Обзор международных и российских подходов к противодействию несанкционированным операциям в сфере розничных платежных услуг

2013

Оглавление

I. Введение

По мере развития применяемых в сфере розничных платежных услуг банковских технологий, в том числе, направленных на повышение уровня безопасного использования платежных карт и каналов связи, совершенствуются методы проведения несанкционированных операций третьими лицами (далее - мошенники), а также применяемое ими оборудование и программное обеспечение.

Следует отметить, что консолидация мошенников и создание ими транснациональных группировок ведет к росту общего числа несанкционированных операций и нанесенного ими ущерба.

Почти все страны осознают опасность сложившейся ситуации и принимают меры по противодействию ей. В большинстве стран противодействием совершению несанкционированных операций в сфере розничных платежных услуг занимаются правоохранительные органы или иные организации по борьбе с преступлениями, иногда в их структурах выделяются специализированные отделы или управления.

В многообразной деятельности, связанной с противодействием несанкционированным операциям, можно выделить основные направления, характерные для всех стран:

разработка соответствующих рекомендаций;

создание специализированных баз данных;

организация взаимодействия между заинтересованными участниками рынка розничных платежных услуг;

повышение финансовой и технической грамотности;

разработка стандартов безопасности и качества оказания розничных платежных услуг.

II. Международный подход к противодействию совершению несанкционированных операций

Общеевропейские подходы

К декабрю 2008 года на территории европейских стран в течение нескольких лет подряд наблюдался рост числа несанкционированных операций в сфере розничных платежных услуг. В этой связи Европейский платежный совет подготовил и опубликовал ряд рекомендаций по внедрению на территории Единого Европейского Платежного Пространства («Single Euro Payments Area», далее - SEPA) различных анти - скимминговых решений для банкоматов (далее - Рекомендации).

Рекомендации включают основные способы повышения уровня безопасности при использовании банкоматов, к которым относятся проведение независимого тестирования банкоматов, разработка и применение систем и процедур, направленных на идентификацию скимминга и иных типов несанкционированных действий, и пр.

Однако из-за быстрого развития программных и технологических решений как представления платежных услуг, так и совершения несанкционированных операций, на сегодняшний день отдельные положения Рекомендаций потеряли свою актуальность и не могут обеспечить безопасность на том же уровне, что и 5 лет назад.

К инфраструктурным решениям в сфере противодействия несанкционированным операциям с платежными картами можно отнести решение о создании Европейским Советом по Платежным Системам («European Payment council») на территории SEPA общеевропейской информационной базы данных по указанным операциям[1] (далее – База данных). Организации, деятельность которых связана с обслуживанием платежных карт, пополняют Базу данных информацией обо всех известных им случаях совершения несанкционированных операций с их использованием.

Целью функционирования Базы данных является повышение осведомленности участников рынка розничных платежных услуг о методах совершения несанкционированных операций с платежными картами, выработка совместного подхода к их предотвращению. На начало 2013 года было реализовано функционирование модуля, отвечающего за сбор

[1]Справочно: по материалам отчета «К созданию Единой Зоны Платежей в Евро. Цели и сроки (Четвертый отчет о проделанной работе)», 2006 год

информации.

Отдельного внимания заслуживает практический опыт ряда европейских стран по противодействию совершению несанкционированных операций в сфере розничных платежных услуг как на уровне заинтересованных участников рынка, так и на уровне центральных (национальных) банков.

Европейский Центральный Банк (далее - ЕЦБ) большое внимание уделяет вопросам повышения уровня безопасности в сфере розничных платежных услуг. В начале 2011 года ЕЦБ создал «Европейский форум по безопасности розничных платежей» («European Forum on the Security of Retail payments», далее - Форум), который 20 апреля 2012 года опубликовал рекомендации по безопасному совершению платежей в сети Интернет. Участниками Форума являются представители Европейской системы центральных банков, Европейской службы банковского надзора, Еврокомиссии и Интерпола и др. Также для обсуждения отдельных тем приглашаются представители рынка розничных платежных услуг и представители организаций, в чью компетенцию входят обсуждаемые вопросы.

