

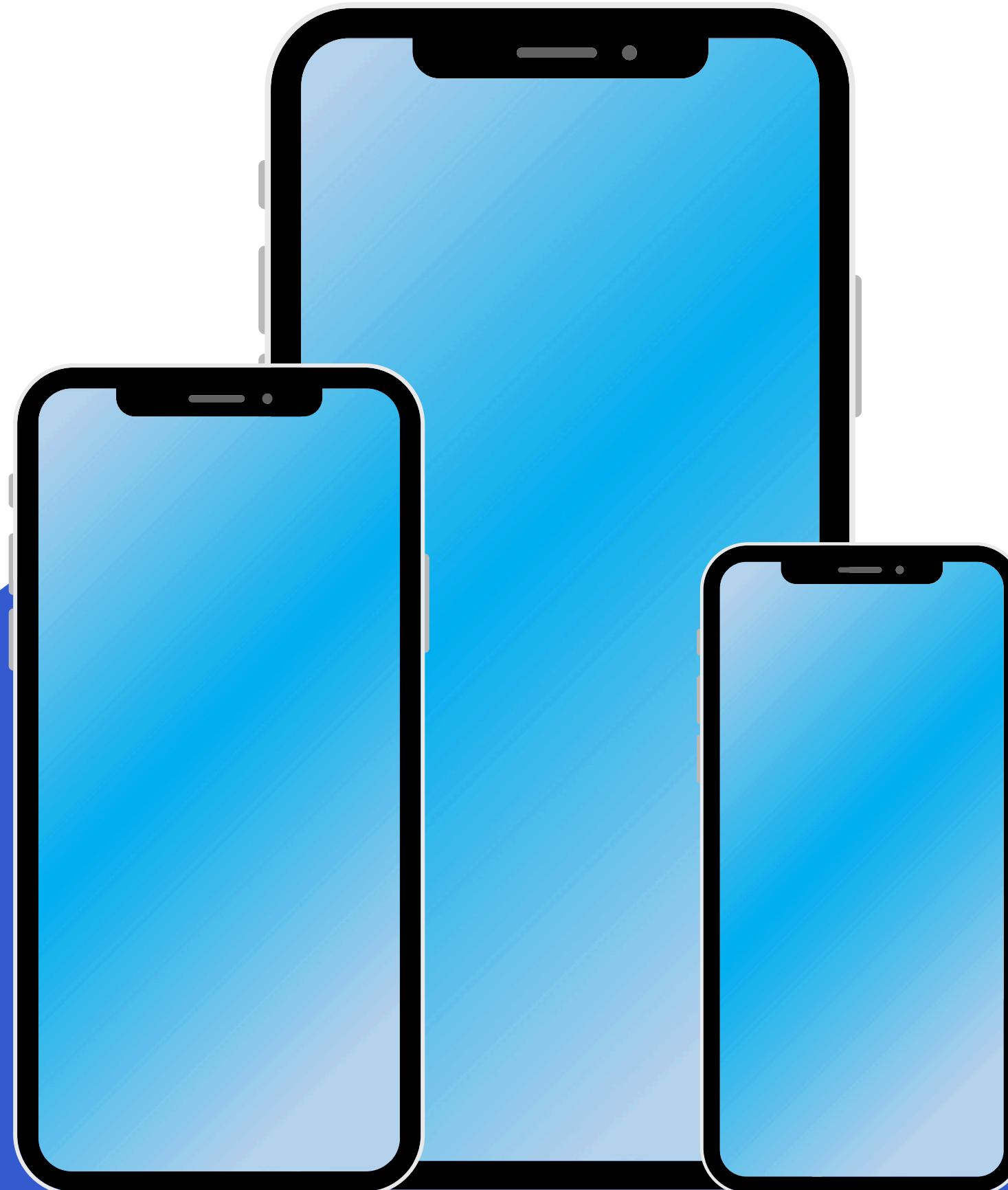


Проектная работа по дисциплине :
«Проектирование информационных систем» тема:
«Использование криптографических методов для
защиты данных на малых и средних
предприятиях»

Выполнили: Меирханова А., Камекова А., Вербилов А., Рағыт М., Кунаев Н.

Группа: УС2-ИС-25-2р

Проверил: Ғазиз Талғатұлы



План

Что такое криптографический метод?

Зачем нужны криптографические методы?

Какие виды существуют?

Какие виды в проекте были реализованы?

Диаграммы

Значимость методов шифрования в реальных
кейсах

Конечный продукт

Что такое криптографические методы шифрования

Криптографические методы — это набор математических алгоритмов и техник для защиты информации путем ее [шифрования](#) (преобразования в нечитаемый код), обеспечения целостности данных, подтверждения подлинности и авторизации, используя ключи, хэш-функции и цифровые подписи, чтобы только авторизованные лица могли получить доступ к данным при их хранении или передаче.



Зачем они нужны? (актуальность)

META UNIVERSITY



01

Конфиденциальность: Шифрование делает данные доступными только тем, кто имеет ключ. Это защищает личную информацию, пароли, банковские данные и государственные секреты от перехвата.

02

Целостность: Гарантирует, что информация не была изменена во время передачи или хранения. Например, хэш-функции проверяют, не был ли файл подделан.

03

Аутентификация: Подтверждает, что отправитель и получатель — это те, за кого себя выдают (например, цифровые подписи).

04

Неотказуемость: Цифровые подписи не позволяют отправителю отрицать факт отправки, а получателю — факт получения сообщения.

В 2025 году кибермошенничество в Казахстане достигло тревожных масштабов:

По данным МВД РК, с начала года совокупный ущерб от преступлений, связанных с криптоактивами, превысил 8 миллиардов тенге. За последние годы зарегистрировано свыше тысячи уголовных дел в этой сфере, из них:

- 60% — **прямое мошенничество** (например, фальшивые инвестиционные платформы и пирамиды),
- 25% — **незаконная деятельность криптообменников**,
- 15% — **отмывание денег через цифровые активы**.

Общее интернет-мошенничество показало рост на 22% по сравнению с прошлым годом: зарегистрировано свыше 14 тысяч случаев только за первые месяцы, с ущербом более 6 миллиардов тенге.

Какие виды существуют?

