К. Н. Прокудова
Научный руководитель
И. Н. Новикова
Белорусский торгово-экономический
университет потребительской кооперации
г. Гомель, Республика Беларусь

КИБЕРБЕЗОПАСНОСТЬ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ РОЗНИЧНЫХ ПЛАТЕЖЕЙ РЕСПУБЛИКИ БЕЛАРУСЬ

Стремительный переход к безналичным расчетам, детально описанный в стратегических документах Национального банка, имеет не только очевидные преимущества в виде скорости и прозрачности, но и порождает новые системные риски. По мере того, как доля безналичных операций в Беларуси приближается к целевым показателям, киберпространство становится основным полем взаимодействий между потребителем, бизнесом и государством. Это взаимодействие неизбежно привлекает внимание злоумышленников.

Стимулирование государством безналичного денежного оборота требует дополнения с точки зрения обеспечения безопасности. Стимул пользоваться банковскими платежными картами и приложениями для потребителя очевидна – скорость платежей, кешбэк. При этом он сталкивается с новым видом транзакционных издержек – ментальными и финансовыми затратами на обеспечение собственной кибербезопасности. Если ранее главным страхом была кража кошелька, то теперь доминирует опасение потерять доступ к счету из-за фишинга или вируса. По данным Глобального альянса по борьбе с мошенничеством (GASA), в минувшем году из-за действий сетевых дельцов по всему миру было утрачено 1,026 трлн долл. США. И это то, что официально известно. Больше всего подобных криминальных схем фиксируется в Соединен-

ных Штатах. Согласно анализу GASA, около 60% пострадавших не сообщают о преступных действиях в правоохранительные органы, а 24% опрошенных не видят смысла это делать, поскольку привлечь аферистов к ответственности очень сложно. Таким образом, исследование GASA показало: 78% из 49,5 млн респондентов сталкивались хотя бы с одной попыткой сетевого обмана за последний год, а 59% – ежемесячно. По статистике, основными инструментами деятельности злоумышленников остаются телефонные звонки (61%) и СМС-сообщения (58%). GASA отмечает, что лишь 0,05% финансовых мошенников попадаются в правоохранительные сети [1].

Поэтому для государства мотивация к развитию систем кибербезопасности приобретает критический характер. Это обусловлено тем, что, во-первых, подрыв доверия к безналичным инструментам из-за волны мошенничеств способен обратить вспять многолетние усилия по цифровизации. Во-вторых, финансовые потери граждан от кибератак требуют либо прямых компенсаций, либо ведут к социальной напряженности. Как отметил председатель правления Национального банка Р. Головченко на расширенном заседании правления в январе 2026 г., «банковская система успешно справилась с задачами по обеспечению стабильности, однако новый вызов – киберустойчивость – требует консолидации усилий государства и частного сектора. Показатель достаточности капитала (19,3%) позволяет банкам инвестировать в передовые системы защиты, но человеческий фактор остается самым уязвимым звеном» [2].

Развитие систем дистанционного банковского обслуживания в Беларуси сопровождалось параллельной эволюцией методов мошенничества. В начале 2000-х основными угрозами были скимминг (устройства на банкоматах) и кража карт. С переходом к бесконтактным технологиям и интернет-эквайрингу акцент сместился в цифровую среду.

Ключевой перелом произошел в 2020–2022 гг., когда пандемия и локдауны вынудили даже консервативных пользователей освоить удаленные каналы оплаты. Именно в этот период резко выросло число случаев социальной инженерии звонков «от службы безопасности банка» или «от правоохранительных органов». Мошенники искусно использовали возросший поток онлайн-покупок и неопытность новых пользователей. Если в 2020 г. доля безналичных операций по картам впервые превысила 50%, то по данным Следственного комитета, количество киберпреступлений за этот же период выросло на 30%.

Следующий этап эволюции угроз связан с усложнением самой платежной инфраструктуры. Распространение QR-кодов, токенизации карт в смартфонах и появление сервиса «КРОК» открывают новые векторы атак: подмена QR-кодов, перехват SMS-подтверждений, фишинговые сайты, имитирующие страницы оплаты.

