вождается этими документами. Сведения, содержащиеся в документе, могут не соответствовать действительности полностью или в какой-то части. Не соответствующими действительности документами также являются первичные учетные документы (бланки строгой отчетности), приобретенные в нарушение установленного законодательством порядка у лиц, не имеющих права их реализовывать, приобретенные одним лицом, но фактически использованные другим лицом (не являющимся стороной в сделке, при совершении которой использован этот первичный учетный документ). При этом документ, в котором зафиксирована фиктивная операция с товарно-материальными ценностями, называют бестоварным, а с денежными средствами – безденежным документом (например, товарный отчет).

Принимая во внимание ранее указанные положения, мы можем определить признаки бестоварности, а именно: отсутствие оформления расхода и поступления товарно-материальных ценностей у субъектов хозяйствования; отсутствие сопроводительных документов; неуказание в накладных необходимых реквизитов; отсутствие предусмотренных формой документа подписей; указание недостоверных данных и т. д.

В этой связи для установления наличия либо отсутствия данных признаков эксперту при проведении экономических экспертиз по бестоварным операциям необходимо: во-первых, выявить наличие либо отсутствие договорных отношений между заказчиком и поставщиком, указанными в товарно-транспортной накладной; во-вторых, провести документальную проверку первичных документов, отражающих отпуск, перемещение, оприходование, оплату и учет товарно-материальных ценностей; в-третьих, обратить внимание при проверке документов, отражающих факт совершения операции по существу и по форме, на наличие подчисток, помарок, неоговоренных исправлений, которые часто возникают вследствие изменения текста документа после того, как совершена операция, и указывают на завышение (занижение) количества товарно-материальных ценностей; в-четвертых, проверить арифметические расчеты (пересчет, таксировка) в документах; в-пятых, проверить данные складского учета, отражающие отпуск товарно-материальных ценностей у поставщика и оприходование их у заказчика.

Процесс исследования строится на ряде наиболее часто используемых методов:

метод документальной проверки, которая включает в себя такие способы проверки, как проверка документов и записей по форме, арифметическая (счетная) проверка документов, нормативная проверка документов;

метод сопоставления документов, одним из приемов которого может выступать встречная проверка.

Таким образом, в связи с тем, что основным способом совершения правонарушений в сфере торговли является бестоварная операция, для эффективного противодействия им необходимо обучать сотрудников правоохранительных органов ряду экономических дисциплин на углубленном уровне и отрабатывать полученные знания на практических занятиях до непосредственного контакта с узкопрофильной преступностью. Это позволит выйти на качественно новый уровень в предупреждении и пресечении преступных посягательств и принесет приемлемый результат в формировании благосостояния общества и государства.

УДК 004.056.5

С.Ю. Воробьёв, Г.В. Мишнев

ПРОТИВОДЕЙСТВИЕ МОШЕННИЧЕСКИМ ОПЕРАЦИЯМ В БАНКОВСКОЙ СФЕРЕ

Цифровизация всех отраслей человеческой деятельности в международной практике сопровождается увеличением числа противоправных действий, совершаемых в киберпространстве, в частности в отношении информационной инфраструктуры банков, основанной на использовании современных информационных систем и технологий предоставления цифровых финансовых услуг.

Необходимо отчетливо осознавать, что практически любая информационная система (ИС) уязвима. Нет систем, не подверженных риску взлома со стороны злоумышленников. «Хорошо» и «плохо» защищенные ИС отличаются только количеством ресурсов (материальных, интеллектуальных, волевых и пр.), которые необходимо потратить на взлом системы. При этом ИС, содержащие ценные сведения (финансовую, банковскую или коммерческую тайну, персональные данные и т. п.), постоянно подвергаются таргетированным атакам в киберпространстве.

В настоящее время перед банками наиболее остро стоит проблема обеспечения безопасности функционирования электронных платежей, совершаемых как юридическими, так и физическими лицами. В первую очередь проблема связана с ростом числа регистрируемых фактов хищения денежных средств со счетов клиентов, увеличением сумм хищений, а также появлением новых сложных схем мошенничества.