На регулярной основе ЕЦБ публикует «Отчет о несанкционированных операциях с платежными картами» («Report on card fraud»), который содержит информацию о динамике несанкционированных операций с платежными картами. Данные отчета свидетельствуют, что объем несанкционированных операций, совершенных с использованием платежных карт в банкоматах, в 2010 году сократился по сравнению с 2007 годом. При этом за аналогичный период времени увеличение объема несанкционированных операций с использованием платежных карт в электронных терминалах, установленных на кассах предприятий торговли (услуг), было незначительно (1,9%). Данный факт ЕЦБ объясняет выдачей на территории SEPA банками - эмитентами своим клиентам платежных карт, соответствующих стандарту EMV, и использованием банками – эквайрерами технологии 3-D Secure[2]. Вместе с тем, следует отметить, что объем несанкционированных операций без физического использования платежных карт (CNP – card not present) за аналогичный период вырос с 554 до 644 миллионов евро (рост на 16%), что свидетельствует о смещении приоритетов мошенников на совершение несанкционированных операций в сети Интернет.

[2]Справочно: 3–D Secure - протокол, добавляющий к процессу финансовой авторизации проверку подлинности в режиме реального времени (on-line), основанной на принципе трех доменов (домен эквайрера, домен эмитента, домен совместимости)

Англия

В Англии к организациям, занимающимся противодействием совершению несанкционированных операций в сфере розничных платежных услуг, относятся:

«Карточная ассоциация Великобритании» («UK cards association limited»);

«Организация по финансовым мошенничествам в Англии» («Financial Fraud Action UK»);

«Координационная группа по контролю над мошенничеством» («Fraud Control Steering Group»);

«Подразделение по борьбе с преступлениями с чеками и картами» («Dedicated Cheque and Plastic Crime Unit»);

«Национальная информационно-аналитическая служба по мошенничеству» («National Fraud Intelligence Bureau»).

Большая часть из перечисленных организаций работает в тесном сотрудничестве как между собой, так и с соответствующими органами государственной власти, что повышает эффективность их деятельности.

«Карточная ассоциация Великобритании» - организация, проводящая широкий спектр мероприятий, целью которых является предотвращение совершения несанкционированных операций с использованием платежных карт. Сотрудничает с государственными структурами (например, с Министерством внутренних дел), предприятиями торговли (услуг) и прочими организациями (например, «CrimeStoppers»[3]), участником может стать любая организация, эмитирующая платежные карты: «American Express Company», «MasterCard Worldwide», «Visa Inc.». При этом организация, эмитировавшая более миллиона платежных карт и/или осуществляющая эквайринг более 2,5% всех операций с ними на территории Англии, получает место в правлении «Карточной ассоциации Великобритании». По данным на январь 2012 года ее участниками являлось более 20 организаций из них в правление входило 16 организаций.

«Организация по финансовым мошенничествам в Англии» - организация, оказывающая помощь «Карточной ассоциации Великобритании» в информировании банковского сообщества о различных способах предотвращения совершения несанкционированных операций с использованием платежных карт, чеков и координации действий по

[3]Справочно: независимая добровольческая организация, которая помогает расследовать преступления, адрес в сети Интернет: www.crimestoppers-uk.org/

повышению безопасного уровня использования платежных карт и чеков.

«Координационная группа по контролю над мошенничеством» - ассоциация банков Англии, формулирующая и обеспечивающая реализацию политики, направленной на противодействие совершению несанкционированных операций с использованием платежных карт и чеков на территории Англии.

«Подразделение по борьбе с преступлениями с чеками и картами» (далее - Подразделение) - специализированное полицейское подразделение, основанное в 2002 году, и состоящее из офицеров Лондонской полиции. Спонсорами Подразделения выступают банки. Кроме того, Подразделение получает информационную поддержку от банков, занимающихся противодействием совершению несанкционированных операций в сфере розничных платежных услуг. Подразделение работает на национальном уровне, в сферу его деятельности входит противодействие (предупреждение) противозаконным действиям, связанным с:

совершением несанкционированных операций в банкоматах;

консолидацией мошенников в группировки;

совершением несанкционированных операций без физического использования платежных карт (CNP).

Результатом деятельности Подразделения в 2010 году стало предотвращение потерь на сумму более 28,1 миллионов фунтов стерлингов[4], арест 53 подозреваемых, пресечение деятельности 22 группировок.

«Национальная информационно-аналитическая служба по мошенничеству» (далее - Служба) - создана правительством в 2006 году. Служба ведет централизованную базу данных, в которой собирается информация по всем подтвержденным случаям несанкционированных операций, попыткам или подозрениям на их совершение в сфере розничных платежных услуг на территории Англии. Информация в Службу поступает от всех заинтересованных организаций государственного и частного сектора. Доступ к данной базе имеют организации, занимающиеся противодействием несанкционированным операциям в сфере розничных платежных услуг на территории Англии.

