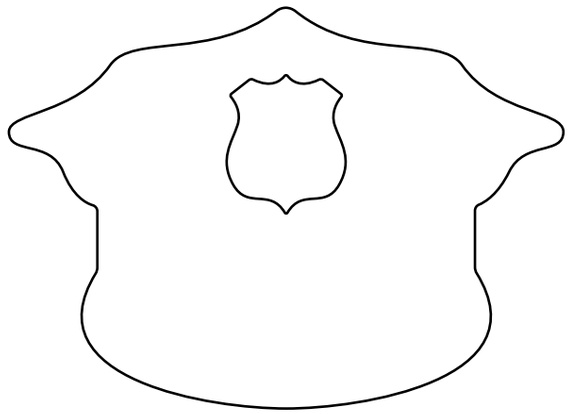


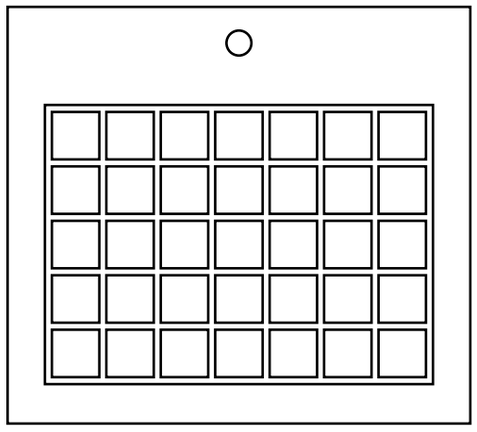
12.
Проверяет подписи
Подписывает бюллетень
Помещает бюллетень в список

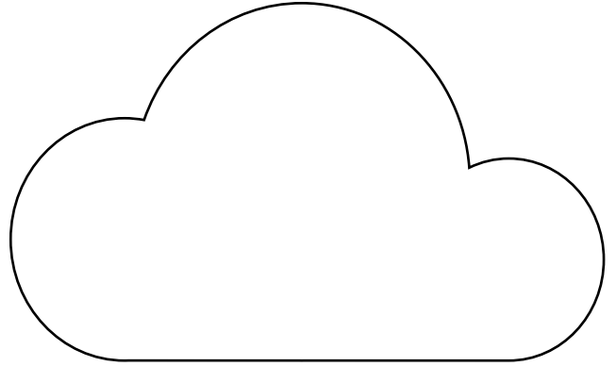


13.
Подписанный учетом бюллетень



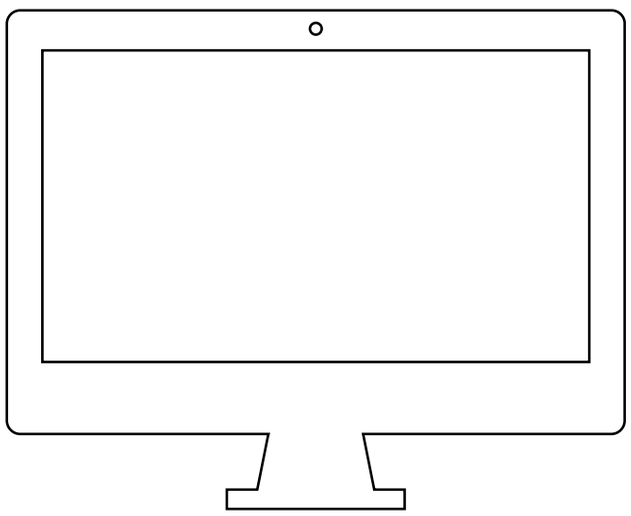






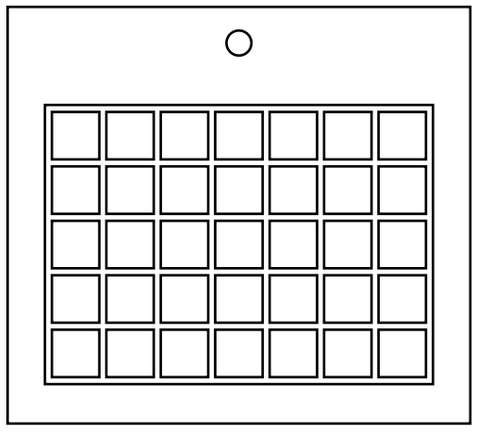
12.
Проверяет подписи
Подписывает бюллетень
Помещает бюллетень в список

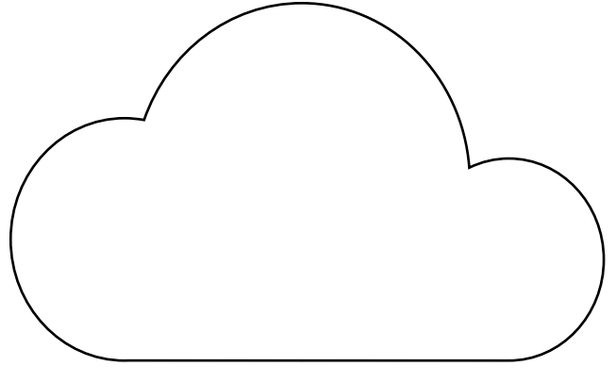
13.
Подписанный учетом бюллетень



Копия базы данных каждые 10 минут

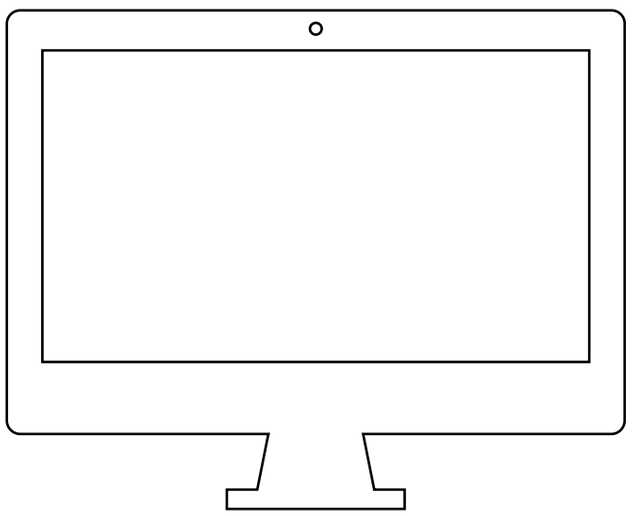
Подсчитывают количество бюллетеней
Сравнивают с количеством подписанных
Проверяют целостность базы данных