META UNIVERSITY



Симметричный
(1 ключ)

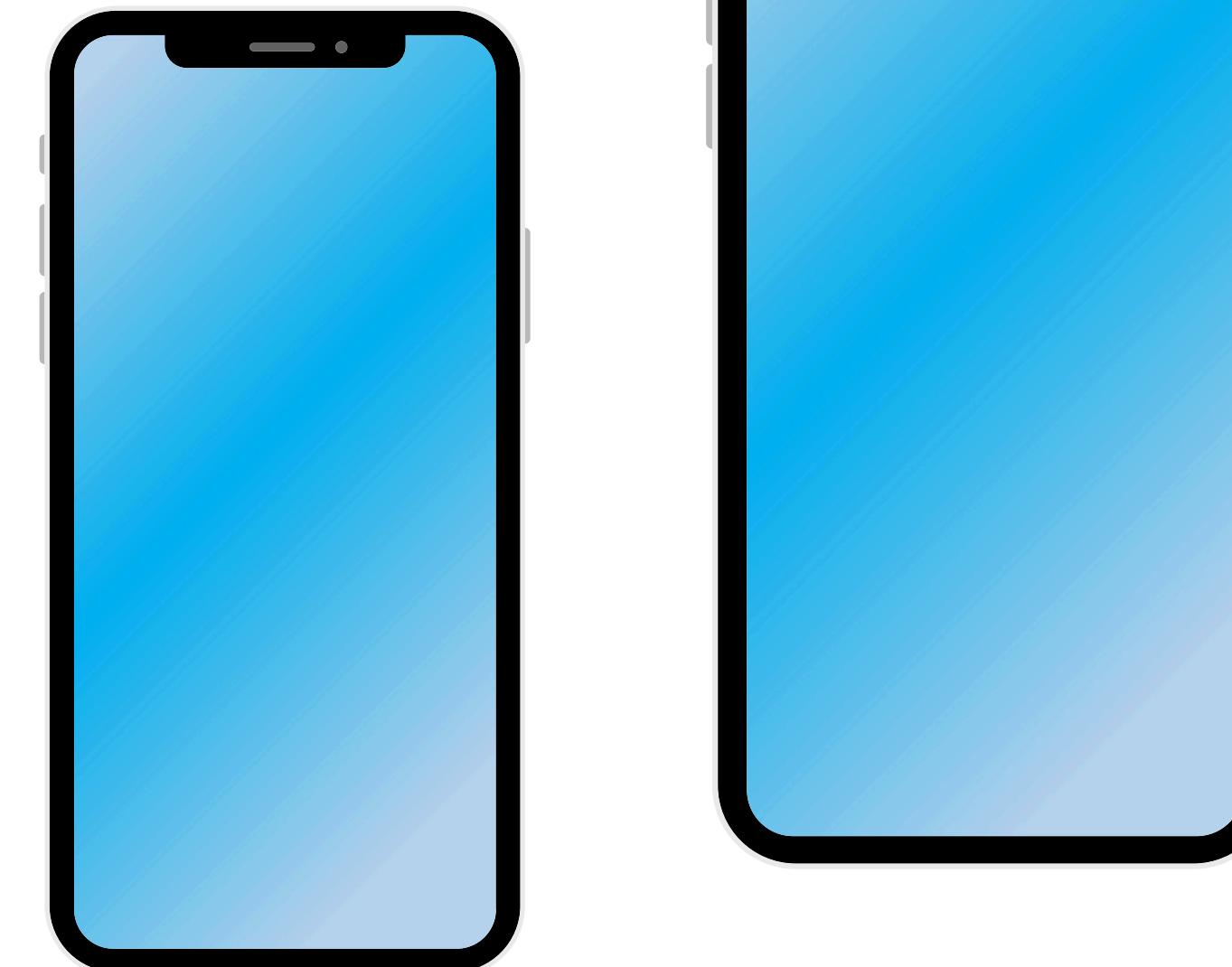
Ассиметричный
(2 ключа)

Смешанный

Асимметричное шифрование —

Асимметричное шифрование — это метод защиты данных, где используются два разных ключа:

- Публичный (открытый) ключ — его можно свободно раздавать всем. Он используется для шифрования сообщения.
- Приватный (закрытый) ключ — хранится в строгом секрете у владельца. Он нужен для расшифровки.



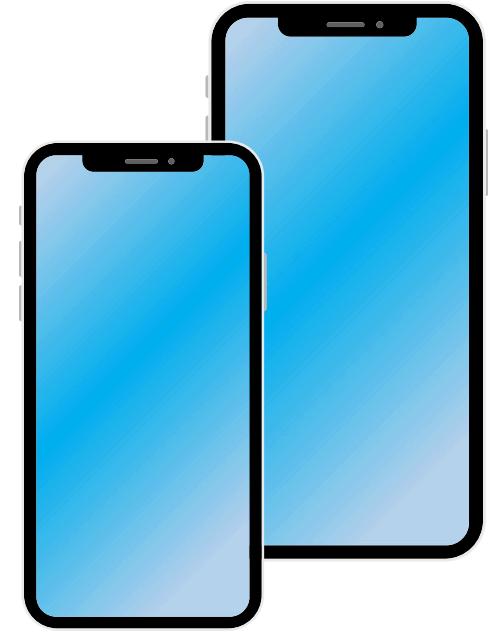
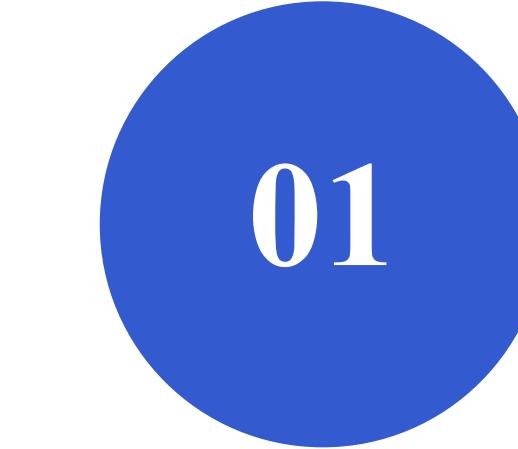
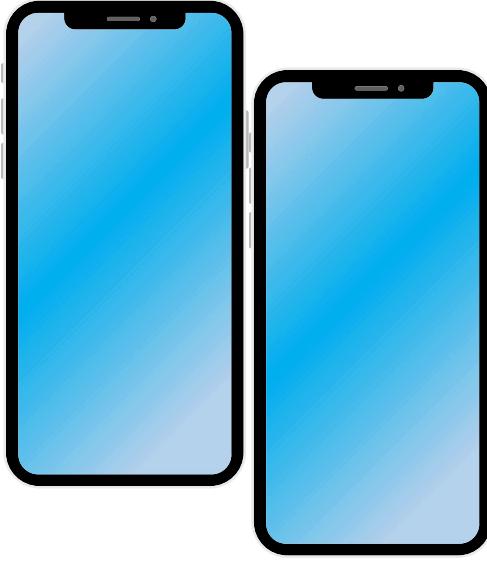
Симметричное шифрование —

Симметричное шифрование — это способ защиты данных, при котором для шифрования (зашифровки) и дешифрования (расшифровки) используется один и тот же секретный ключ. Этот ключ должен быть известен обеим сторонам заранее (отправителю и получателю), и он хранится в тайне. Без ключа данные выглядят как бессмысленный набор символов.



Смешанное шифрование —

Смешанное (гибридное) шифрование — это метод защиты данных, который комбинирует симметричное и асимметричное шифрование, чтобы взять лучшее от обоих подходов и устраниить их основные недостатки.



Криптосистема Rabin — это асимметричный алгоритм шифрования, предложенный Майклом Рабином в 1979 году. Он основан на сложности факторизации больших чисел (как и RSA), но использует квадратичные вычеты по модулю составного числа. Для шифрования используется открытый ключ, а для расшифровки — закрытый (секретные простые множители).