В Англии в рамках государственной программы по повышению финансовой грамотности населения по вопросам безопасного использования

[4]Справочно: с начала своей деятельности Подразделение предотвратило потери на сумму более 368 миллионов фунтов стерлингов

информационных технологий (в том числе, осуществления операций без физического использования платежных карт (CNP)) был запущен проект «Остановись. Подумай. Подключись» («Stop. Think. Connect», далее - Проект). Проект находится под управлением Национального альянса по информационной безопасности («National CyberSecurity Alliance»). В рамках реализации Проекта проводятся различные мероприятия, в частности:

в организациях, в том числе учебных, на постоянной основе распространяются тематические брошюры, содержащие рекомендации по повышению финансовой грамотности для каждой социальной и возрастной группы населения;

ежегодно проводится Месяц повышения финансовой грамотности населения относительно безопасного использования продуктов информационных технологий, в ходе которого по радио и телевидению транслируются тематические передачи, распространяются соответствующие материалы, в том числе, размещаемые в сети Интернет;

осуществляется сотрудничество с зарубежными партнерами (например, «VISA Inc.», «Facebook»[5] и др.).

Соединенные Штаты Америки

В США вопросы безопасного дистанционного банковского обслуживания (далее – ДБО) клиентов находятся в сфере деятельности коммерческих организаций.

В частности, компания «Cyber Source»[6] (далее – Компания) осуществляет мониторинг тенденций в сфере несанкционированных операций с использованием систем ДБО, подготовку соответствующих отчетов, аналитических материалов и публикаций.

Помимо выпуска различных отчетов о состоянии рынка услуг ДБО, Компания организует и проводит встречи с представителями предприятий торговли (услуг) по вопросам предотвращения совершения несанкционированных операций в сфере розничных платежных услуг. Компания анализирует мнения участников рынка, полученные в ходе встреч, и готовит на основе указанного анализа соответствующие отчеты. По данным отчета Компании, выпущенного в 2011 году, потери от несанкционированных операций с использованием систем ДБО выросли с 2,7 миллиардов долларов

[5]Справочно: «Facebook» - крупнейшая всемирная социальная сеть, на конец октября 2012 года число пользователей превышало 1 миллиард человек, адрес в сети Интернет: www.facebook.com
[6]Справочно: адрес в сети Интернет: www.cybersource.com

США в 2010 году до 3,4 миллиардов долларов США в 2011 году.

В 2011 году Компанией были рассмотрены современные методы борьбы с несанкционированными операциями и проведен анализ их эффективности. По данным Компании, на 2011 год самыми широко распространенными методами предотвращения совершения несанкционированных операций при оплате товаров (работ, услуг) в сети Интернет без физического использования платежных карт (CNP) являлись:

проверка контрольного кода карты (например, код CVC2/CVV2[7]);

подтверждение личности физического лица, осуществляющего платеж, посредством проверки его домашнего адреса[8].

В США функционируют различные Интернет сайты, которые позволяют физическим лицам подавать заявления о выявленных фактах и/или подозрениях, связанных с совершением несанкционированных операций. Некоторые из провайдеров указанных Интернет сайтов ведут свою деятельность в сотрудничестве с государственными органами, в том числе, осуществляющими следственную деятельность[9].

Канада

Одним из направлений деятельности полиции Канады[10] является проведение мероприятий, направленных на уменьшение числа несанкционированных операций с использование платежных карт, в рамках чего готовятся и публикуются соответствующие материалы. В частности, полицией Канады была разработана подробная инструкция[11], касающаяся порядка действий держателя платежной карты в случае совершения несанкционированных операций как в отношении самого держателя, так и в отношении платежной карты.

Кроме того, на территории Канады функционирует «Канадский центр по противодействию мошенничеству» («Canadian Anti-Fraud Centre»), осуществляющий сбор информации о случаях совершения несанкционированных операций с использованием платежных карт. Центр был создан в январе 1993 года Барри Эллиотом, сотрудником подразделения по

[7]Справочно: код проверки подлинности платежной карты, получаемый с помощью специального алгоритма и используемый для противодействия подделке платежных карт и/или несанкционированным операциям в сети Интернет

[8] Справочно: специальная система проверки клиентских адресов AVS (Address Verification System)

[9]Справочно: например, «United States Computer Emergence Readiness Team», адрес в сети Интернет: http://www.us-cert.gov/nav/report_phishing.html

[10]Справочно: полное название – «Королевская канадская конная полиция» («Royal Canadian Mounted Police»)

[11]Справочно: адрес в сети Интернет: www.rcmp-grc.gc.ca/scams-fraudes/index-eng.htm

противодействию мошенничеству местной полиции Онтарио (Ontario Provincial Police).