12.
Проверяет подписи
Подписывает бюллетень
Помещает бюллетень в список

13.
Подписанный учетом бюллетень

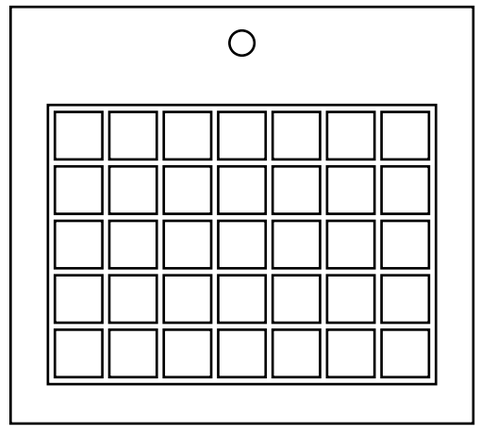


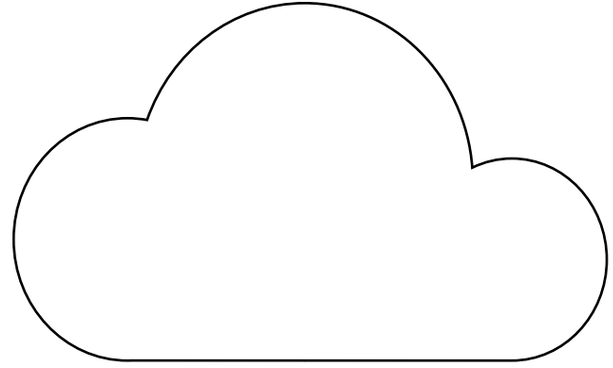
Копия базы данных по запросу

Копия базы данных каждые 10 минут

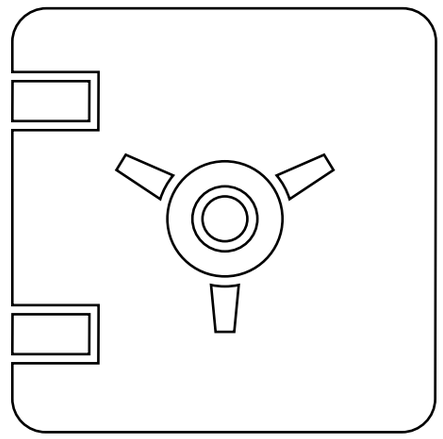
Подсчитывают количество бюллетеней
Сравнивают с количеством подписанных
Проверяют целостность базы данных