02

ECC(Elliptic Curve Cryptography — Криптография на эллиптических кривых)

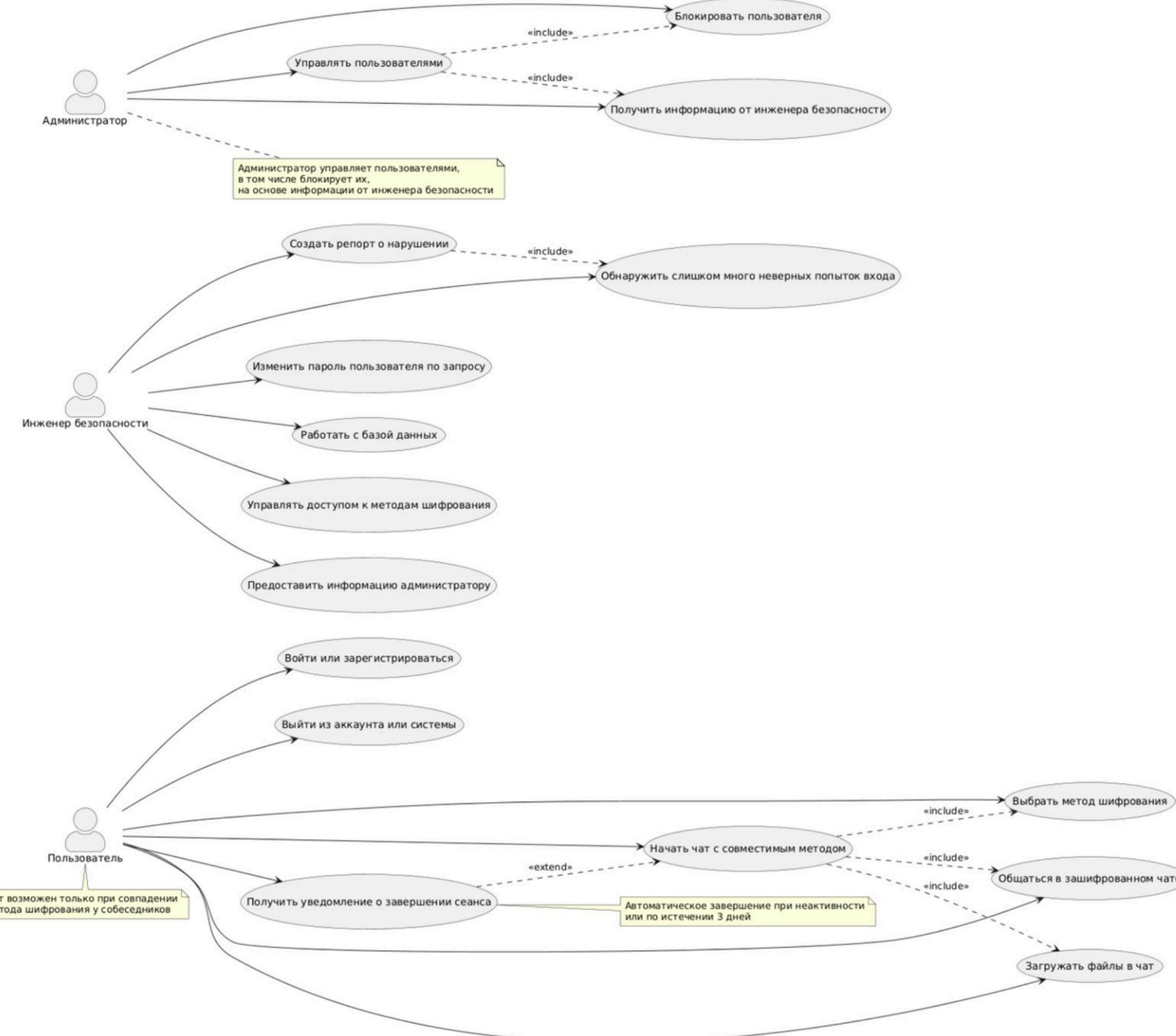
— это асимметричный криптографический метод, основанный на алгебраических свойствах эллиптических кривых над конечными полями. Он использует задачу дискретного логарифма на эллиптической кривой, которая значительно сложнее, чем факторизация или обычный дискретный логарифм.