Важным направлением деятельности Канадского центра по противодействию мошенничеству является проведение мероприятий, связанных с повышением финансовой грамотности населения и предупреждением его о наиболее распространенных способах совершения несанкционированных операций с использованием платежных карт.

Итогом реализации на территории Канады подобных инициатив всех заинтересованных участников рынка розничных платежных услуг стало снижение объема несанкционированных операций с использованием платежных карт в 2010 году по сравнению с 2009 годом на 23,3 миллиона канадских долларов[12].

Австралия

Основанная Координационным Комитетом Реформы Клиринговой Системы в 1992 году саморегулирующаяся «Австралийская Ассоциация Платежного Клиринга» («Australian Payments Clearing Association», далее - ААПК) совместно с участниками рынка розничных платежных услуг вырабатывает единые стандарты осуществления расчетов, в том числе стандарты безопасности в сфере розничных платежных услуг. При этом ААПК на постоянной основе осуществляет мониторинг информации о несанкционированных операциях с использованием платежных карт, а также проводит мероприятия, направленные на снижение числа несанкционированных операций с использованием платежных карт. В результате указанной деятельности, по данным ААПК, доля несанкционированных операций с использованием платежных карт в период с июня 2010 года по июнь 2011 года сократилась с 0,0107% до 0,0041% в общем объеме операций с использованием платежных карт.

В рамках государственной программы повышения финансовой грамотности населения в сфере использования инновационных технологий реализуются мероприятия, в том числе направленные на подготовку материалов по повышению уровня безопасности при использовании сети Интернет и ДБО[13].

Подходы операторов международных карточных систем

[12]Справочно: адрес в сети Интернет: www.rcmp-grc.gc.ca/scams-fraudes/index-eng.htm
[13]Справочно: например, проект «Stay Smart Online»

«Совет по стандартам безопасности индустрии платежных карт»[14] («Payment Card Industry Security Standards Council») разработал стандарт безопасности данных, используемых в индустрии платежных карт – «Payment Card Industry Security Standard»[15] (далее - PCI DSS). С 2006 года данный стандарт введен на территории региона CEMEA (Центральная и Восточная Европа, Ближний Восток и Африка) как обязательный. Соответственно, его действие распространяется и на Российскую Федерацию. Стандарт PCI DSS представляет собой совокупность требований по безопасному хранению, обработке и передаче как реквизитов платежных карт, так и данных об их держателях. Основными являются 12 направлений указанных требований:

установка и обеспечение функционирования межсетевых экранов для защиты данных держателей карт;

неиспользование выставленных по умолчанию производителями системных паролей и других параметров безопасности;

обеспечение защиты данных держателей карт в ходе их хранения;

обеспечение шифрования данных держателей карт при их передаче через общедоступные сети;

использование и регулярное обновление антивирусного программного обеспечения;

разработка и поддержка безопасных систем и приложений;

разграничение доступа к данным держателей карт ответственных сотрудников организации в соответствии со служебной необходимостью;

присвоение уникального идентификатора каждому лицу, имеющему доступ к информационной инфраструктуре;

ограничение физического доступа посторонних лиц к базам данных держателей карт;

контроль и отслеживание всех сеансов доступа к сетевым ресурсам и данным держателей карт;

регулярное тестирование систем и процессов обеспечения безопасности;

разработка, поддержка и исполнение политики безопасности.

Согласно отчету компании «Trustwave»[16] в 2011 году среди предприятий торговли (услуг), ранее прошедших процедуру сертификации на соответствие стандартам PCI DSS, в которых за указанный год совершались

[14]Справочно: был учрежден в 2006 году системами «VISA Inc.», «MasterCard Worldwide», «American Express Company»
[15]Справочно: адрес в сети Интернет: www.pcisecuritystandards.org
[16]Справочно: адрес в сети Интернет: www.trustwave.com

несанкционированные операции с использованием платежных карт, более чем 93% не соблюдали, как минимум, одно из вышеперечисленных требований.

III. Российский подход к противодействию совершению несанкционированных операций

В Российской Федерации существуют различные инициативы по противодействию совершению несанкционированных операций с использованием платежных карт, успешно реализуемые как банковским сообществом, так и частными компаниями.