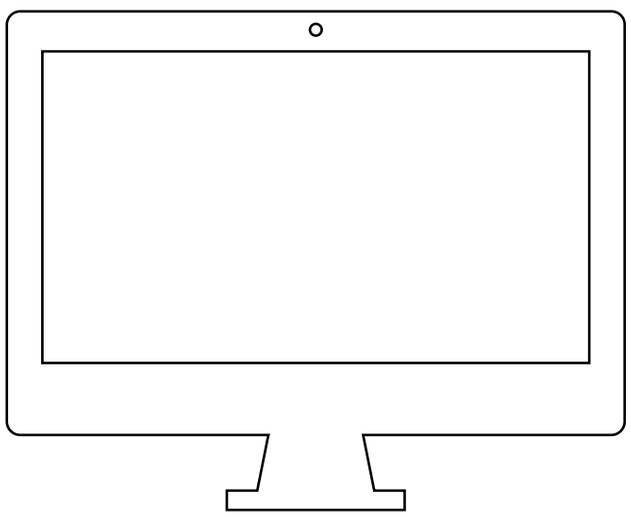
Время голосования закончилось

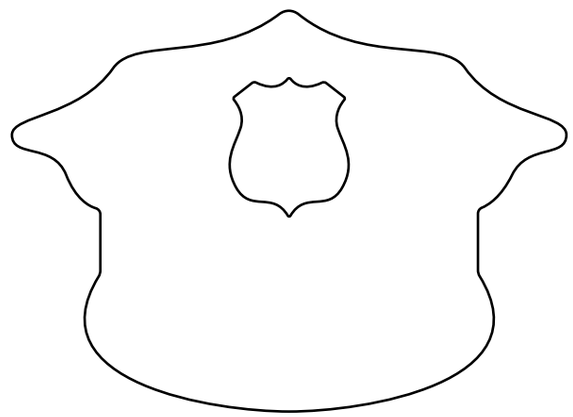




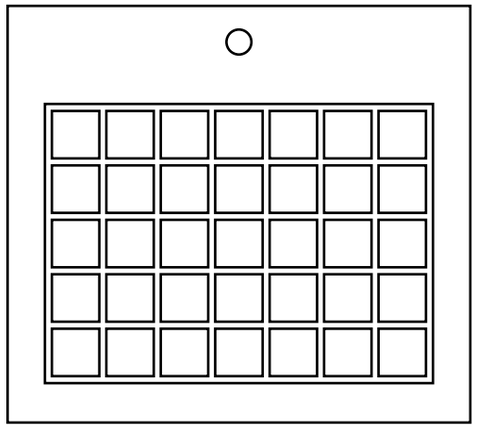
14.
Открытый ключ
Секретный ключ

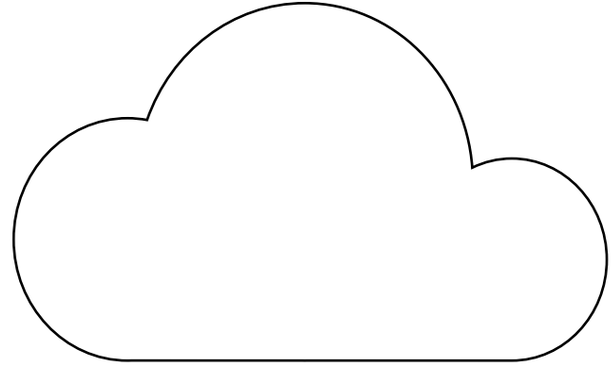




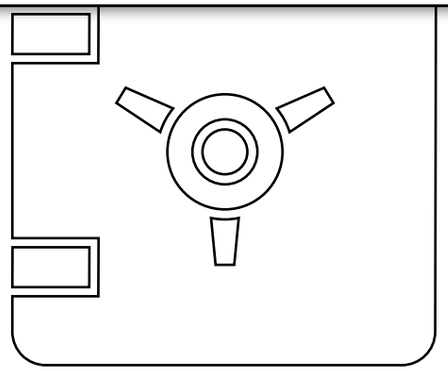


Время голосования закончилось

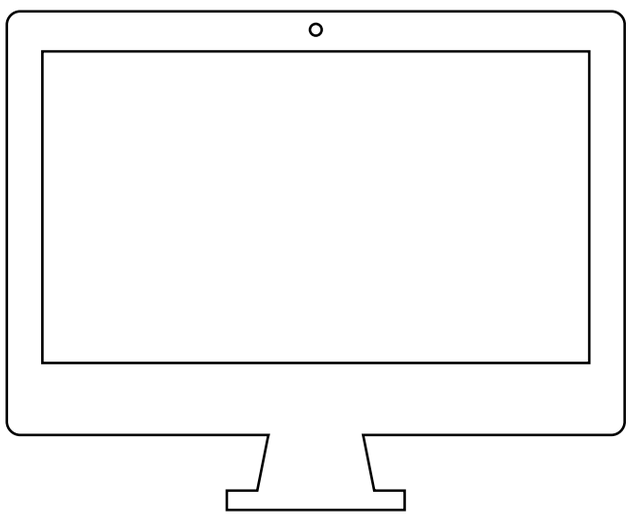


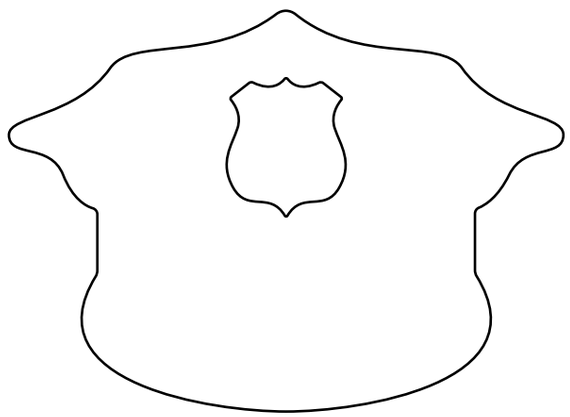


15.
Сохраняет секретные ключи
Расшифровывает бюллетени
Считает результат

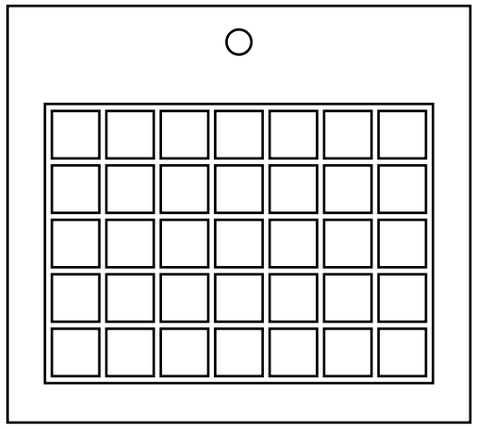


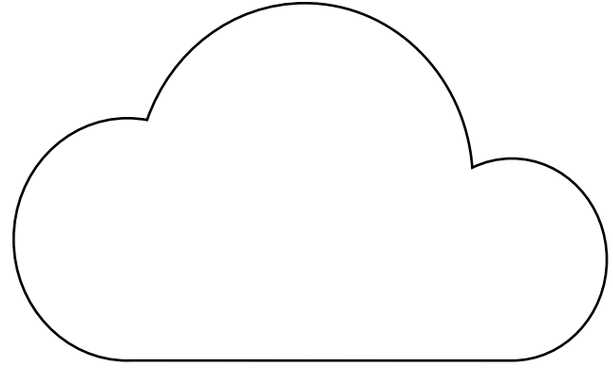
14.
Открытый ключ
Секретный ключ



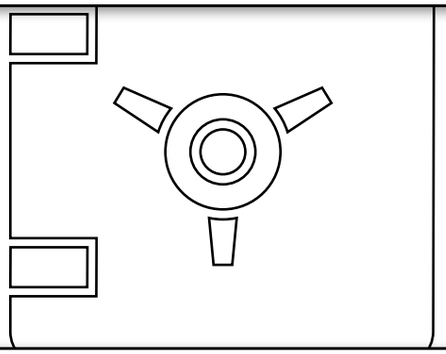


Время голосования закончилось

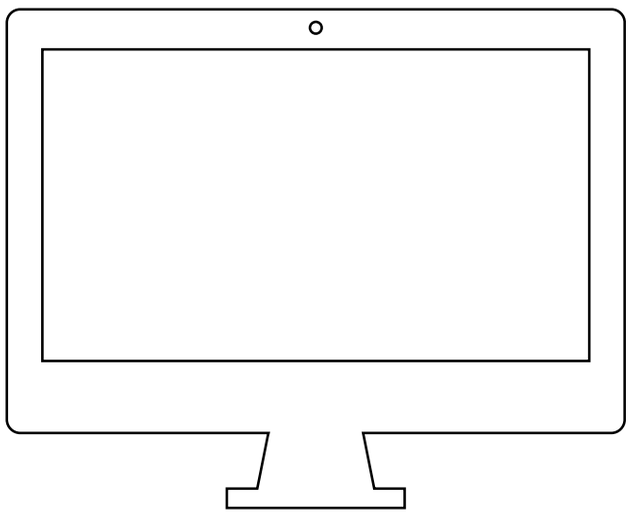




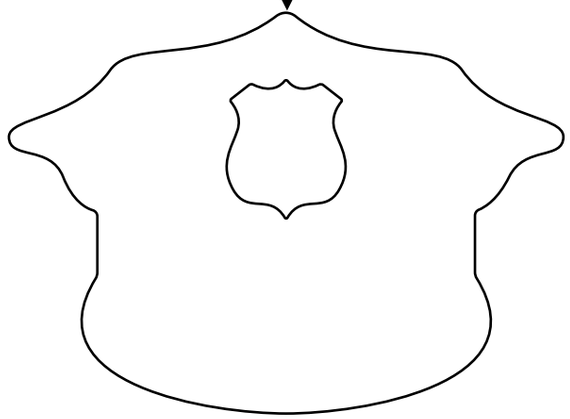
15.
Сохраняет секретные ключи
Расшифровывает бюллетени
Считает результат



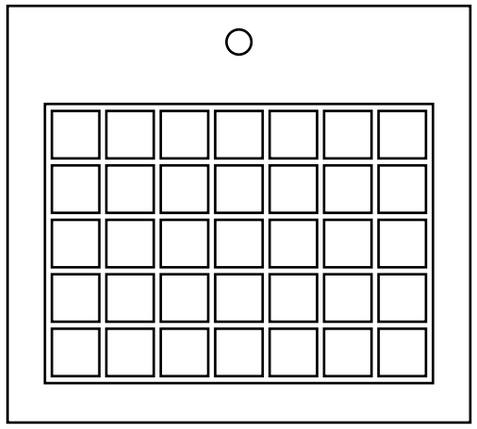
14.
Открытый ключ
Секретный ключ

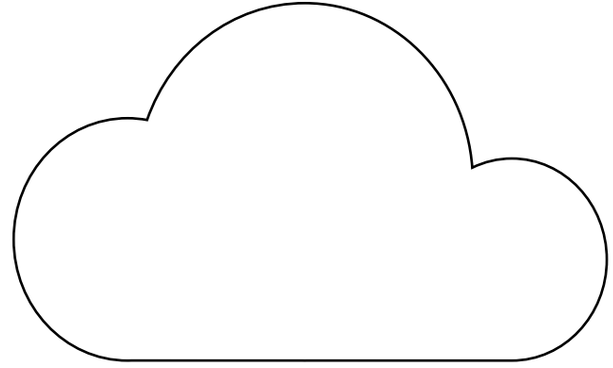


16.
Результат голосования
Финальная копия базы данных
Секретные ключи

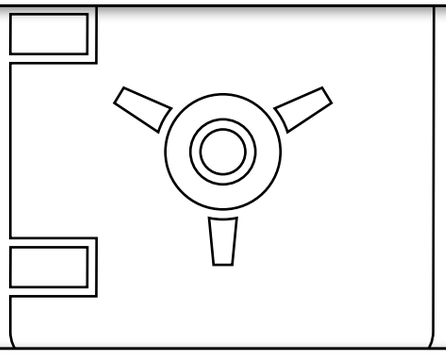


Время голосования закончилось

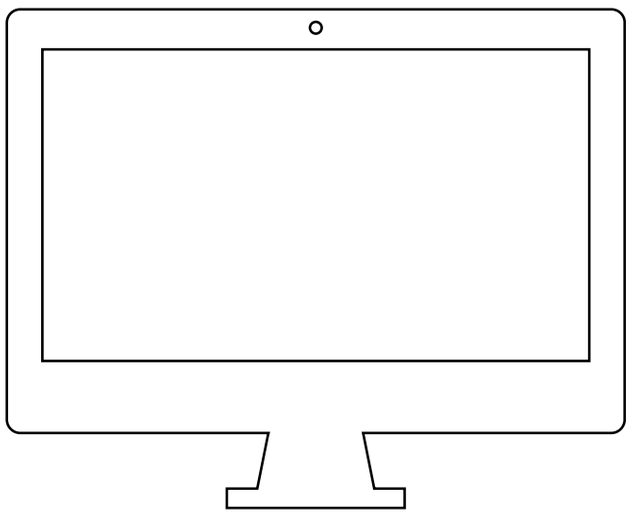




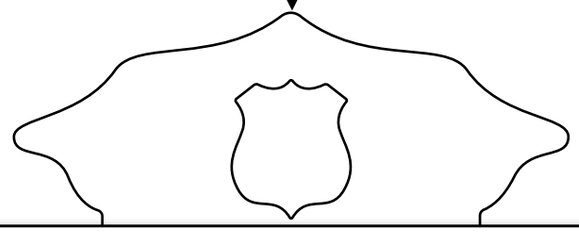
15.
Сохраняет секретные ключи
Расшифровывает бюллетени
Считает результат



