Финансы: ПОЛЕ КИБЕРЗАЩИТЫ

Сегодня банковская сфера – одна из сильнейших в вопросах кибербезопасности. Здесь, например, требования, сформированные регулятором в 2023 году для аттестации центров кибербезопасности, были введены уже давно. Сейчас внедряются дополнительные системы – уже «на основании опыта сотрудников банков».

О траекториях, по которым сейчас движется кибербез в банковской сфере, рассказал первый заместитель председателя правления Нацбанка Александр ЕГОРОВ.

ПОРТРЕТ КИБЕРАТАК НА БАНКИ

По данным автоматизированной системы Нацбанка, за первые 10 месяцев 2025 года зафиксировано более 500 нарушений безопасности. Для сравнения: за весь 2024 год их было всего 170. Рост более чем трехкратный.

В Беларуси ситуация в области кибербезопасности финансового сектора коррелирует с общемировыми трендами. Лидирует сканирование портов – это разведка, поиск «брешей» в сетях банков. На втором месте – массовые DDoS-атаки, цель которых – парализовать работу онлайн-сервисов. Далее следуют целенаправленные попытки эксплуатации выявленных уязвимостей. Эксперты ожидают,

что с развитием инструментов на основе искусственного интеллекта объем и изощренность таких атак будут только нарастать.

В глобальной повестке для банков сегодня доминируют три ключевые угрозы.

Первая – массовые DDoS-атаки. Их проведение «подпитывается» наличием значительного числа устройств, которые не только не защищены даже простыми инструментами, но и не обновляются.

Вторая угроза связана с развитием Open Banking и рисками, которые эта технология несет. Так, когда доступ к финансовым операциям получают сторонние финтех-компании через открытые API, закономерно расширяется и поле для потенциальных уязвимостей.

> В 2025 году в топ-3 нарушений безопасности в белорусской банковской сфере входили сканирование портов, DDoS-атаки, попытки эксплуатации выявленных уязвимостей. Эксперты ожидают, что с развитием инструментов на основе искусственного интеллекта объем и изощренность таких атак будут только нарастать.

И наконец, третья проблема – целенаправленные атаки на подрядчиков банков. Если собственная защита финансовой организации выстроена надежно, злоумышленники ищут обходной путь через менее защищенных поставщиков программного обеспечения и услуг.

КИБЕРМОШЕННИЧЕСТВО

Банки также задействованы и в борьбе с кибермошенничеством, из-за которого финансовые потери граждан достигают колоссальных сумм. За 10 месяцев 2025 года, по информации Нацбанка, у жителей страны похитили порядка 47 миллионов рублей. Количество зафиксированных инцидентов превысило 16 тысяч. Банковские антифрод-системы, использующие в том числе искусственный интеллект, сумели предотвратить часть переводов мошенникам и сохранить владельцам около 4 миллионов рублей. «Эти цифры пока незначительны. Без активной бдительности самих клиентов и тотальной разъяснительной работы со стороны банков существенно увеличить долю спасенных средств крайне сложно», – отмечает Александр Егоров.

> За 10 месяцев 2025 года, по информации Нацбанка, у жителей страны похитили порядка 47 миллионов рублей. Количество зафиксированных инцидентов превысило 16 тысяч.

Анализ инцидентов позволяет выделить три наиболее распространенные схемы. На первом месте – инвестиционные ловушки: граждане переводят деньги, как правило, за рубеж на платформы-однодневки, после того как увидели таргетированную рекламу, обещающую сверхдоходы. На втором – многоступенчатые звонки от лжесотрудников правоохранительных органов с требованием срочно «задекларировать» средства. И на третьем – оплата товаров, после получения которой зачастую и товар, и продавец исчезают.

Мошенники не стоят на месте. Так, по словам представителя Нацбанка, сейчас отмечается рост использования технологии NFC для кражи данных с токенизированных инструментов (например, смартфонов с привязанными картами). Еще один тревожный тренд – активный вывод похищенных средств через криптобиржи, что значительно затрудняет отслеживание и возврат денег. Нацбанк совместно с коммерческими банками и криптоплощадками уже ведет работу по минимизации таких рисков.

2026: ТРИ КИТА ИБ

В новом году Национальный банк планирует ввести три новых ключевых стандарта, которые «должны сформировать единое поле информационной безопасности во всем банковском секторе».

Первый стандарт – это «Банковская деятельность. Обеспечение информационной безопасности. Общие требования». Этот документ станет базой. В нем будут определены обязательные для всех банков минимальные требования для обеспечения информационной безопасности. Речь идет о комплексных мерах: правовых, организационных и технических. Фактически стандарт установит минимальную планку защиты, ниже которой опускаться нельзя.

> В 2026 году Национальный банк планирует ввести три новых ключевых стандарта, которые «должны сформировать единое поле информационной безопасности во всем банковском секторе».

Второй документ – «Банковская деятельность. Обеспечение информационной безопасности. Условия для реализации требований». Если первый стандарт отвечает на вопрос «Что делать?», то второй детально прописывает, как это сделать. Его цель – исключить неоднозначное толкование правил и максимально конкретизировать механизмы реализации. Это позволит всем участникам рынка одинаково понимать и выполнять требования.

И третий стандарт – «Обеспечение информационной безопасности. Оценка уровня соответствия информационной безопасности требованиям». Это завершающий элемент системы. Стандарт оценки введет четкую методологию, как измерять уровень защищенности конкретного банка. «Это не просто проверка «по списку», а инструмент для определения реального, а не декларативного состояния ИБ. Он позволит и нам как регулятору, и самим банкам понимать, на каком уровне обеспечения защиты информации они находятся», – рассказал

первый заместитель председателя правления Нацбанка.

Сейчас в системе Нацбанка требования в области кибербезопасности фрагментарно прописаны в разных нормативных актах. Это не очень удобно в работе. Утверждение триады стандартов должно не только решить существующую проблему, но и усовершенствовать систему.

В планах Нацбанка на 2026 год – продолжать развивать механизм информационного взаимодействия с правоохранительными органами для оперативной блокировки мошеннических операций. Банки получат право приостанавливать на срок до двух рабочих дней денежные переводы, которые вызывают подозрения у банковских работников. Правоохранительные органы смогут блокировать расходные операции по счетам на срок до 10 суток. Эти меры призваны создать критически важный временной буфер для спасения средств граждан.

В 2026 году банки получат право приостанавливать на срок до двух рабочих дней денежные переводы, которые вызывают подозрения у банковских работников. Правоохранительные органы смогут блокировать расходные операции по счетам на срок до 10 суток.

Нацбанк создает несущий каркас для защиты всего банковского сектора. Безопасность перестает быть лишь ответом на угрозы. Отныне она становится неотъемлемым элементом архитектуры финансовых услуг. ВС

Анастасия МАНУИЛОВА