1. По инициативе Банка России была начата деятельность по разработке национального стандарта финансовых операций на основе стандарта ISO 20022, который является принятой в международной практике методологией описания процедур осуществления финансовых операций и форматов финансовых сообщений. В декабре 2010 года в соответствии с приказом Федерального агентства по техническому регулированию и метрологии на добровольной основе создан заинтересованными организациями Технический комитет по стандартизации № 122 «Стандарты финансовых операций» (далее – ТК № 122)[17] в целях организации и проведения работ по национальной, межгосударственной и международной стандартизации финансовых операций. В 2011 году была утверждена организационная структура и основные направления его деятельности. В настоящее время ТК № 122 состоит из пяти подкомитетов: ПК № 1 «Безопасность финансовых (банковских) операций», ПК № 2 «Технологии операций на финансовых рынках», ПК № 3 «Технологии основных финансовых (банковских) операций», ПК № 4 «Процедуры и технологии расчетов с использованием банковских карт и иных инструментов розничных платежей» (далее – ПК № 4) и ПК № 5 «Мобильные платежи» (далее – ПК № 5). Помимо Банка России, в ТК № 122 участвуют более 50 организаций, представляющих органы государственной власти, кредитные организации и их ассоциации, инфраструктурные организации финансовых рынков и иные заинтересованные стороны, в том числе представители рынка розничных платежных услуг.

К приоритетному направлению деятельности ПК № 4 и ПК № 5 можно отнести выработку национального стандарта по предотвращению совершения несанкционированных операций с использованием электронных средств платежа (далее – ЭСП), включая разработку подходов к организации единой

[17]Справочно: адрес в сети Интернет: www.tk122.ru

базы данных по несанкционированным операциям, а также соответствующих общероссийских стандартов сбора, обработки, хранения и обмена информацией о совершенных несанкционированных операциях. Кроме того, целью деятельности ПК № 4 и ПК № 5 является повышение уровня раскрываемости случаев несанкционированных операций в сфере розничных услуг и разработка соответствующих рекомендаций кредитным организациям и пр.

2. В рамках «Ассоциации Российских членов Европей» (АРЧЕ), «Ассоциации российских банков» (АРБ) и «Сообщества ABISS» в 2009 году реализован проект по созданию межбанковского информационного ресурса, обеспечивающего закрытый канал обмена данными по инцидентам с платежными картами и информационной безопасностью (условное название «горячая линия») и позволяющего банкам:

быстро и с большой точностью выявлять места компрометации карт;

своевременно блокировать карты, подвергшиеся компрометации;

получать дополнительную, достоверную информацию при рассмотрении заявлений клиентов;

выявлять новые схемы совершения несанкционированных операций и вырабатывать меры противодействия;

обмениваться практическим опытом в области противодействия мошенникам и статистической информацией;

вести профессиональный диалог с правоохранительными органами и информировать банковское сообщество о соответствующих судебных решениях и пр.

В настоящее время сертифицированными пользователями «горячей линии» являются около 450 представителей более 150 крупнейших банков России, Украины, Белоруссии и Казахстана.

IV. Выводы

Международная и российская практика организации и проведения мероприятий, направленных на предотвращение несанкционированных операций в сфере розничных платежных услуг в различных ее сегментах, свидетельствует о необходимости:

создания информационной системы сбора и предоставления участниками национальной платежной системы сведений о фактах хищения денежных средств;

создания механизма мониторинга и обмена информацией между

заинтересованными участниками рынка розничных платежных услуг о случаях совершения несанкционированных операций с использованием платежных карт;

предоставления всеми участниками рынка розничных платежных услуг информации о несанкционированных операциях с платежными картами;

разработки требований к обеспечению безопасного предоставления кредитными организациями ДБО, в том числе с использованием инновационных технологий, в сфере розничных платежных услуг;

разработки рекомендаций по взаимодействию операторов по переводу денежных средств с целью блокировки операций в случае выявления фактов хищения при переводах денежных средств с использованием ЭСП;

комплексного анализа и подготовки экспертных оценок эффективности механизмов противодействия совершению несанкционированных операций;

разработки проектов и учебных программ по повышению финансовой грамотности населения по вопросам безопасности использования ЭСП, а также проведения работы по разъяснению позиции Банка России по указанным вопросам и доведения до участников рынка розничных платежных услуг и широкой общественности соответствующей информации.