Диаграммы

META UNIVERSITY



Use Case



Текст абзаца

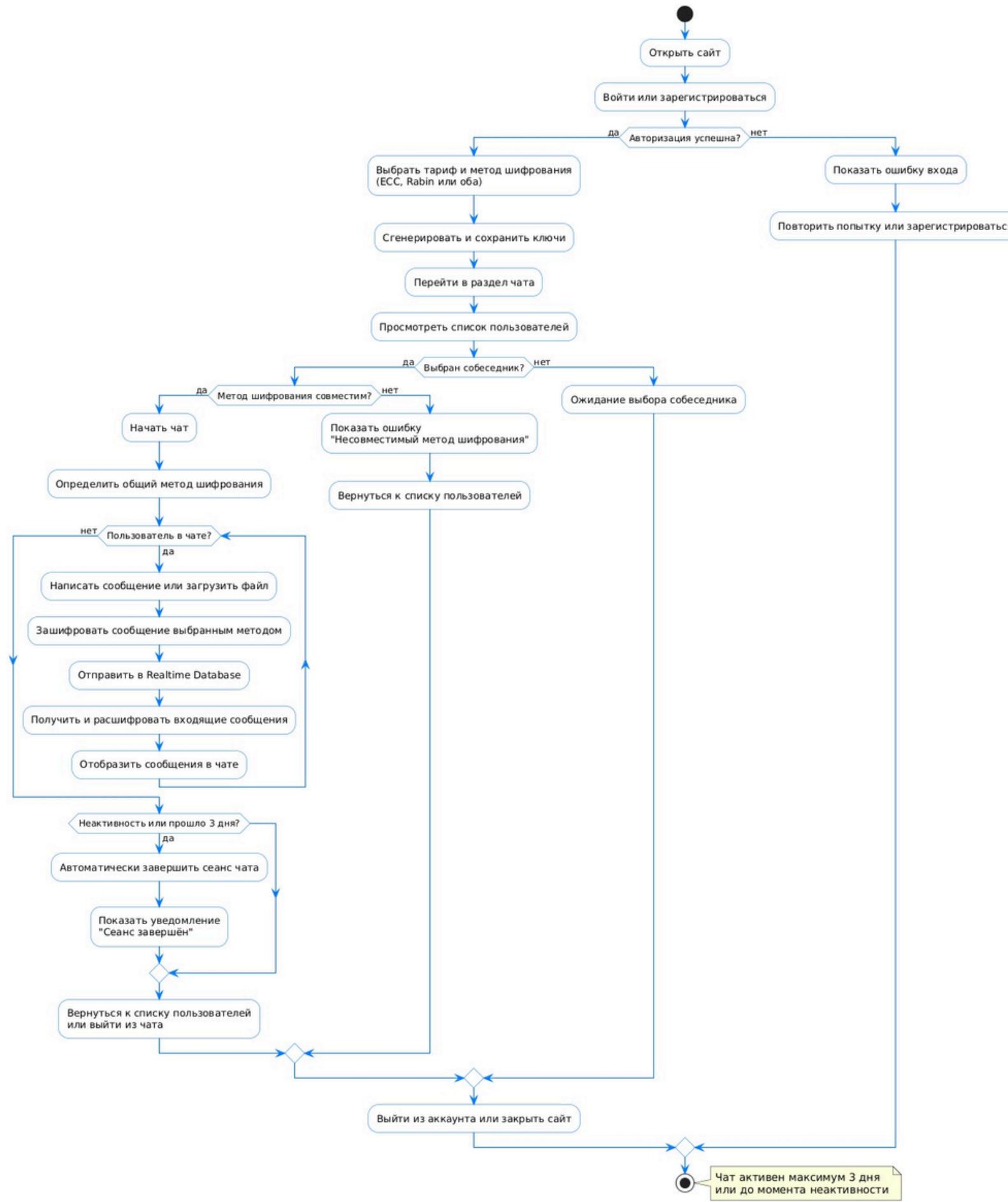


диаграмма деятельности

диаграмма классов

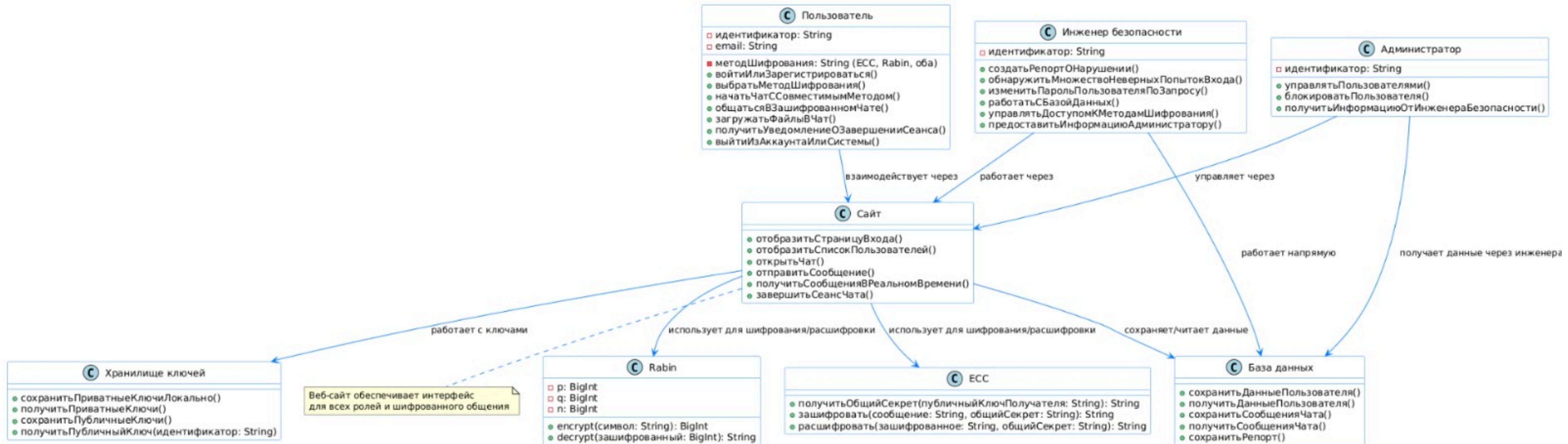


диаграмма пакетов

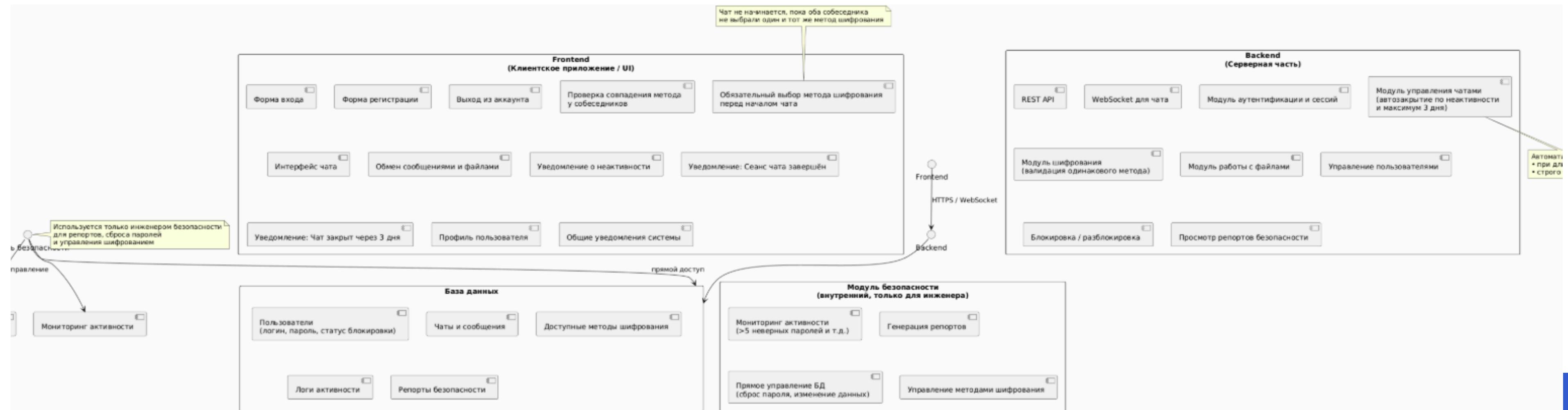
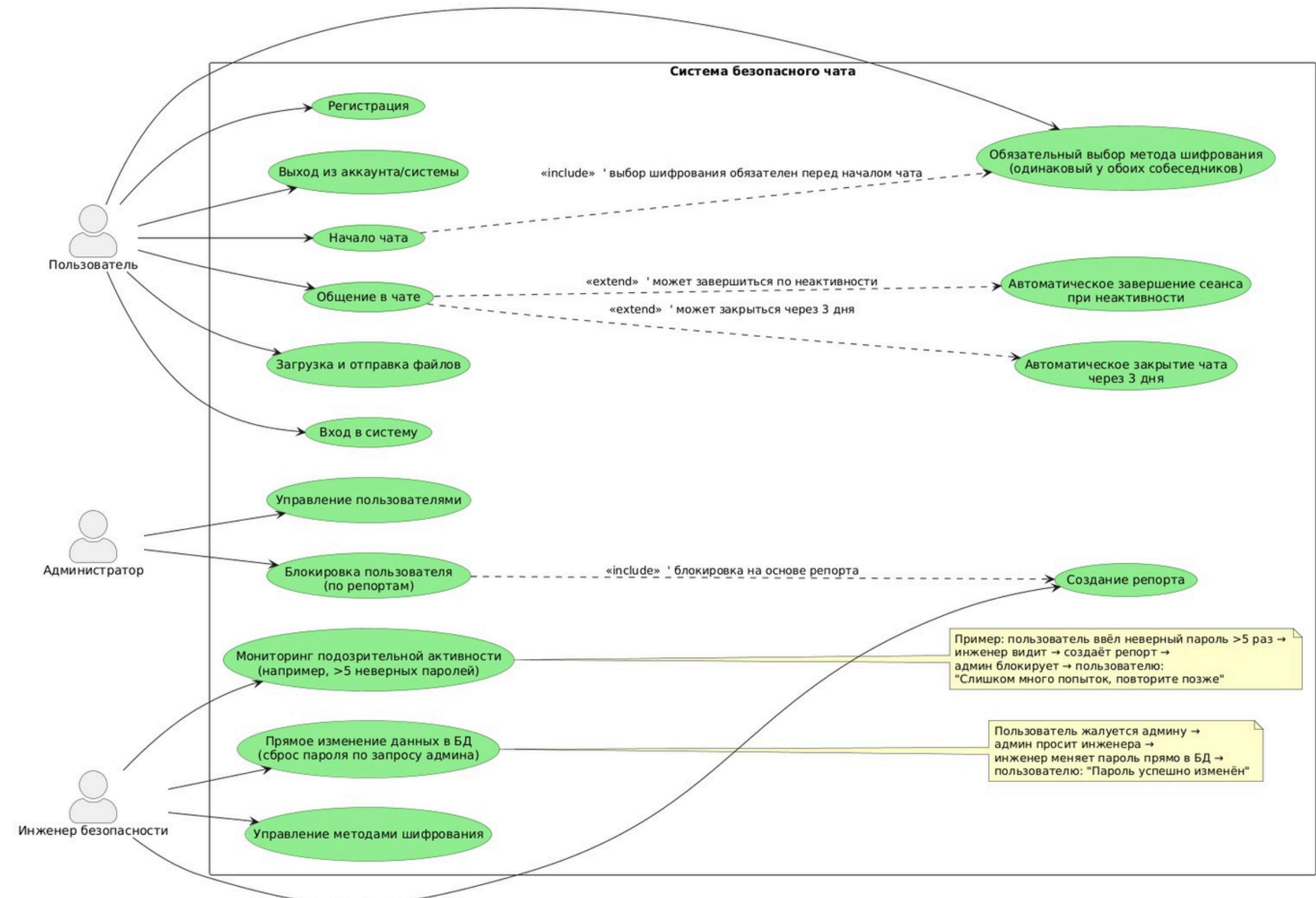