14.
Открытый ключ
Секретный ключ

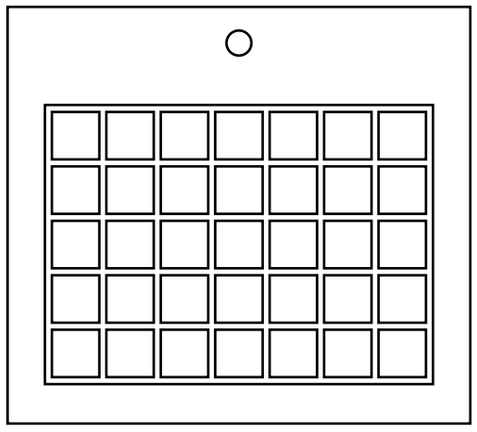


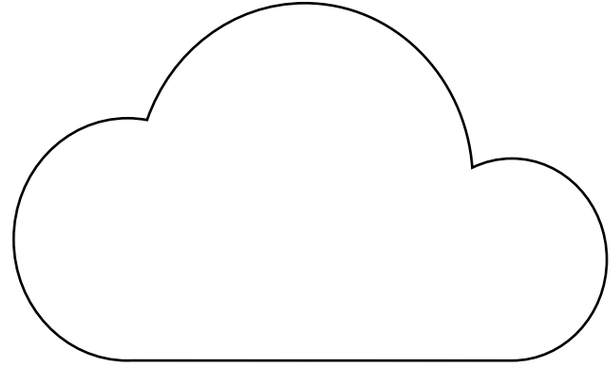
16.
Результат голосования
Финальная копия базы данных
Секретные ключи



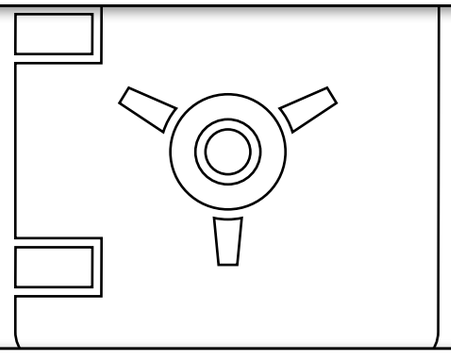
Производят аудит результатов голосования

