

БЕЗОПАСНОСТЬ ИНТЕРНЕТ-БАНКИНГА: СОВРЕМЕННЫЕ УГРОЗЫ И МЕТОДЫ ЗАЩИТЫ

Е.И. Лобандиевская, 2 курс

Научный руководитель – **К.С. Королёнок**, старший преподаватель
Белорусский национальный технический университет

С развитием информационных технологий и широким использованием интернета в различных финансовых операциях, интернет-банкинг стал неотъемлемой частью современного банковского обслуживания. Тем не менее, наряду со всеми его преимуществами, возникают вопросы безопасности и риска мошенничества.

Интернет-банкинг, или онлайн-банкинг, представляет собой использование интернет-платформ для выполнения банковских операций. Современные технологии открывают новые горизонты для управления финансами, позволяя пользователям проводить банковские операции в любое время и в любом месте. Тем не менее, этот элемент удобства ставит под угрозу безопасность персональных данных и средств клиентов. Сложные схемы мошенничества, фишинг и кибератаки становятся все более распространенными, что вызывает беспокойство у пользователей интернет-банков.

По данным Национального банка на 2024 год в Республике Беларусь 21 действующий банк и все предоставляют услуги интернет-банкинга. Первым в Беларуси открыл систему интернет-банкинга ОАО «Приорбанк» в 2004 году, однако она имела огромное количество недостатков, поэтому была отправлена на доработку и в 2008 году выпущена заново. На начало 2024 года, количество пользователей интернета в Республике Беларусь насчитывалось 8,48 млн. человек, и для многих банков развитие электронных банковских услуг стало стратегическим направлением деятельности [1].

В условиях широкого использования мобильных устройств, кроме классического интернет-банкинга, позволяющего использовать сервисы банка через компьютер, перспективным направлением стало развитие мобильного банкинга. Мобильный банкинг доступен на мобильных устройствах (смартфонах, планшетах) через специализированные приложения и позволяет выполнять операции в любое время и в любом месте, что делает его особенно удобным для осуществления простых транзакций (денежные переводы, оплата счетов и т.п.). Интернет-банкинг, как правило, требует больше времени для выполнения операций, так как пользователи чаще работают с более сложным интерфейсом.

Во многих случаях мобильные приложения могут предлагать дополнительные функции, например, возможность сканирования QR-кодов, управление картами через NFC, включая бесконтактные платежи, оплата одной кнопкой и т.д. Интернет-банкинг, в свою очередь, может предоставлять более полный и детализированный функционал, необходимый для сложных финансовых операций. [2]

Интернет-банкинг имеет ряд преимуществ по сравнению с обычным банком:

1. **Удобство и доступность:** пользователи могут осуществлять банковские операции в любое время в круглосуточном режиме, что исключает необходимость посещения банка. Удобный интерфейс веб-приложения позволяет легко находить нужные функции и управлять финансами со своего устройства.
2. **Экономия времени и средств.** Клиенты интернет-банкинга могут осуществить необходимые операции без ожидания очереди в банке, а также воспользоваться сниженными тарифами на услуги. Например, открыть депозит или получить кредит под более выгодный процент, осуществить перевод без комиссии, оформить карту на льготных условиях и т.п.
3. **Широкий спектр услуг.** Возможность мгновенных переводов между счетами, оплата коммунальных и мобильных услуг, налоговых счетов, заказ дебетовых и кредитных карт, открытие и пополнение вкладов, оплата штрафов и многие другие услуги.
4. **Управление счетами:** пользователи могут отслеживать свои расходы, получить выписку, анализировать финансовые отчеты и управлять несколькими счетами сразу.

Стоит отметить тот факт, что система дистанционного банковского обслуживания выгодна и для самих банков, т.к. они повышают свои конкурентные преимущества и привлекают новых кли-

ентов, а также снижается нагрузка на офисы и на сотрудников банка, что приводит к значительному сокращению финансовых издержек.