диаграмма precedентов



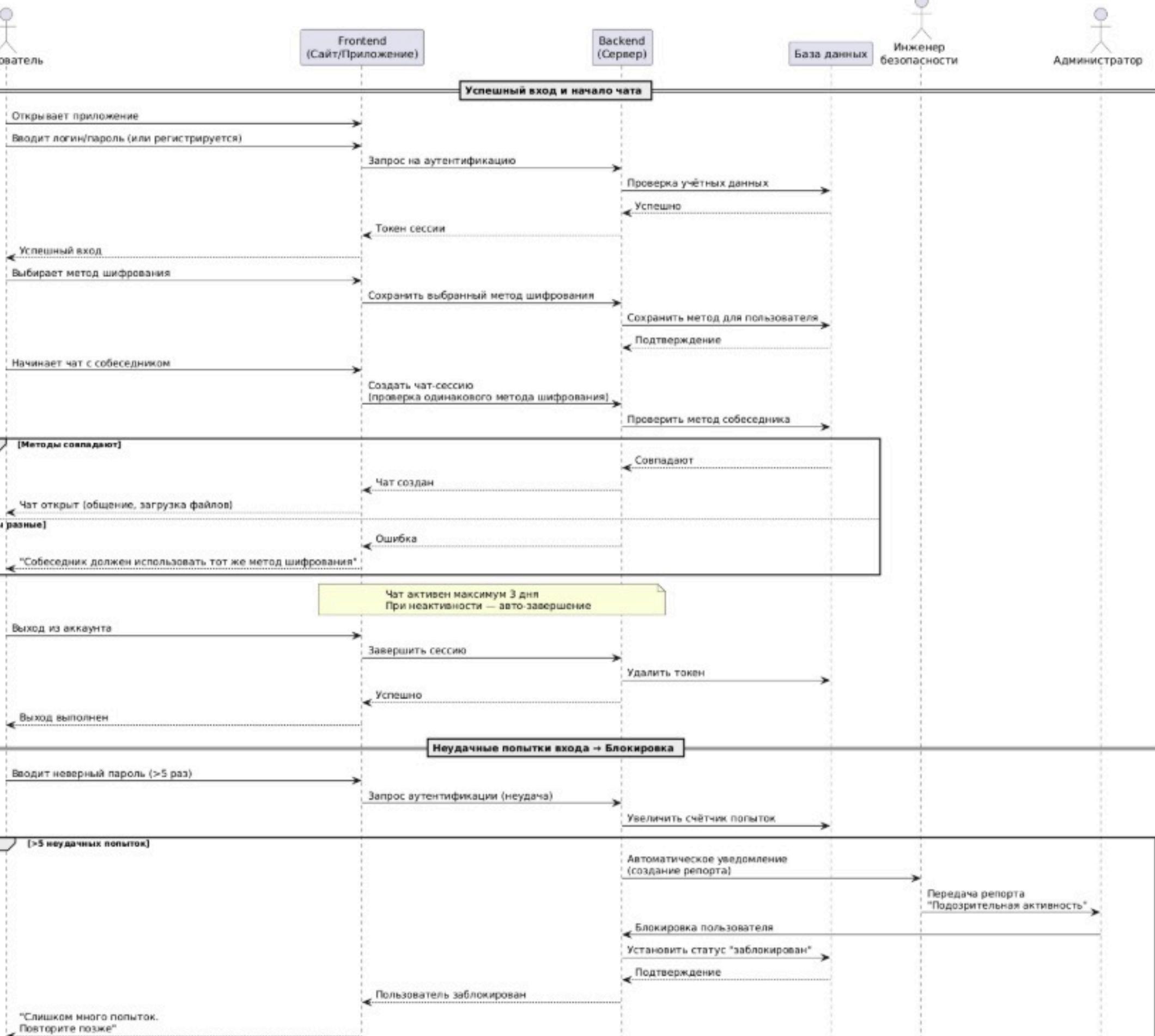
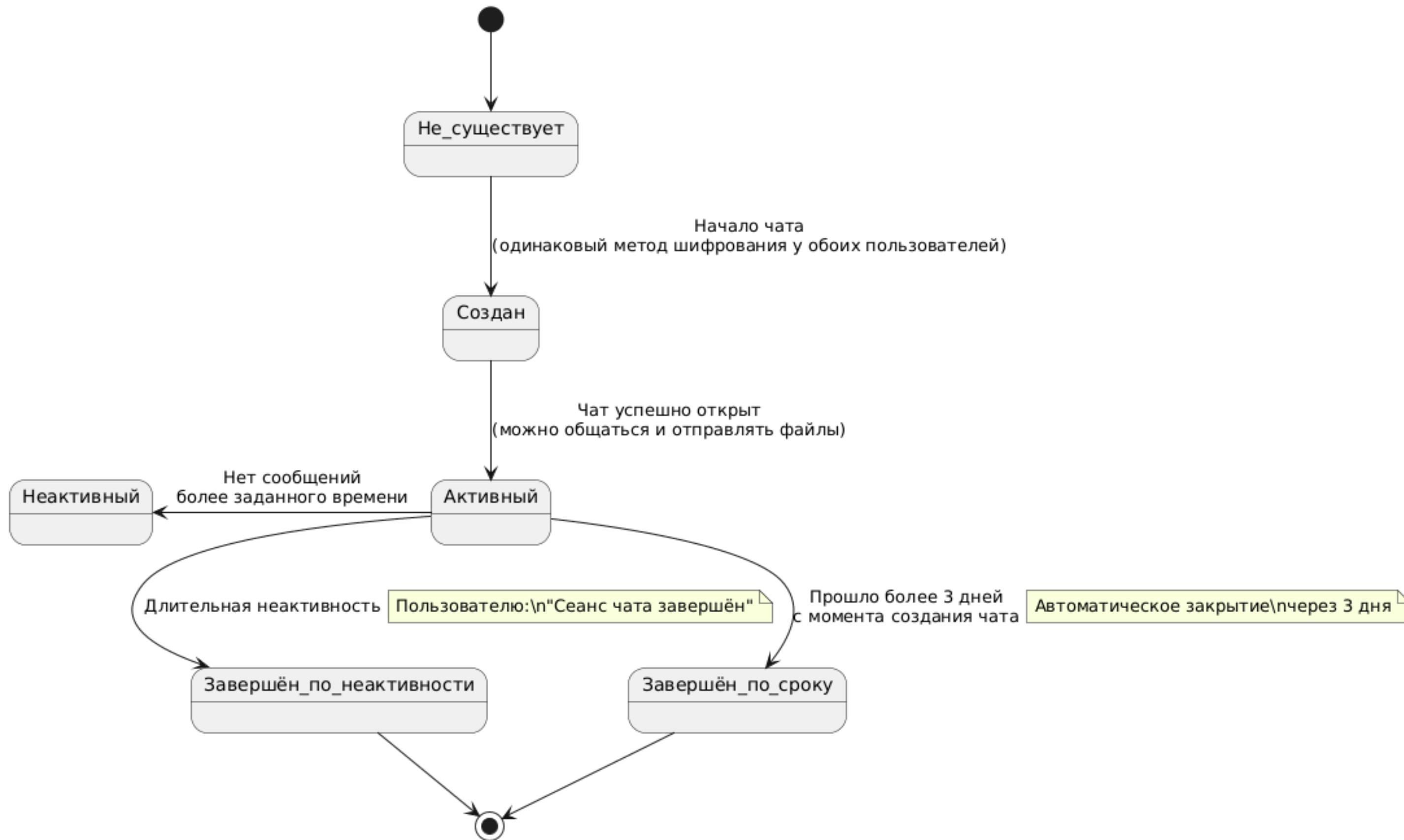