Чрезвычайно востребованным инструментом для выявления мошеннических операций в банковской деятельности является фрод-мониторинг.

В соответствии с Концепцией безопасного функционирования объектов банков, небанковских кредитно-финансовых организаций, открытого акционерного общества «Банк развития Республики Беларусь» система антифрода (фрод-мониторинга) – это система, предназначенная для оценки финансовых транзакций в глобальной компьютерной сети Интернет на предмет подозрительности с точки зрения мошенничества и предполагающая рекомендации по их дальнейшей обработке. Примером системы фрод-мониторинга является ограничение на сумму платежа.

Используемые белорусскими банками системы фрод-мониторинга разнообразны по функциональным возможностям, стоимости, интегрированности в процессинговую систему банка. Для целей фрод-мониторинга может использоваться и система расходных лимитов, и сложная дорогостоящая специализированная система.

Среди основных требований, предъявляемых к системе фрод-мониторинга, как правило, выделяют следующие: соответствие требованиям VISA и MasterCard; обеспечение уровня безопасности операций, соответствующего политике управления рисками банка; сохранение простоты и удобства процедуры выполнения операции по картам и терминалам банка; использование больших массивов данных об операциях для определения стандартного поведения точек приема и карт; создание разных профилей поведения для разных точек приема карт (объектов торговой сети), разных категорий карт; удобство управления правилами и параметрами фрод-мониторинга; поддержка расследования подозрительных операций; взаимодействие (возможность интеграции) с системой управления претензионной работы банка, системами процессинга, банковской учетной системой; наличие инструментов, обеспечивающих надежность и безопасность, сертификатов по международным стандартам безопасности (например, PA DSS) VISA и MasterCard.

Национальный банк Республики Беларусь уделяет серьезное внимание вопросам управления киберриском и обеспечения кибербезопасности банков. Нацбанк поддерживает и стимулирует обновление имеющихся и использование банками новых технических средств, систем и технологий работы с информацией с учетом всесторонней оценки рисков, присущих такой деятельности. В 2016 г. Нацбанком были разработаны и доведены до всех заинтересованных Рекомендации по безопасному использованию банковских платежных карточек – документ рекомендательного характера, выполнение требований которого позволит обеспечить максимальную сохранность денежных средств владельца карточки, а также снизить вероятные риски при совершении операций.

В настоящее время приоритетной задачей является создание нормативной правовой базы для применения систем фрод-мониторинга в банковском секторе государства. Требуют совершенствования правовые аспекты обмена информацией о лицах, вовлеченных в схемы хищений денежных средств в электронных платежных системах. Целесообразны разработка, внедрение и организация работы общереспубликанской системы, в которой будут осуществляться накопление и распространение информации о фактах несанкционированного перевода денежных средств.

Для успешного отражения банками кибератак и защиты информационных активов необходимо: обеспечение независимости подразделения информационной безопасности от профильного ИТ-подразделения; использование актуальных аппаратных, программных и программно-аппаратных комплексов средств защиты информации; применение DLP- и SIEM-систем; постоянное повышение квалификации работников, отвечающих за информационную безопасность; обучение работников банков основам информационной безопасности; поддержание здорового климата в коллективе; информирование клиентов банков о финансовой и цифровой грамотности и соответствующее обучение; разработка пакета нормативной документации, регламентирующей сферу информационной безопасности в банке; создание команды, занимающейся расследованием инцидентов, связанных с информационной безопасностью, из числа наиболее подготовленных сотрудников; тщательный подбор персонала для работы в банковских организациях с учетом профессиональных, нравственных и моральных качеств кандидатов; регламентация порядка управления проектами по разработке, приобретению, внедрению новых и (или) обновлению имеющихся объектов информационной инфраструктуры; создание дублирующих и резервных объектов информационной инфраструктуры; взаимодействие и обмен информацией о кибератаках между банками, правоохранительными органами и организациями, осуществляющими помощь в борьбе с угрозами в сфере цифрового пространства.

Создание современной и надежной системы информационной безопасности и соблюдение ее требований всеми участниками информационного обмена является залогом доверия не только к конкретной кредитно-финансовой организации, но и ко всей банковской системе государства.