Несмотря на все преимущества, интернет-банкинг имеет некоторые недостатки. В первую очередь они связаны с несанкционированным доступом к банковским счетам третьих лиц. Следствием этого может быть совершение мошеннических или иных противоправных действий. Хотя банковские организации имеют очень высокий уровень защиты, ни одна система не может быть на 100% безопасной.

Самым популярным способом кражи информации на сегодняшний день являются фишинг: злоумышленники выдают себя за доверенные организации или лица. Они создают поддельные электронные письма или сообщения, которые выглядят как приходящие от известного банка, содержат логотипы и фирменные знаки для повышения узнаваемости, и просьбу перейти по ссылке для подтверждения учетной записи, восстановления доступа или проверки информации. Эти ссылки ведут на поддельные веб-сайты, которые внешне похожи на настоящие. На поддельном сайте пользователя просят ввести личные данные, логин и пароль, которые попадают к злоумышленнику.

Риск лишиться своих персональных данных для входа в онлайн-банкинг и доступа к счетам повышается и с утерей устройства, так как в большинстве случаев это приводит к проблемам с восстановлением доступа и несанкционированному использованию банковских приложений и данных.

Также к недостаткам можно отнести и отсутствие некоторого функционала в онлайн-банкинге. Хотя многие банки стремятся улучшить возможности своих интернет-сервисов, все же зачастую наблюдаются определенные ограничения на открытие сложных депозитов или управление инвестициями, а также на доступность полной информации о своих счетах или услугах, что связано, прежде всего, с обеспечением безопасности.

Для того чтобы сократить количество краж существуют эффективные методы защиты конфиденциальной информации, а именно:

- двухфакторная аутентификация,
- регулярное обновление программного обеспечения,
- мониторинг транзакций [3].

Однако со временем эти методы могут терять свою эффективность, поэтому разработка новых методов защиты становится крайне актуальной задачей. Для повышения уровня безопасности стали использовать интегрированные технологий анализа отпечатков пальцев, распознавания лиц и звуковой биометрии. Например, вместо SMS-кода можно использовать отпечаток пальца или голос человека для завершения денежных операций, это уменьшит уровень риска и усложнит задачу киберпреступникам.

В настоящее время, с учетом развития информационных технологий, прибегают к использованию искусственного интеллекта – на его основе разрабатывают и внедряют алгоритмы, способные анализировать поведение пользователей, предотвращать и выявлять угрозы, связанные с кражей денег.

Использование различных систем для хранения и обработки транзакционных данных также значительно усложняет процесс взлома. Разделение данных по множеству платформ или применение многоуровневой системы безопасности позволяют обеспечить защиту информации и снизить риск несанкционированного доступа.

Безопасность интернет-банкинга остается одной из самых актуальных тем в условиях современного развития технологий и постоянного роста числа киберпреступлений. Сочетание быстро развивающихся методов обеспечения безопасности конфиденциальных данных с осведомленностью и внимательностью пользователей является ключевым элементом в борьбе с угрозами для интернет-банкинга. Это позволит не только минимизировать риски, но и создать безопасную финансовую среду для пользователей.

Список использованных источников

1. Соколова, Н. А. Интернет-банкинг: состояние и перспективы развития в Республике Беларусь / Н. А. Соколова // Материалы четвертой международной научно-практической конференции по вопросам банков-

ской экономики, Пинск, 16-17 мая 2013 г. – Полесский государственный университет; редкол.: К. К. Шебеко [и др.]. – Пинск, 2013. – С. 264-266

2. Любимова, Е. А. Интернет-банкинг и мобильный банкинг: проблемы и перспективы развития / Е. А. Любимова // Финансовые рынки и банки. – 2022. – № 2 – С. 46-51.

3. Интернет-банкинг [Электронный ресурс]. – Режим доступа: https://spravochnick.ru/bankovskoe_delo/internet-banking. – Дата доступа: 23.03.2025.