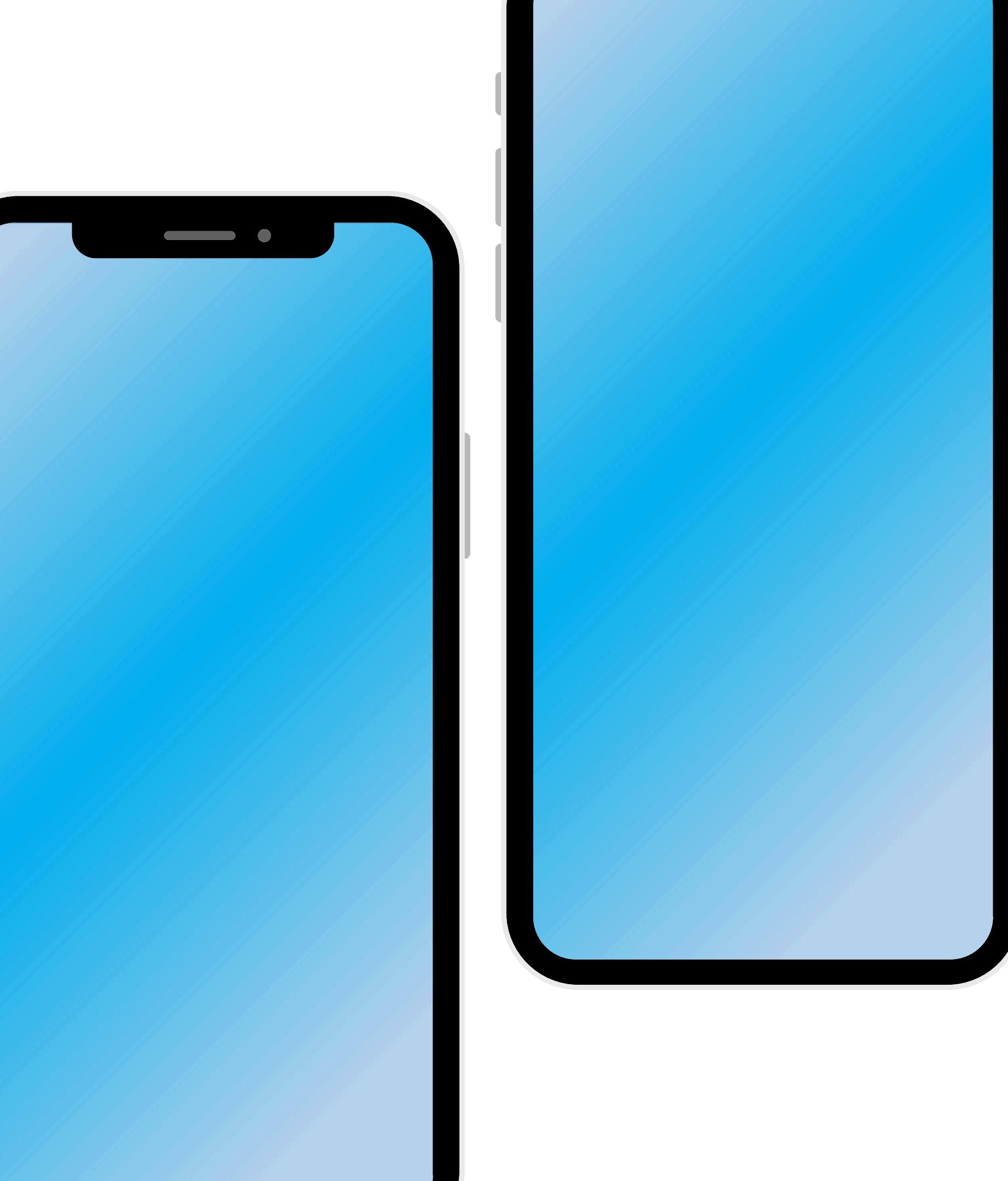
диаграмма взаимодействия

диаграмма жизненный цикл

META UNIVERSITY



Значимость методов шифрования в реальных кейсах



Утечки персональных данных — реальность: в 2025-м стало известно, что данные ≈ 16 млн граждан Казахстана (фамилии, ИИН, адреса, телефоны и др.) были скомпрометированы и оказались в открытом доступе.

