Лечить подорожником ИБ неэффективно

Анализ развития ИБ во втором полугодии 2025 года на фоне изменений бизнес-моделей хакерского сообщества говорит об усилении роли регулирования, модернизации инфраструктурных сервисов, а также о расширении сферы применения риск-менеджмента



Текст
ВАДИМ ФЕРЕНЕЦ,
ОБОЗРЕВАТЕЛЬ **«Б.О»**



Первое полугодие было насыщено появлением новых нормативных актов в области ИБ, напрямую касающихся финансовой сферы. «О внесении изменений в отдельные законодательные акты Российской Федерации в целях противодействия операциям по внесению наличных денежных средств на банковские счета с применением токенизированных (цифровых) платежных карт с использованием банкоматов или иных технических устройств без согласия лица, вносящего наличные денежные средства, или с согласия лица, полученного под влиянием обмана или при злоупотреблении доверием». Закон установил обязанность банков ограничивать внесение денег на счет через банкомат с помощью вновь токенизированной карты. А 1 апреля 2025 года был подписал Закон № 41-ФЗ о противодействии телефонному и кибермошенничеству.

Регулирование и наказание

Придало импульс развитию отечественных программных аппаратных комплексов (ПАК) подписание Закона № 58-ФЗ от 07.04.2025 «О внесении изменений в Федеральный закон "О безопасности критической информационной инфраструктуры"». Этот закон предписывает правительству и Банку России «жестко определить типовые объекты критической информационной инфраструктуры и установить не менее жесткие сроки перехода на отечественные решения». Все ждут новостей от регулятора к осени 2025 года.

Ближе к концу первого полугодия, 1 июня, хорошо знакомый 115-ФЗ обрел новую цель — противодействие экстремизму. В этот закон добавилось понятие «финансирование экстремистской деятельности» — предоставление или сбор средств либо оказание финансовых услуг, заведомо предназначенных для финансирования организации, подготовки и совершения хотя бы одного из преступлений экстремистской направленности. Лицам, включенным в перечень Росфинмониторинга, будут заморожены все денежные средства и иное имущество в банках и иных субъектах во исполнение закона. Разморозка предусмотрена только после исключения таких фигурантов из перечня.

Кроме того, был подписан Федеральный закон от 24.06.2025 № 176-ФЗ «О внесении изменений в статью 187 Уголовного кодекса». Теперь дропперов будут наказывать принудительными работами на срок до пяти лет со штрафом в размере от трехсот тысяч до одного миллиона рублей.

Принятые нормативные акты, а также те, которые вступили в силу в этом году, например заработавший с 5 февраля 2025 года «Реестр контролируемых лиц», а также внешне безобидные поправки в УК (ст. 272.1) и КоАП (ст. 13.11), вступившие в силу 30 мая 2025 года, — головная боль прежде всего самих банков. Но существуют и изменения инфраструктурного характера, которые затрагивают финансовую отрасль в целом.

На острие изменений

В ходе XIII Технологической конференции НСПК, прошедшей 23 июня 2025 года в Москве, **Игорь Голдовский,** главный архитектор и директор департамента инноваций НСПК, сообщил: «По заключению авторитетных экспертов в области платежных технологий (PCI SSC, EMVCo, GlobalPlatform) и криптографии (NIST), криптостойкости используемых сегодня алгоритмов (например, 3DES с тройным ключом в 168 бит или RSA с длиной модуля открытого ключа в 2048 бит) будет недостаточно для выполнения безопасных платежных операций уже в третьем десятилетии». Вычислительные возможности криминала растут, и для обеспечения безопасности финансовых операций требуется перейти на новые криптографические алгоритмы, имеющие криптостойкость не меньше 128 бит.

В требованиях Банка России, зафиксированных в его Положении № 821-П от 17.08.2023, в частности в п. 5.6, касающемся операторов значимых платежных систем, записано: «Операторы должны обеспечить использование СКЗИ, реализующих иностранные криптографические алгоритмы и криптографические алгоритмы РФ, имеющих подтверждение соответствия требованиям ФОИВ в области обеспечения безопасности, в иных технических средствах информационной инфраструктуры платежной системы, используемых при осуществлении переводов денежных средств, типы которых определяются Банком России по согласованию с ФОИВами». Срок исполнения — до 1 января 2031 года.