Время голосования закончилось



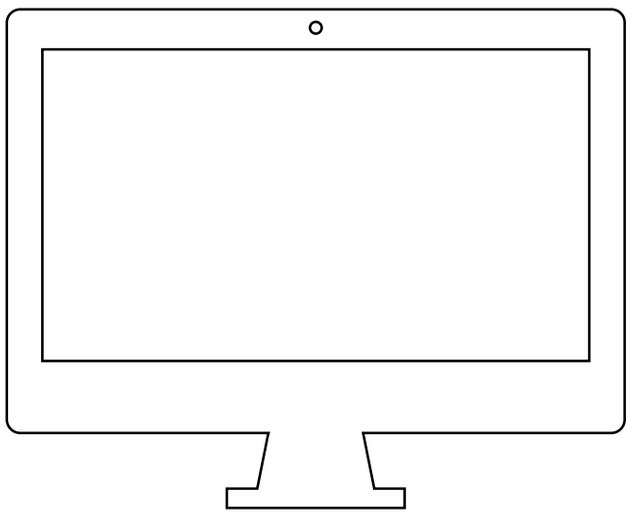


15.
Сохраняет секретные ключи
Расшифровывает бюллетени
Считает результат

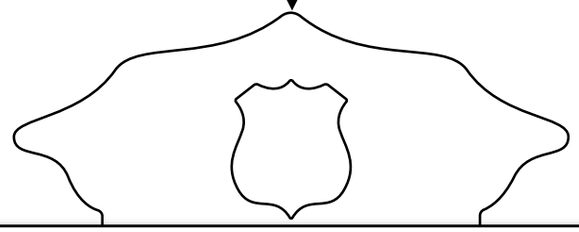


14.
Открытый ключ
Секретный ключ

16.
Результат голосования
Финальная копия базы данных
Секретные ключи

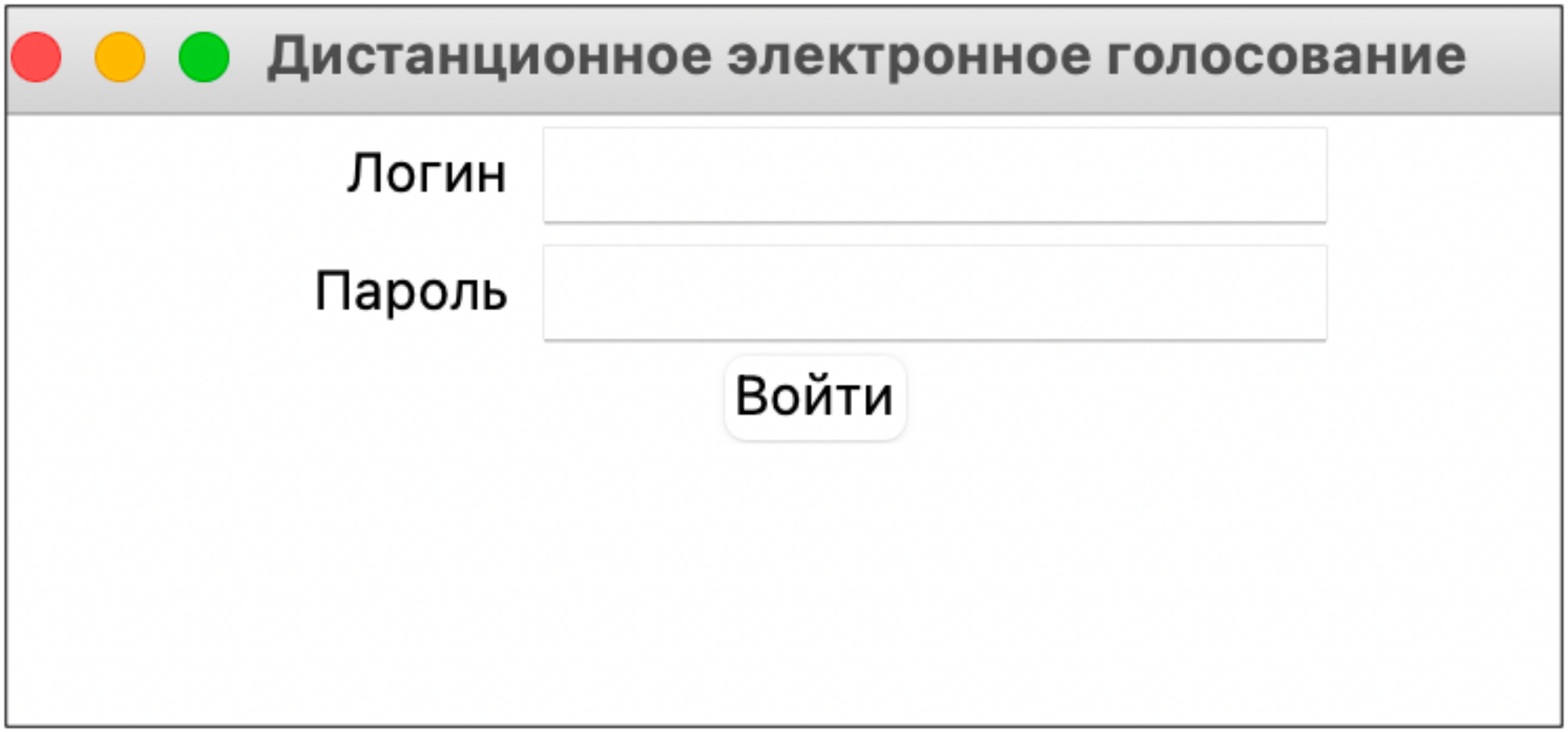


Финальная копия
Секретные ключи

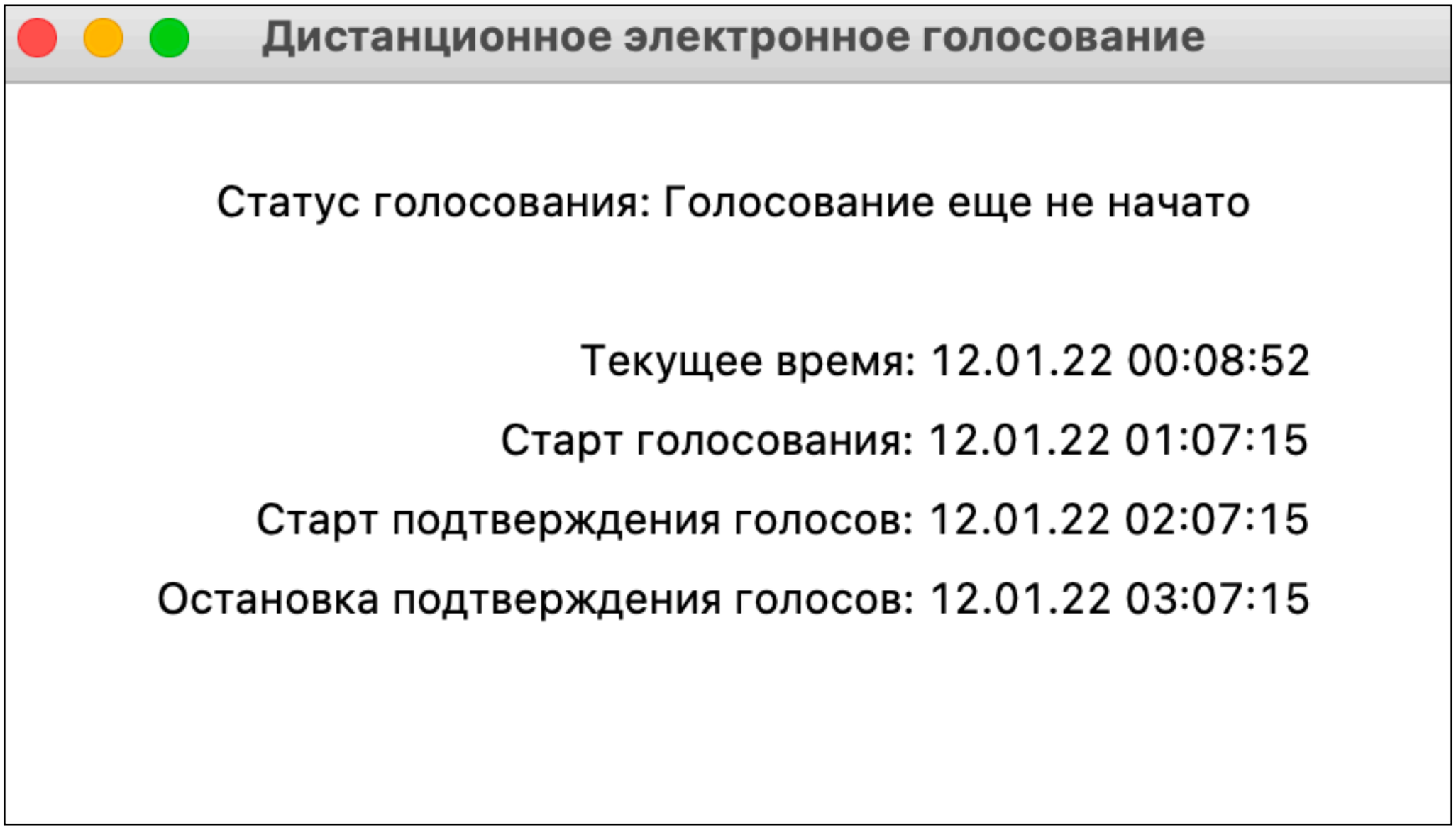


Производят аудит результатов голосования

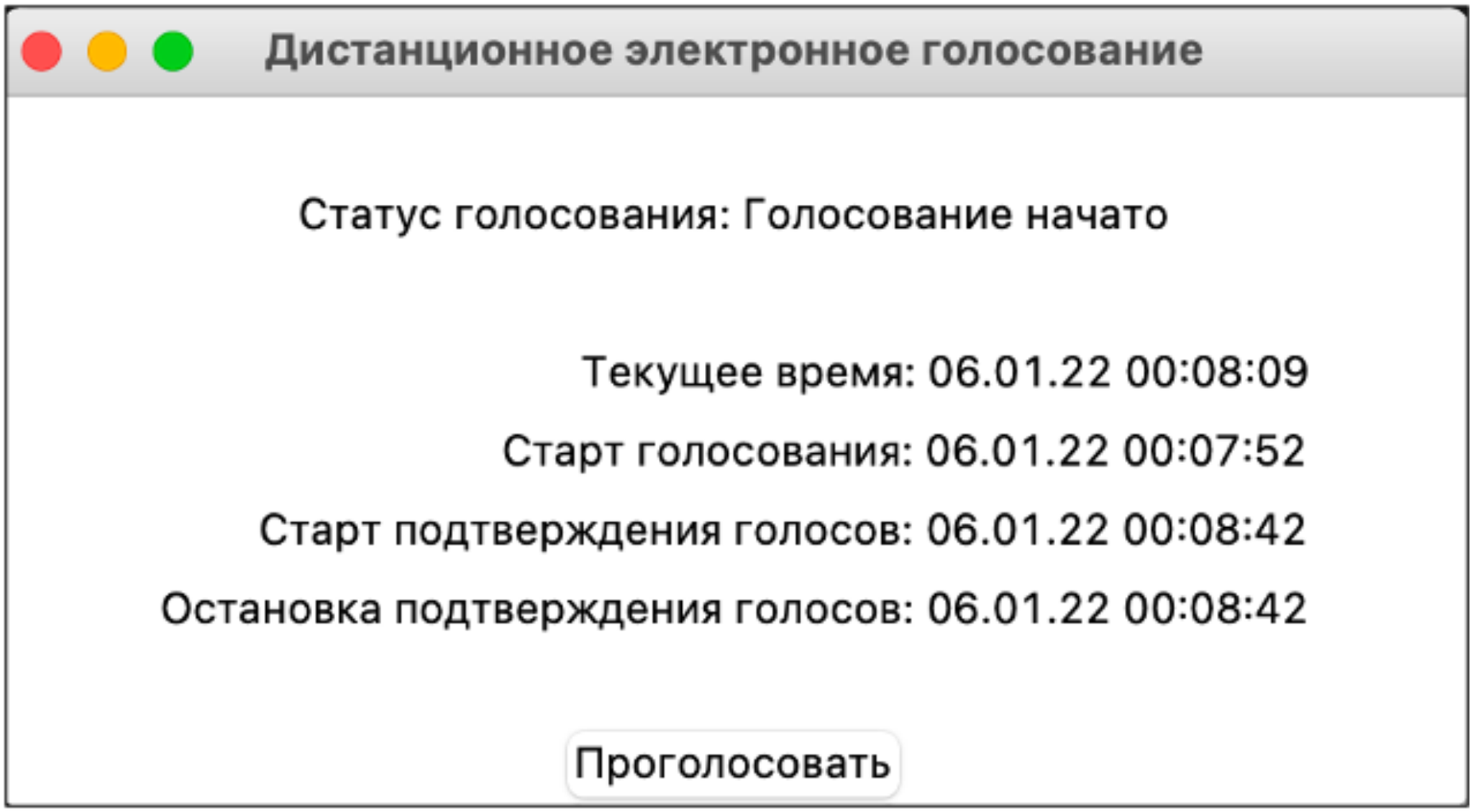