В течение 2025-го официально зарегистрированы 43 крупных инцидента утечки критических данных (личные данные, базы, возможно — корпоративные).

По международному рейтингу National Cyber Security Index (NCSI) — для 2023 года: Казахстан занял 78-е место из 176 стран, с общим баллом $\sim 48\%$.

По другим источникам, жертвы интернет-мошенников за 2024 г. потеряли 7,1 млрд тенге за семь месяцев — из них 6,8 млрд тенге — физлица, 304,1 млн — юрлица.

Кроме атак на системы, распространено мошенничество в интернете: в 2024 году ущерб, причинённый онлайн-мошенниками, по разным оценкам, составил 11,4 млрд тенге (по данным судебной статистики)

Конечный продукт

[Главная](#)[Тарифы](#)[Чат](#)

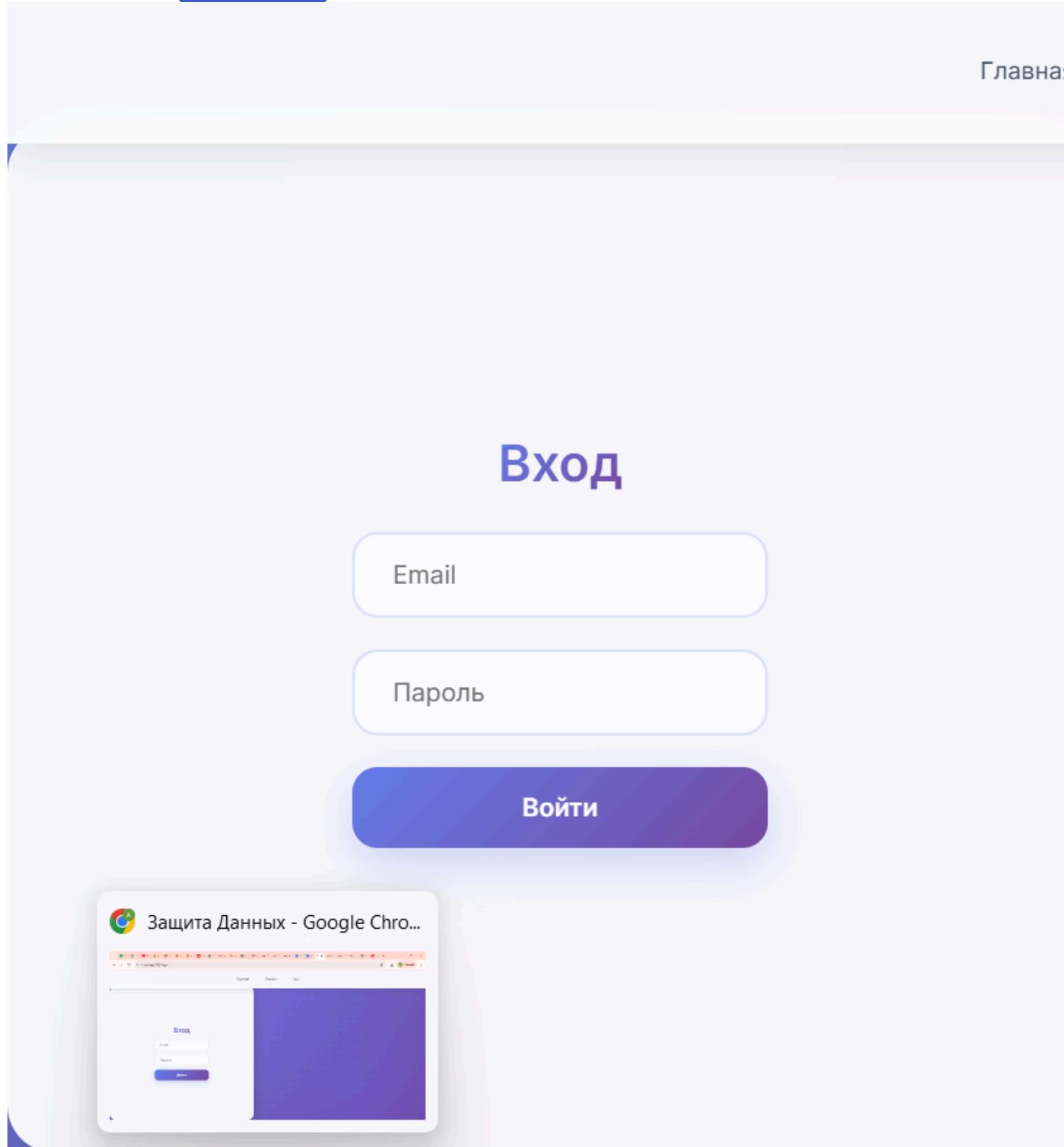
Добро пожаловать на
платформу для защиты
данных!

Наш сайт посвящен использованию криптографических методов
(ECC и Rabin) для безопасного обмена данными.

[Регистрация](#)[Войти](#)

Конечный продукт

META UNIVERSITY



Главная Тарифы Чат

Вход

Email

Пароль

Войти

Защита Данных - Google Chro...

A screenshot of a web application showing a login form. The title of the page is 'Вход' (Login). It features two input fields: 'Email' and 'Пароль' (Password), both with placeholder text. Below them is a large blue button labeled 'Войти' (Enter). At the bottom left, there is a small preview window showing the same login interface on a mobile device. The background of the main page is purple.

