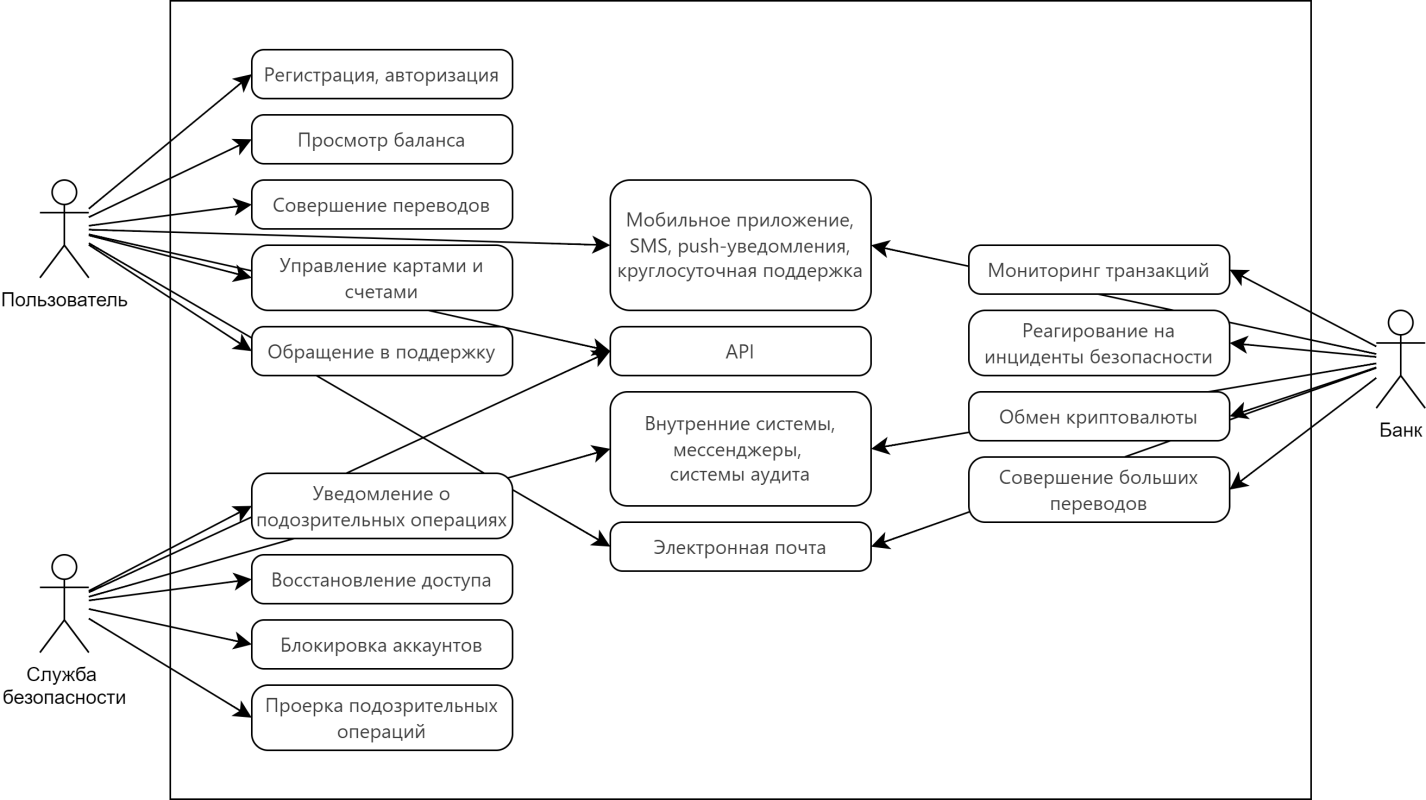
**Варианты использования**

**(Даненко Д.A., Луценко Д.А., Харлова А.А.)**

**Банковское приложение "E-Bank"**



|  |  |
| --- | --- |
| **Основное действующее лицо** | **Вариант использования** |
| Пользователь (клиент банка) | 1. Регистрация в приложении через ввод персональных данных и подтверждение через SMS. 2. Вход в приложение с использованием логина и пароля или биометрических данных. 3. Просмотр баланса на банковских счетах, картах и криптовалютных кошельках. 4. Совершение денежных переводов на другие счета (внутри банка, сторонние банки, криптокошельки). 5. Открытие новых счетов (фиатных и криптовалютных). 6. Заказ банковских карт (фиатных и криптовалютных). 7. Создание вкладов (фиатных и криптовалютных). 8. Обмен фиатных валют на криптовалюту и наоборот. 9. Просмотр истории транзакций (переводы, обмены, пополнения, списания). 10. Управление криптовалютными активами (покупка, продажа, хранение). 11. Настройка уведомлений о транзакциях, обновлениях баланса и изменениях курсов криптовалют. 12. Оплата услуг (коммунальные платежи, мобильная связь, интернет и т.д.). 13. Пополнение мобильного телефона через приложение. 14. Установка лимитов на расходы по картам и транзакциям. 15. Использование функций "Оплатить по QR-коду" или "NFC-платежи". 16. Смена пароля или восстановление доступа к аккаунту. 17. Просмотр акций и предложений от банка (например, кредиты, вклады, страхование). 18. Обращение в круглосуточную техническую поддержку через чат или звонок. 19. Совершение больших переводов с лояльными условиями (без ограничений по сумме). |
| Банк (администратор) | 1. Мониторинг активности пользователей и транзакций. 2. Отправка уведомлений пользователям о новых услугах, акциях или изменениях в приложении. 3. Блокировка аккаунта пользователя в случае подозрения на мошенничество. 4. Выпуск новых карт и счетов для пользователей через приложение. 5. Предоставление технической поддержки пользователям через чат или звонок. 6. Управление курсами обмена фиатных валют на криптовалюту и наоборот. 7. Обеспечение безопасности операций с криптовалютой и большими переводами. |
| Служба безопасности банка | 1. Мониторинг транзакций на предмет подозрительной активности. 2. Блокировка аккаунта пользователя при обнаружении мошеннических операций. 3. Проверка безопасности данных пользователей при регистрации и авторизации. 4. Реагирование на утечки данных и их предотвращение. 5. Обеспечение защиты криптовалютных кошельков и транзакций. 6. Проведение аудита систем безопасности приложения. 7. Установка и обновление систем антивирусной защиты и антиспама. 8. Обучение сотрудников банка и пользователей по вопросам безопасности. 9. Реагирование на инциденты безопасности (например, взломы, DDoS-атаки). 10. Разработка политик безопасности для защиты данных и операций. |