

УДК 336.74

## Безопасность и защита интернет-платежей: современные вызовы и решения

Салов Игорь Владимирович, старший преподаватель, Уфимский университет науки и технологий, igo777rus@mail.ru

Ермолаева Арина Витальевна, студент, Уфимский университет науки и технологий, arina.ermolaeva2003@gmail.com

В данной статье всесторонне анализируется проблема безопасности электронных платежей в условиях интенсивной цифровизации экономики. Авторы проводят детальный анализ современных угроз, технологий защиты и правового регулирования интернет-платежей. Особое внимание уделяется сравнительному анализу платежных систем, методам противодействия мошенничеству и перспективам развития технологий безопасности в данной сфере.

Ключевые слова: кибербезопасность, электронная коммерция, платежные системы, защита персональных данных, фрод-мониторинг, биометрическая аутентификация, блокчейн-технологии.

Современный этап развития финансовых технологий характеризуется значительным ростом объема электронных платежей. Центральный банк Российской Федерации сообщает, что в 2023 г. доля безналичных расчетов в розничном сегменте достигла 75 %, а более 60 % транзакций осуществляется через мобильные приложения. Глобализация финансовых услуг и последствия пандемии ускорили переход потребителей на дистанционные каналы обслуживания, что поставило перед системами безопасности новые задачи.

Электронные платежные системы превратились в критическую инфраструктуру мировой экономики, что обуславливает необходимость разработки новых подходов к обеспечению их надежности. Масштабы совершаемых операций наглядно демонстрируют возможные последствия: даже при доле мошеннических транзакций в 0,1 % финансовые потери могут быть значительными.

К основным угрозам в сфере электронных платежей относятся утечка персональных данных, снижение доверия потребителей к участникам рынка, развитие мошеннических схем и прямые финансовые убытки. Полученные злоумышленниками сведения о клиентах (имена, адреса, контактные данные, платежная информация) реализуются на теневых интернет-площадках и впоследствии используются для противоправных действий. Потеря доверия пользователей к сервису или торговой площадке приводит к сокращению клиентской базы и значительным затратам на восстановление деловой репутации. Утечки персональных данных, кроме того, влекут за собой штрафные санкции в соответствии с действующим законодательством.

Современные схемы кибермошенничества можно условно классифицировать по трем направлениям: технические атаки, методы социальной инженерии и деятельность организованных преступных групп. К первой группе относятся фишинг, таргетированные атаки, распространение вредоносного программного обеспечения, а также эксплуатация уязвимостей в платежных шлюзах. Методы социальной инженерии включают скимминг, поддельные звонки от имени службы безопасности банка, а также вишинг (голововой фишинг). Организованная киберпреступность проявляется в создании поддельных интернет-магазинов, использовании схем кардинга и в операциях по отмыванию денежных средств через платежные системы.

Анализ практики показывает, что наиболее уязвимыми элементами в сфере электронных платежей являются устаревшие CMS интернет-магазинов, недостаточный уровень защиты API платежных систем, уязвимости мобильных банковских приложений, а также человеческий фактор, включающий ошибки как сотрудников, так и пользователей.

Технологии защиты электронных платежей базируются на многоуровневом подходе, включающем шифрование данных для обеспечения конфиденциальности при передаче информации, замещение реквизитов платежных карт уникальными идентификаторами, а также многофакторную аутентификацию, предполагающую использование нескольких методов верификации личности пользователя. Важным элементом защиты являются системы мониторинга и предотвращения мошенничества, работающие в режиме реального времени и позволяющие выявлять и блокировать подозрительные операции.

К современным протоколам безопасности относятся протокол трехдоменной защиты, предусматривающий адаптивную аутентификацию на основе оценки рисков, биометрическую проверку личности (распознавание лица и отпечатков пальцев) и встраивание в мобильные приложения; замещение платежных данных уникальными идентификаторами, что исключает хранение реквизитов карт у торговых организаций; а также блокчейн-решения, обеспечивающие неизменяемость транзакций, упрощающие аудит операций и снижающие издержки при международных переводах. Все большее распространение получают системы искусственного интеллекта, применяемые в фрод-мониторинге: они используют поведенческую аналитику, алгоритмы машинного обучения для выявления аномалий и блокировку подозрительных транзакций в режиме реального времени.

Правовое регулирование сферы электронных платежей в Российской Федерации опирается на комплекс нормативных актов. Основным является Федеральный закон от 27 июня 2011 г. N 161-ФЗ «О национальной платежной системе», регулирующий деятельность операторов платежных систем, операторов электронных денежных средств, банков-эмитентов и банков-эквайеров. Федеральный закон от 27 июля 2006 г. N 152-ФЗ «О персональных данных» устанавливает требования к обработке и защите персональных данных клиентов. Существенную роль играет Федеральный закон от 7 августа 2001 г. N 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма». Кроме того, Гражданский кодекс Российской Федерации и законодательство о защите прав потребителей регулируют вопросы договорных отношений при использовании электронных платежных сервисов и обеспечивают защиту интересов пользователей. Центральный банк Российской Федерации выступает ключевым регулятором, устанавливая требования к обеспечению безопасности, управлению рисками и защите прав потребителей посредством нормативных актов.

Повышение уровня безопасности интернет-платежей требует

участия всех участников экосистемы. Для пользователей целесообразно применять виртуальные карты с ограниченным лимитом, активировать уведомления о совершаемых операциях и регулярно обновлять мобильные банковские приложения. Для бизнеса ключевое значение имеют внедрение сертифицированных платежных шлюзов, проведение регулярного аудита безопасности и обучение персонала основам кибергигиены. Для регуляторов важными направлениями остаются развитие механизмов быстрого реагирования на инциденты, создание условий для внедрения криптографических решений, устойчивых к квантовым вычислениям, а также расширение международного сотрудничества в сфере противодействия киберпреступности.

#### Примечания

1. Колтынюк Б. А. Сетевая экономика: учебное пособие. СПб., 2013.
2. Мартынов В. Г., Андреев А. Ф., Кузнецов В. А., Шамраев А. В. Электронные деньги. Интернет-платежи. М., 2010.
3. Ревенков П. В. Финансовый мониторинг в условиях интернет-платежей. М., 2016.

#### English version

Security and protection of online payments: modern challenges and solutions

Salov Igor' Vladimirovich, senior lecturer, Ufa University of Science and Technology

Ermolaeva Arina Vital'evna, student, Ufa University of Science and Technology

This article provides a comprehensive analysis of the problem of electronic payment security in the context of rapid digitalization of the economy. The authors examine in detail modern threats, protection technologies, and the legal regulation of online payments. Special attention is paid to a comparative analysis of payment systems, methods of countering fraud, and the prospects for the development of security technologies in this field. Keywords: cybersecurity, e-commerce, payment systems, personal data protection, fraud monitoring, biometric authentication, blockchain technologies.

Безопасность интернет-платежей представляет собой комплексную задачу, требующую сочетания технологических, организационных и правовых мер. В ближайшей перспективе ожидается дальнейшее распространение бесконтактных биометрических платежных технологий, развитие децентрализованных финансовых систем, а также внедрение квантово-устойчивых алгоритмов шифрования. Комплексный подход, объединяющий инновационные технологические решения с повышением финансовой грамотности населения, является необходимым условием устойчивого развития цифровых платежных экосистем.