Игорь Голдовский дал следующую трактовку применительно к индустрии платежных карт: «К 1 января 2031 года необходимо, чтобы на нашем рынке появились терминалы и карты, работающие на базе в том числе и отечественной криптографии». Другими словами, перед банковским сообществом встает задача в оставшееся до нового десятилетия время приступить к миграции на российские и зарубежные криптографические алгоритмы с криптостойкостью не ниже 128 бит.

На словах все просто, но если принять во внимание масштаб задачи и число затронутых миграцией информационных систем, то станет понятно, что рынку, НСПК и банкам придется засучить рукава и приступить к решению задачи уже сейчас. При этом НСПК обязуется взять на себя значительный объем работ и сделать миграцию на новую криптографию максимально комфортной для банков.

По словам Игоря Голдовского, новые криптографические алгоритмы хорошо известны и уже используются при решении отдельных задач в НСПК.

Суть, как обычно, кроется в деталях, а именно в том, что новые криптографические алгоритмы обладают свойствами, требующими изменения протоколов, в которых эти алгоритмы будут использоваться. В этой связи EMVCo в конце 2022 года выпустила две спецификации, обеспечивающие совместимость с новой криптографией.

Первая спецификация, EMV4.4, определяет контактный интерфейс взаимодействия терминала и карты. В нем определены новая процедура офлайн-аутентификации карты Extended Data Authentication и процедура организации защищенного соединения между картой и терминалом Offline Data Encipherment.

Во второй спецификации на бесконтактное универсальное ядро EMV Contactless Kernel C-8 реализовано несколько интересных и оригинальных подходов, например, уменьшающих время диалога карты и терминала из-за отсутствия необходимости формирования подписи на стороне карты. Офлайн-аутентификация карты производится с помощью механизма слепого множителя, формируемого картой. Спецификация C-8 также обеспечивает запись и чтение специальных данных, которые могут использоваться, например, для оплаты проезда на транспортных маршрутах со сложной тарификацией проезда, а также поддерживает эффективный протокол для противодействия распространившимся в последнее время relay-атакам. Важная особенность C-8 заключается в том, что это ядро умеет работать с тремя разными криптографическими наборами. В частности, к этому ядру может быть подключена российская криптография.

НСПК разработала дорожную карту реализации этого масштабного проекта, первые спецификации должны появиться в 2025–2026 годах, они будут посвящены разработке платежного и мобильного приложений, а также процедуре сертификации и тестирования этих приложений. Участвует НСПК и в создании новых HSM-модулей, поддерживающих ГОСТ-криптографию.

Причины изменений

Все сказанное выше является ответом на изменение поведения киберпреступников, изменяющих традиционную модель разработки вредоносного программного обеспечения «собственными силами» на новую концепцию, известную как «malware-as-a-service». Сегодня организаторы преступных схем предоставляют начинающим злоумышленникам доступ к аутсорсинговым мощностям и инструментам для осуществления новых типов атак: автоматизированного сбора данных о жертвах, скрытой передачи информации через промежуточные узлы сети («edge») и целевых взломов.

Кроме того, ИИ привнес в киберсреду высочайшие скорости подготовки и проведения атак, а на пороге — выход в промышленную эксплуатацию квантовых компьютеров, способных серьезно изменить расстановку сил в криптографическом мире. Поэтому новую изощренную атаку на какой угодно банк и какую угодно финансовую сферу в целом ждать можно в любой момент. А защитить все, как известно, невозможно. Поэтому приходится выбирать для защиты главное на основе риск-менеджмента. Но и это уже, похоже, устаревает, поскольку, как утверждает новый ИБ-мем: «Лечить подорожником ИБ неэффективно».

Сергей Демидов, заместитель председателя правления по ИБ Московской биржи, отметил: «В традиционных попытках разделить риски по видам мы за деревьями не можем увидеть леса. А лес заключается в том, что в 2025 году, по нашему мнению, наступает некая критическая точка, после которой будет необходимо вообще переосмыслить роль риск-менеджмента в крайне динамичном мире. Поэтому придется вспомнить, с чего он начинался, и вернуться к истокам: “Учиться предвидеть события и их последствия”». Б.О