Конечный продукт

META UNIVERSITY

Главная Тарифы Чат Админ Выйти

Админ-панель

Управление пользователями

Все пользователи

fuck18283
Email: fuck1@gmail.com
Роль: user
Статус: Активен

Заблокировать

test1296
Email: test@test.com
Роль: user
Статус: Активен

Заблокировать

arug1652
Email: arug1652@gmail.com
Роль: admin
Статус: Активен

Заблокировать

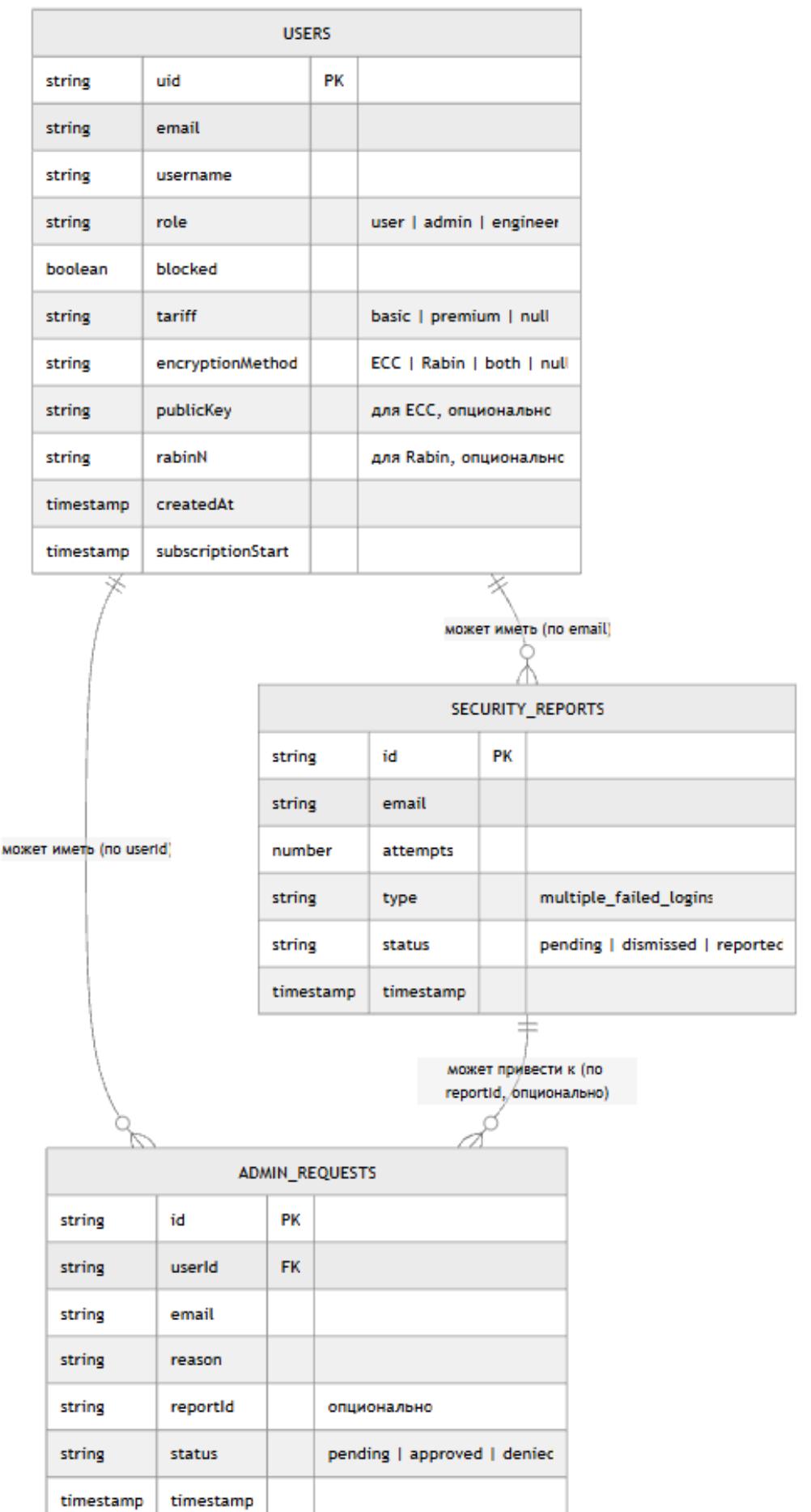
Конечный продукт

[Главная](#)[Тарифы](#)[Чат](#)[Безопасность](#)[Выйти](#)

Панель безопасности

Отчеты о подозрительной активности

Нет активных отчетов



ER

диаграмма

Архитектура сайта

META UNIVERSITY

- **Frontend:** Pure Vanilla JS (**SPA с клиентским роутингом via history API**)
- **Backend:** Firebase (**No server-side logic в client-коде**)
 - **Authentication:** Firebase Auth (**email/password**)
 - **Database:** Firestore (**users, security_reports, admin_requests**) + Realtime DB (**возможно для чата**)
- **Шифрование:** Клиентское (ECC via elliptic.js, Rabin custom)
- **Хостинг:** Firebase Hosting (**public/ как root**)
- **Поток данных:** Клиент ↔ Firebase напрямую (**real-time listeners для чата/отчетов**)

```
ENCRYPTION/
├── node_modules/
└── public/
    ├── app.js
    ├── index.html
    └── styles.css
├── .firebaserc
├── .gitignore
└── package-lock.json
├── package.json
└── server.js
```

Анализ требований проекта

Проект представляет собой веб-приложение для безопасного обмена сообщениями с использованием криптографических методов шифрования (ECC и Rabin). Основная цель — демонстрация клиентского энд-то-энд шифрования данных при передаче через публичный канал (Firebase).

Ключевые функциональные требования:

- Регистрация и аутентификация пользователей через Firebase Auth (email/password).
- Выбор тарифного плана (Базовый — один метод шифрования, Премиум — оба метода).
- Безопасный чат с end-to-end шифрованием (ECC на базе secp256k1 или крипtosистема Рабина).
- Генерация и обмен публичными ключами между пользователями.
- Ролевая модель доступа: обычный пользователь, инженер безопасности, администратор.
- Мониторинг подозрительной активности (множественные неудачные попытки входа) с автоматической генерацией отчётов.
- Двухуровневая система реагирования: инженер безопасности анализирует отчёты → передаёт запрос администратору → блокировка/разблокировка пользователя.

Нефункциональные требования:

- Полностью клиентское шифрование (приватные ключи хранятся только в localStorage браузера).
- Responsive дизайн с современным UI (glassmorphism, анимации).
- Одностраничное приложение (SPA) с клиентским роутингом.
- Развёртывание на Firebase Hosting с использованием Firestore для хранения метаданных пользователей и отчётов.

Проект сочетает образовательные цели (демонстрация ECC и Рабина) с практическими аспектами безопасности: ролевой доступ, обнаружение атак brute-force и административное управление пользователями.

Использованная литература

1. **Elliptic library** (для ECC на кривой secp256k1, ECDH и генерации ключей): GitHub: <https://github.com/indutny/elliptic> Документация и примеры ECDH.
2. **Rabin cryptosystem** (основы алгоритма, генерация Blum primes $\equiv 3 \pmod{4}$, дешифровка квадратных корней): https://en.wikipedia.org/wiki/Rabin_cryptosystem GeeksforGeeks (пример реализации): <https://www.geeksforgeeks.org/java/rabin-cryptosystem-with-implementation/>
3. **ECDH с симметричным шифрованием (XOR-шифр на основе derived shared secret, обработка UTF-8)**: MDN Web Crypto API (`deriveKey/deriveBits`): <https://developer.mozilla.org/en-US/docs/Web/API/SubtleCrypto/deriveKey> Примеры XOR на ECDH: <https://www.asecuritysite.com/encryption/js08>
4. **Firebase (авторизация, Firestore, Realtime Database в веб-приложениях)**: Официальная документация: <https://firebase.google.com/docs/auth/web/start> <https://firebase.google.com/docs/database/web/start>
5. **Обработка UTF-8 в JavaScript (encodeURIComponent/escape для байтового XOR)**: Stack Overflow / MDN: <https://stackoverflow.com/questions/13356493/decode-utf-8-with-javascript> `TextEncoder/TextDecoder`

Спасибо за внимание!

<https://github.com/progenel/project/>