Интерфейс клиентского приложения



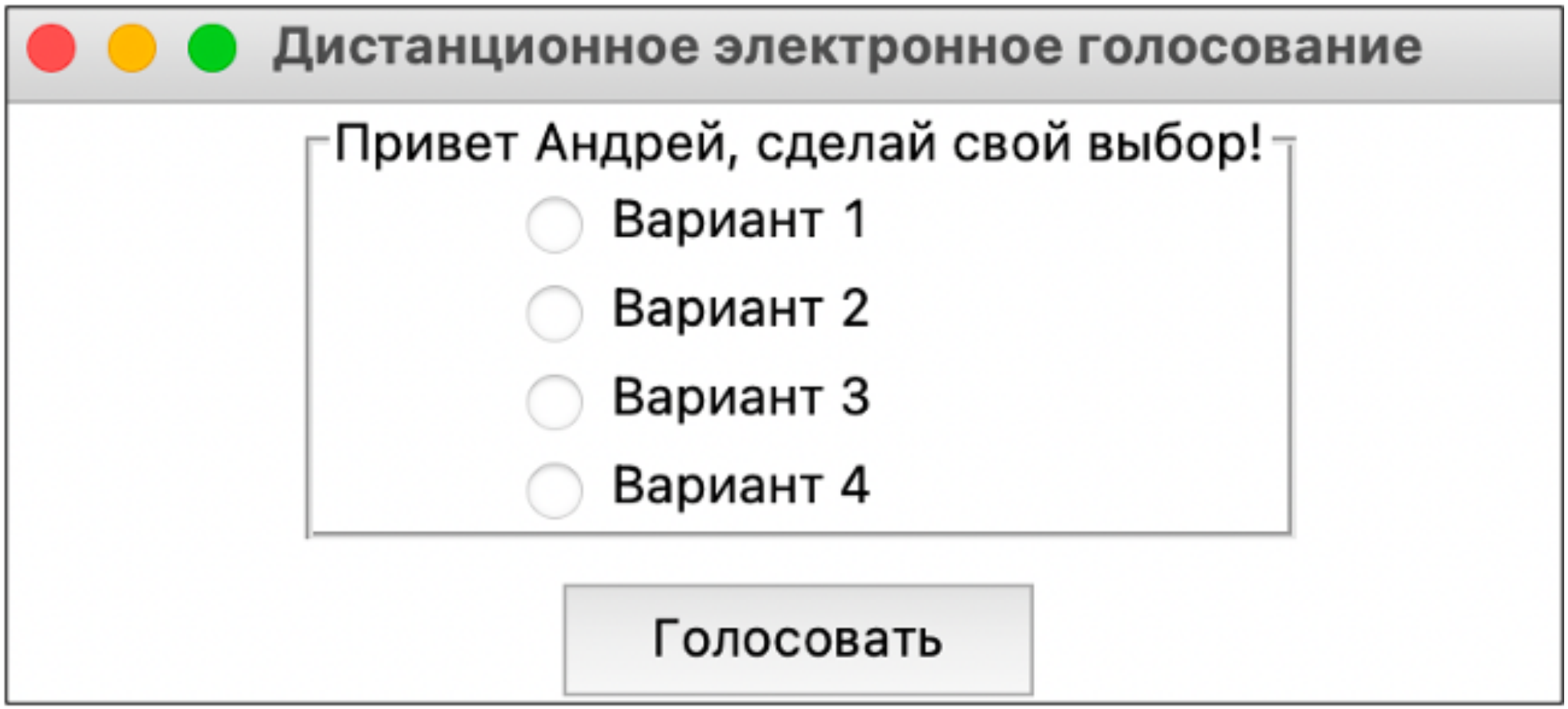
Интерфейс клиентского приложения



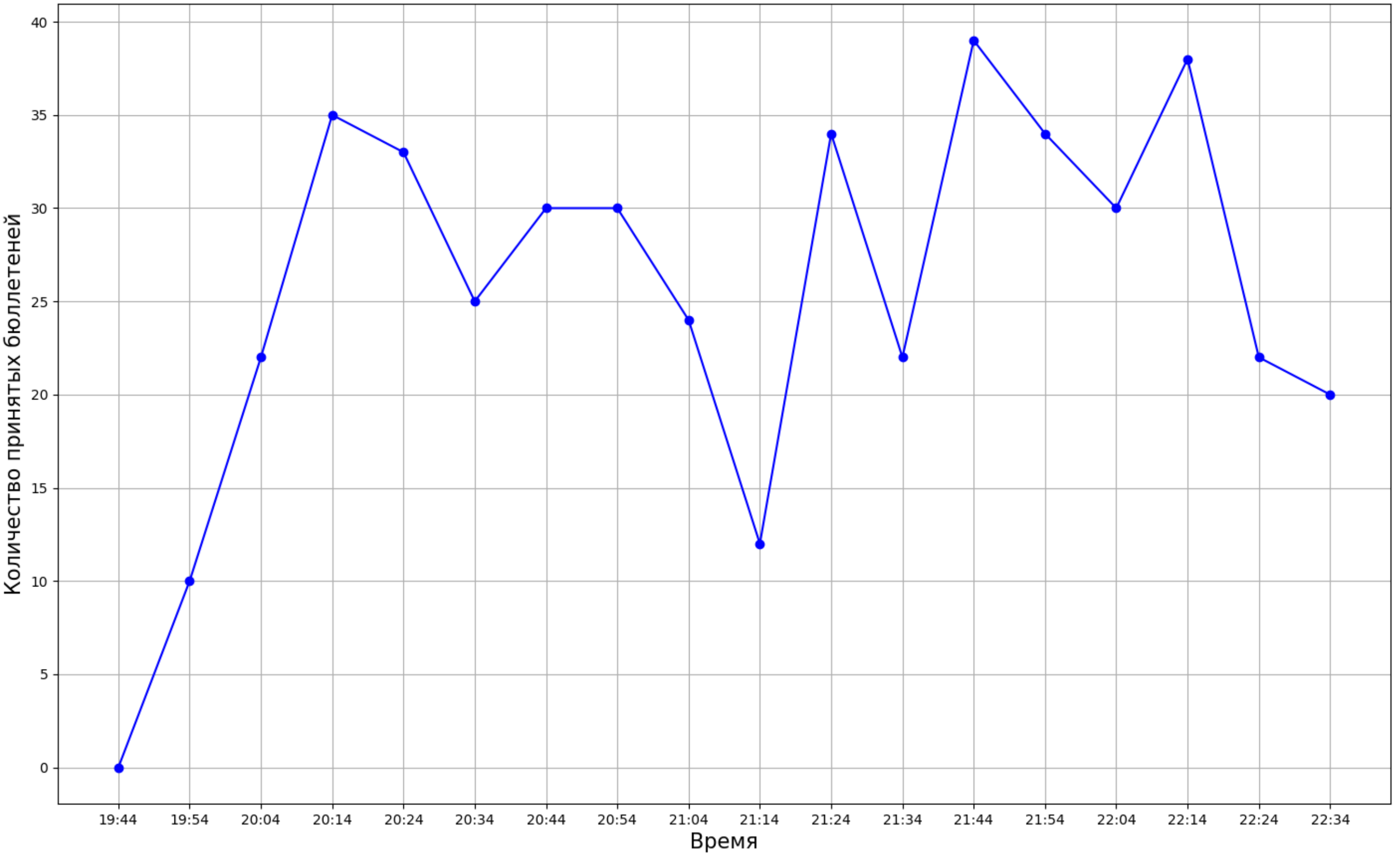
Интерфейс клиентского приложения



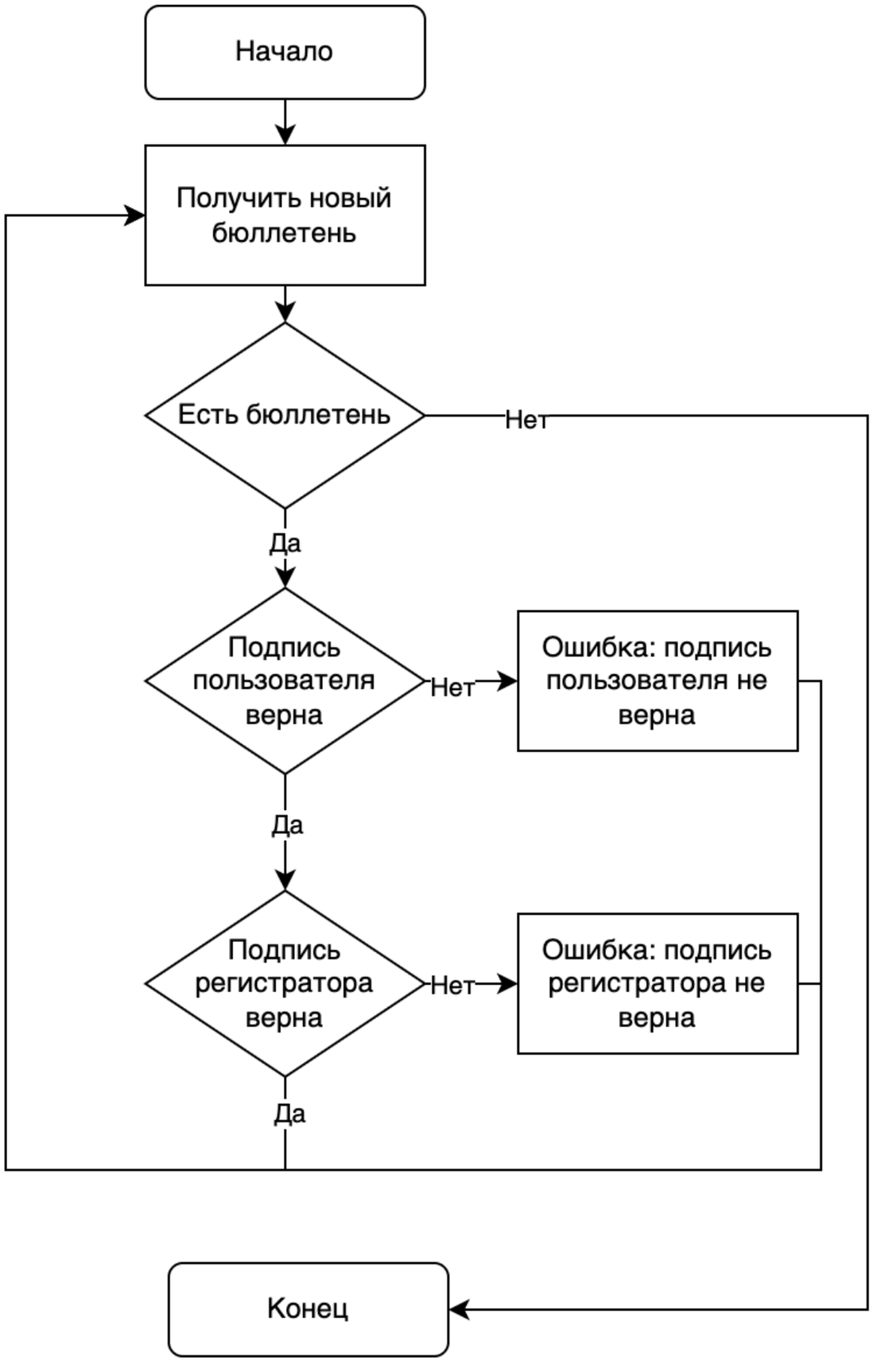
Интерфейс клиентского приложения



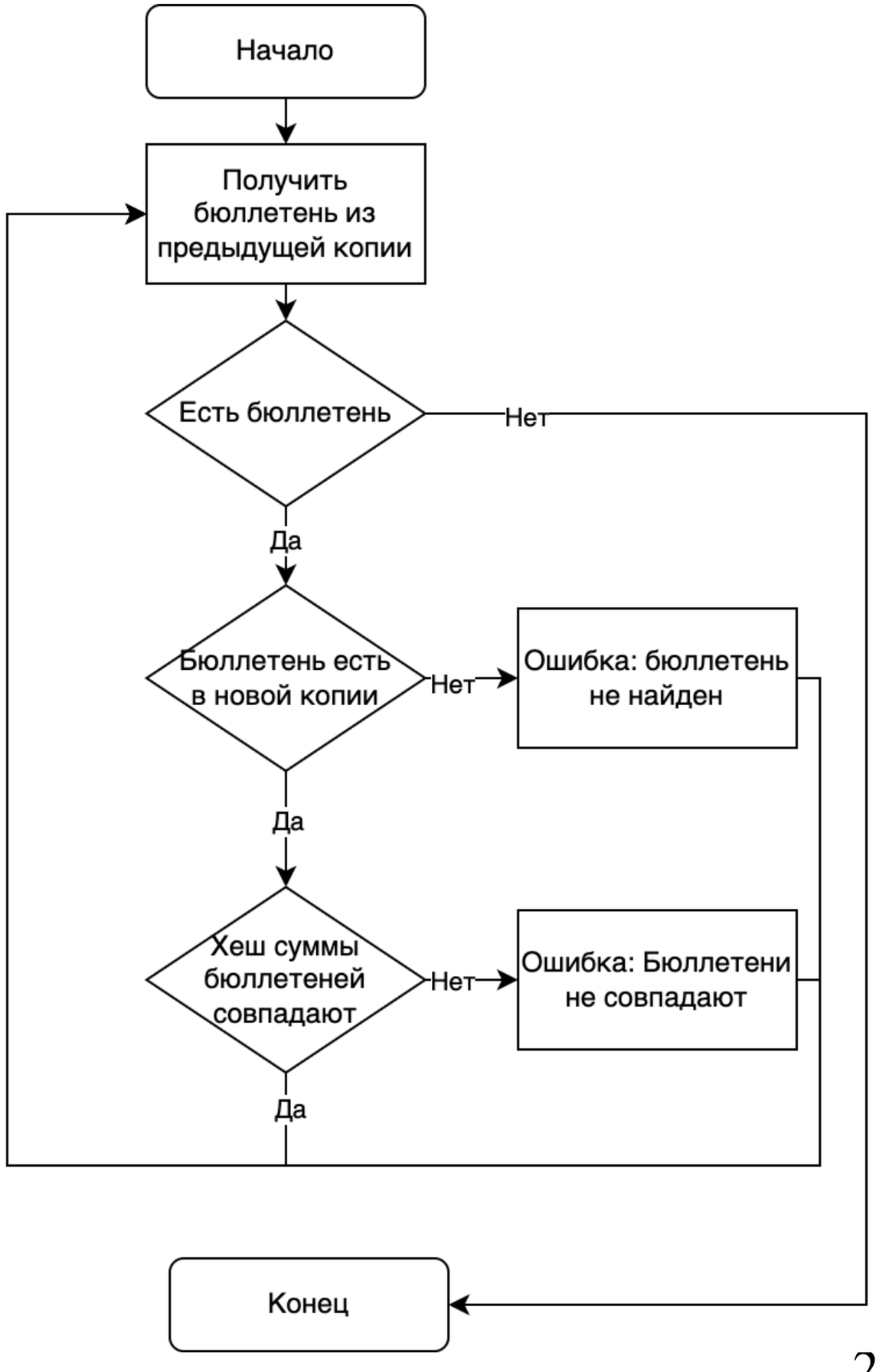
Модуль аудита



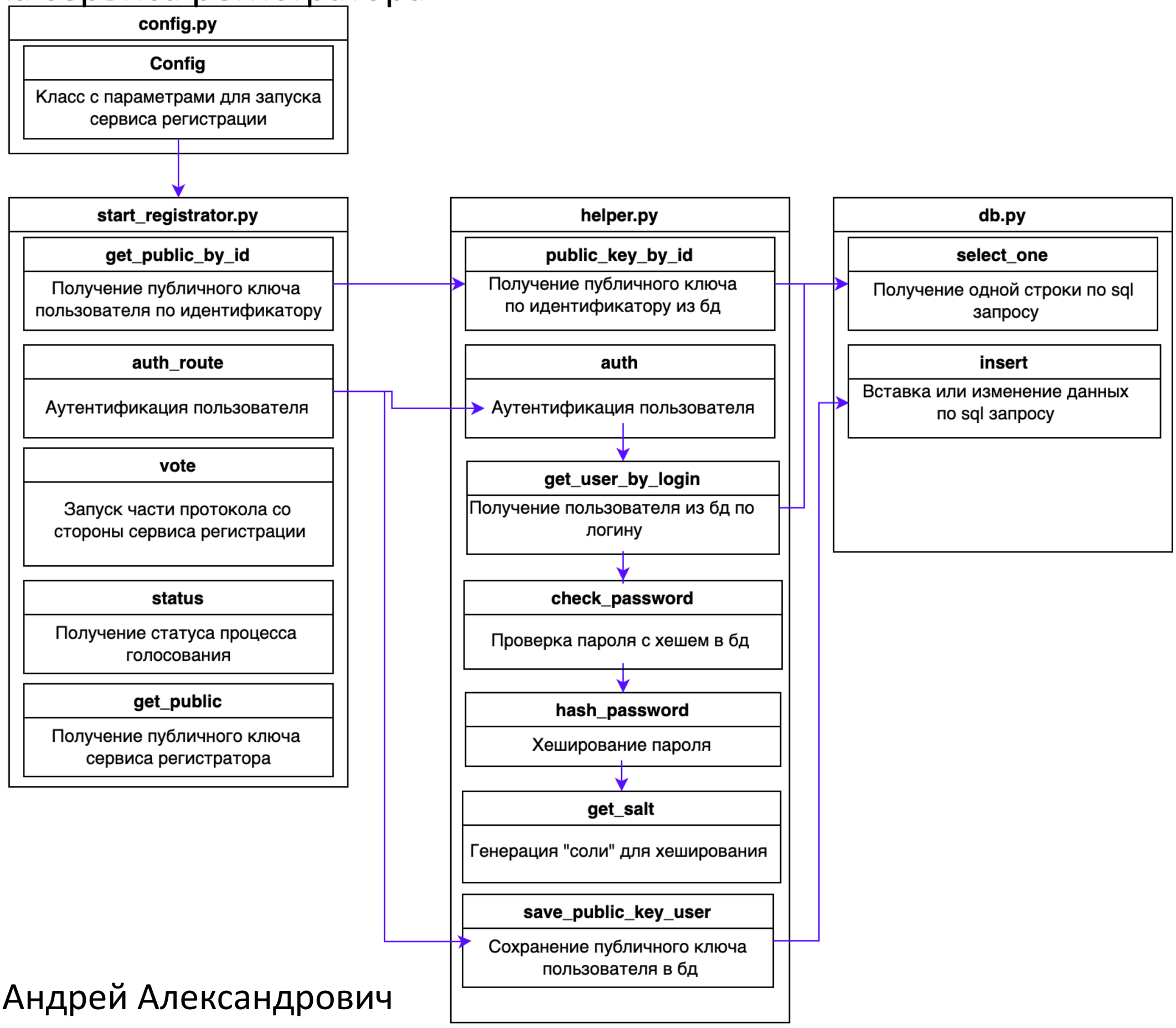
Проверка подписей



Проверка целостности



Разработка сервиса регистратора



Сервис учета голосов

config_validator.py

Config

Класс с параметрами для запуска сервиса

start_validator.py

accept

Сохранение приватного ключа пользователя

vote

Сохранение зашифрованного бюллетеня пользователя

get_public

Получение публичного ключа сервиса

get_results

Получение результата голосования

get_keys_for_replicas

Получение ключей для дешифровки копий бд

helper.py

update_private

Сохранение приватного ключа в бд

check_sign

Проверка электронной подписи

insert_message

Сохранение бюллетеня в бд

sign

Электронная подпись сообщения

decrypt_messages

Дешифровка всех бюллетеней и подсчет голосов

get_keys

Получение связки id бюллетеня и приватного ключа

db.py

insert

Вставка или изменение данных по sql запросу

select

Получение даных по sql запросу

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

Технико-экономическое обоснование работы

- Себестоимость: 84962,9 руб.
- Цена с учетом НДС: 122346,56 руб.
- Экономия времени за одно голосования: 3,5 часа
- Условная экономия на заработной плате за год, в среднем 5 голосований за день: 1 808 152 руб.

Спасибо за внимание