УДК 336.71

ПОВЫШЕНИЕ БЕЗОПАСНОСТИ НА РЫНКЕ ИНТЕРНЕТ-УСЛУГ МЕТОДОМ МНОГОФАКТОРНОЙ АУТЕНТИФИКАЦИИ ПОСРЕДСТВОМ ТОТР

Д.А. РОДИОНОВА
(Представлено: И.А. СТРОГАНОВА)

Статья посвящена повышению качества обслуживания физических лиц и конкурентоспособности ОАО «АСБ Беларусбанк» путём внедрения многофакторной аутентификации на основе ТОТР. Подчёркивается значение усиления информационной безопасности для развития интернет-услуг и укрепления доверия клиентов.

Современные вызовы в области кибербезопасности требуют от банков усиления механизмов защиты данных. Учитывая рост количества мошеннических атак, переход на ТОТР вместо SMS-аутентификации позволит снизить риски фишинговых атак, социальной инженерии и перехвата паролей. Кроме того, этот метод соответствует глобальным стандартам безопасности, принятым в крупнейших финансовых организациях мира, обеспечивая защиту средств клиентов и укрепляя репутацию банка.

Многофакторная аутентификация (МФА) посредством ТОТР (Time-Based One-Time Password) представляет собой эффективный способ повышения безопасности в банковской сфере за счёт использования динамически генерируемых одноразовых паролей, действующих в течение ограниченного времени. Этот метод требует от пользователя, помимо основного фактора – например, логина и пароля, – ввести временный код, который создаётся с помощью специального приложения (например, Google Authenticator или аналогичного генератора ТОТР) на основании синхронизации с текущим временем. Код меняется каждые 30 или 60 секунд, и, даже если он будет перехвачен злоумышленником, его использование становится невозможным после истечения срока действия.

Данный метод авторизации обеспечивает дополнительную, двухэтапную защиту аккаунта от взлома. Кроме того, ТОТР-авторизация не требует доступа к интернету для генерации кода, что делает ее универсальной.

Данная инициатива направлена на совершенствование качества обслуживания физических лиц, повышение уровня доверия к банковским сервисам, укрепление конкурентоспособности на рынке интернет-услуг и соответствие современным требованиям безопасности. Рассматриваемое мероприятие фокусируется на усилении защиты клиентских данных и операций.

МФА с использованием ТОТР обеспечивает прозрачность и надежность процессов аутентификации и подтверждения операций, что способствует укреплению имиджа банка как технологически продвинутой и ответственной организации.

Разработанный метод основан на принципе двухфакторной аутентификации, где кроме традиционного логина и пароля используется дополнительный одноразовый код (рисунок 1), который генерируется в мобильном приложении банка и обновляется через фиксированные промежутки времени. В отличие от стандартного метода SMS-аутентификации, использование ТОТР исключает зависимость от мобильной сети и снижает риски перехвата сообщений злоумышленниками.

ТОТР может быть интегрирован в мобильное приложение ОАО «АСБ Беларусбанк» M-Belarusbank, обеспечивая безопасный доступ к учетной записи без необходимости получения SMS-кодов. Клиенты смогут активировать функцию одноразовых паролей, используя QR-код для привязки приложения к банковской системе. При каждом входе в систему будет требоваться ввод сгенерированного пароля, который действителен только в течение короткого времени и не может быть повторно использован, а также доступен только на устройстве пользователя.

Основные направления проекта сосредоточены на:

1. Информационной безопасности: внедрение надежной системы аутентификации, повышающей защиту клиентских данных и снижающей вероятность несанкционированного доступа к счетам.
2. Соответствии законодательству: обеспечение соответствия требованиям национальных и международных стандартов по защите данных, включая внедрение многофакторной аутентификации как обязательного элемента безопасности.
3. Повышении доверия клиентов: внедрение механизма, гарантирующего надежность входа в систему интернет-банкинга, снижение вероятности взлома учетных записей и формирование уверенности клиентов в безопасности их данных.