По состоянию на начало 2026 г., несмотря на эмиссию более 18 млн банковских платежных карт и наличие 180 тыс. POS-терминалов, уровень защищенности остается неравномерным. С одной стороны, Национальный банк инициировал ряд обязательных требований: переход на чип-технологии (EMV), обязательное информирование клиентов о подозрительных операциях. С другой стороны, сохраняется критическая уязвимость в виде низкого уровня цифровой грамотности. Основную тревогу вызывает сегмент интернет-эквайринга: объем онлайн-платежей за 2025 г. вырос на 27%, и значительная их часть проходит на маркетплейсах, где данные карт могут храниться у продавцов.

Запланированный на 2026 г. запуск сервиса «КРОК» преследует не только цель вовлечения малого бизнеса в безналичный оборот, но и задачу повышения безопасности микроплатежей. Традиционный эквайринг с использованием POS-терминалов требовал сертифицированного оборудования, что было дорого, но безопасно. «КРОК» с его упрощенным входом (распечатанный QR-код) создает новые риски подмены. Разработчики системы учли эти угрозы. Архитектура сервиса базируется на динамических QR-кодах, генерируемых для каждой транзакции (в приложении продавца), либо на статических кодах, но с обязательным подтверждением от покупателя суммы в приложении. Ключевое отличие от существующих решений – использование единого стандарта безопасности, исключающего возможность перехвата данных при переходе между банками. Внедрение сервиса «КРОК» должно сопровождаться массовой информационной кампанией, предупреждающей граждан о том, как отличить подлинный код от мошеннического.

Параллельно развивается проект цифрового рубля, в котором безопасность закладывается на архитектурном уровне. Технология смарт-контрактов позволяет не только отслеживать целевое расходование средств, но и ограничивать круг потенциальных получателей, что минимизирует риски хищения при госзакупках. Пилотный проект 2027 г. будет тщательно проверяться на проникновение.

Таким образом, достижение 70% доли безналичных расчетов к 2030 г. [3] невозможно без решения проблемы доверия. Позитивным фактором является высокая степень проникновения смартфонов и техническая возможность внедрения продвинутых методов биометрической аутентификации. Уже сегодня многие банки предлагают вход в приложения по отпечатку пальца или сканеру лица, что значительно усложняет жизнь мошенникам.

Сдерживающим фактором остается возрастная структура: население старше 60 лет (около 23%) наиболее уязвимо для социальной инженерии. Социологические опросы фиксируют, что именно пенсионеры чаще всего становятся жертвами телефонных мошенников. Требуется не просто установка терминалов, а регулярная разъяснительная работа, которую ведут банки и почтовые отделения. Проведенное исследование показывает, что рост числа киберпреступлений коррелирует с ростом доли безналичных расчетов. Для достижения безопасной цифровой среды необходимо, чтобы темпы внедрения средств защиты и роста цифровой грамотности опережали темпы роста доли безналичных операций. Целевой показатель в 70% безналичного оборота достижим, но только в том случае, если он будет обеспечен соответствующим уровнем киберустойчивости всей системы.

Список использованной литературы

1. **Пашков, И. М.** Пираты XXI века. В 2023 году интернет-мошенники похитили не менее одного процента мирового ВВП / И. М. Пашков. – URL: https://house.gov.by/special/ru/interview-ru/view/piraty-xxi-veka-v-2023-godu-internet-moshenniki-poxitili-ne-menee-odnogo-protsenta-mirovogo-vvp-11547/ (дата обращения: 12.03.2026).

2. **Головченко, Р.** В Беларуси растет уровень доверия к национальной валюте и банковской системе / Р. Головченко // Минск-новости. – 2026. – URL: https://minsknews.by (дата обращения: 25.02.2026).

3. **Концепция** развития платежного рынка Республики Беларусь до 2030 года // Национальный банк Респ. Беларусь. – URL: https://www.nbrb.by/payment/koncepcija-rasvitija-platioznogo-rinka_2023-2025.pdf (дата обращения: 25.02.2026).