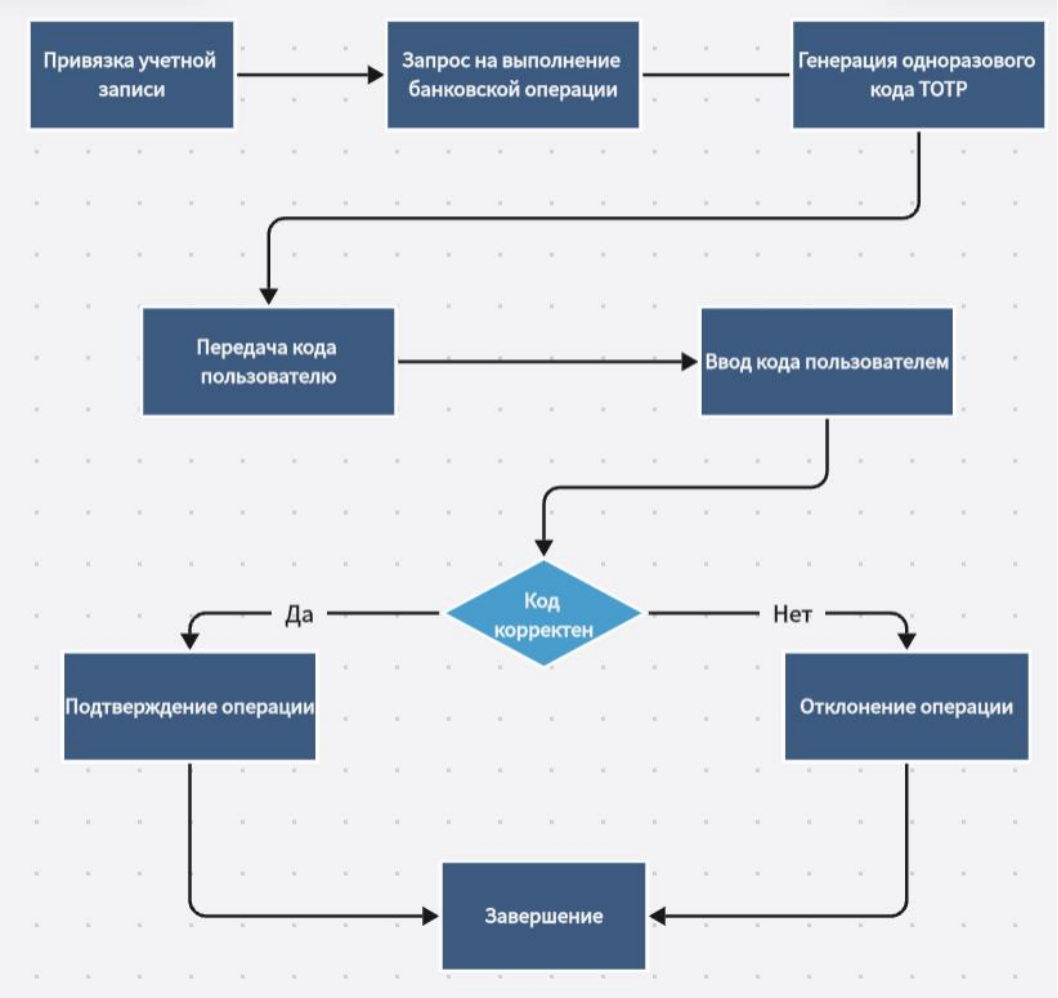

Рисунок 1. – Алгоритм работы TOTP в мобильном приложении

Источник: собственная разработка.

Метод многофакторной аутентификации посредством TOTP (Time-Based One-Time Password) может быть применен в мобильном приложении банка не только для безопасного входа в систему, но и для защиты других важных операций:

1. Подтверждение транзакций – клиент может использовать TOTP для подтверждения платежей, перевода средств или изменения настроек аккаунта, вместо SMS-кодов. Это значительно повышает безопасность и исключает вероятность перехвата сообщений злоумышленниками.
2. Авторизация при смене устройств – если клиент устанавливает приложение на новый смартфон, система может запрашивать TOTP-код для подтверждения его личности. Это предотвратит попытки несанкционированного входа с чужих устройств.
3. Дополнительная защита при изменении персональных данных – любые изменения данных клиента (например, номера телефона или электронной почты) могут требовать подтверждения через TOTP. Это повысит безопасность и снизит риск мошеннических действий.
4. Ограничение доступа к определенным функциям – некоторые операции, такие как запрос на крупный кредит или управление инвестициями, могут требовать дополнительного уровня подтверждения. Использование TOTP поможет усилить контроль за такими транзакциями.
5. Восстановление доступа без обращения в банк – если клиент забыл пароль, восстановление аккаунта можно сделать через TOTP, исключая необходимость звонка в колл-центр или посещения отделения банка.

Таким образом, разработанный метод многофакторной аутентификации посредством TOTP представляет собой эффективное решение для повышения безопасности банковских сервисов, усиления защиты учетных записей и укрепления доверия клиентов. Внедрение данной технологии в интернет-банкинг ОАО «АСБ Беларусбанк» позволит повысить надежность финансовых операций, соответствовать требованиям информационной безопасности и улучшить конкурентные позиции банка в цифровой сфере.

ЛИТЕРАТУРА

1. Методы аутентификации пользователей в интернете [Электронный ресурс]. – Режим доступа: https://seferisrael.co.il/catalog/category/книги/науки-и-образование/page/859/?view=grid&v=df3f079de696. – Дата доступа: 22.06.2025.
2. Kaspersky daily «Двухфакторная аутентификация» [Электронный ресурс]. – Режим доступа: https://www.kaspersky.ru/blog/what_is_two_factor_authenticatio/4272. – Дата доступа: 22.06.2025.
3. Сравнительный анализ достоинств и недостатков наиболее распространенных методов идентификации и аутентификации пользователей и других участников идентификационных процессов [Электронный ресурс]. – https://cyberleninka.ru/article/n/sravnitelnyy-analiz-dostoinstv-i-nedostatkov-naibolee-rasprostranennyh-metodov-identifikatsii-i-autentifikatsii-polzovateley-i. – Дата доступа: 22.06.2025.