

МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное казенное образовательное учреждение
высшего образования «Казанский юридический институт
Министерства внутренних дел Российской Федерации»

Кафедра экономики, финансового права и информационных технологий
в деятельности ОВД

Научно-практическое пособие

О.Г.Шмелева, Г.Н.Хадиуллина

МОШЕННИЧЕСТВО В БАНКОВСКОЙ СФЕРЕ С ИСПОЛЬЗОВАНИЕМ
ЭЛЕКТРОННЫХ ПЛАТЕЖНЫХ ПЛАСТИКОВЫХ КАРТ

Казань 2016

Мошенничество в банковской сфере с использованием электронных платежных пластиковых карт: Научно-практическое пособие / О.Г.Шмелева, Г.Н. Хадиуллина. – Казань: КЮИ МВД России, 2016. – 51 стр.

Научно-практическое пособие подготовлено начальником кафедры экономики, финансового права и информационных технологий в деятельности ОВД, кандидатом экономических наук, подполковником полиции Шевко Н.Р., профессором кафедры экономики, финансового права и информационных технологий в деятельности ОВД, доктором экономических наук, майором полиции Шмелевой О.Г., профессором кафедры экономики, финансового права и информационных технологий в деятельности ОВД, доктором экономических наук, полковником полиции Хадиуллиной Г.Н.

Рецензенты:

1. Хисматуллин О.Ю., начальник кафедры гражданско-правовых дисциплин Уфимского юридического института МВД России, кандидат юридических наук, полковник полиции;

2. Нугуманова Л.Ф., профессор кафедры экономического права ФГБОУ ВПО «Казанский национальный исследовательский технический университет им. А.Н.Туполева- КАИ», доктор экономических наук, доцент.

Настоящее научно-практическое пособие обсуждено и одобрено:

- на заседании кафедры экономики, финансового права и информационных технологий в деятельности ОВД КЮИ МВД России 23 июня 2015 г., протокол № 25;

- на заседании методического совета КЮИ МВД России 21 июля 2015 г., протокол №11;

- на заседании Ученого совета КЮИ МВД России 17 августа 2015 г., протокол № 8.

Научно-практическое пособие предназначено для банковских работников, работников подразделений УЭБ и ПК МВД по Республике Татарстан, а также для использования в образовательном процессе КЮИ МВД России в ходе обучения курсантов и слушателей Казанского юридического института МВД России по направлениям подготовки (специальностям) 40.05.01 – Правовое обеспечение национальной безопасности, 40.05.02 – Правоохранительная деятельность.

© Казанский юридический институт МВД РФ, 2016

Содержание

		Стр.
	Введение	4
Глава 1	Обеспечение экономической безопасности банковской системы России в современных условиях	7
1.1.	Понятие экономической безопасности в банковской сфере	7
1.2.	Виды преступлений в банковской сфере	10
1.3.	Современное состояние в сфере обращения банковских платежных пластиковых карт в России	13
Глава 2	Методы предотвращения мошенничества, связанного с использованием электронных платежных пластиковых карт	20
2.1.	Уголовно-правовая характеристика и проблемы квалификации мошенничества, совершаемого в банковской сфере с использованием электронных платежных пластиковых карт	20
2.2.	Криминалистическая характеристика мошенничества с использованием платежных карт	28
2.3.	Характеристика личности преступника, совершившего общественно опасные деяния в сфере проведения безналичных расчетов, производимых с использованием банковских карт	33
2.4	Способы противодействия мошенничеству, связанному с использованием электронных платежных пластиковых карт	36
	Заключение	43
	Список использованных источников и литературы	48

ВВЕДЕНИЕ

Поступательное развитие рыночной экономики, активизация процессов глобализации и внедрение в повседневную жизнь информационных технологий привели к широкому распространению в Российской Федерации и в мировом сообществе безналичных денежных расчетов, одним из элементов которых выступают расчеты, осуществляемые с использованием электронных платежных банковских карт. Так, по данным Национального агентства финансовых исследований, в 2015 г. в среднем у каждого пользователя банковской карты имеется 2,3 карты, при этом 85% держателей карт имеют зарплатную карту, 71% - дебетовую карту, 65% - кредитную карту¹. Согласно данным правоохранительных органов РФ, среди преступлений с использованием высоких технологий наибольшие темпы роста имеют показатели количества противоправных деяний с использованием платежных карт².

Неизбежным следствием расширения сферы применения банковских карт выступают новые виды преступных посягательств на собственность, что предполагает необходимость изменения уголовного законодательства. Федеральным законом от 29 ноября 2012 г. N 207-ФЗ в УК РФ введена ст. 159.3, предусматривающая ответственность за мошенничество с использованием платежных карт, что обусловлено стремлением законодателя решить проблему квалификации хищения с использованием карт. Однако введение подобной нормы в уголовное законодательство не привело к однозначному решению проблемы, поскольку из ее формальной интерпретации следует вывод о том, что хищение с использованием банковских карт может совершаться только в форме мошенничества. В действительности существуют и иные формы, а именно: факт использования банковских карт может рассматриваться как иное преступление против собственности, в частности кража. Таким образом, несовершенство российского законодательства вызывало сложности в квалификации выявленных преступлений по УК РФ. В то же время с 29.09.2011 г. вступили в силу нормы Федерального закона РФ от 27.06.2011 N 161-ФЗ «О национальной платежной системе», которые предусматривают постепенный переход всех агентов экономических отношений в электронные системы платежей, что с неизбежностью приведет к росту числа преступлений в указанной сфере.

Латентный характер преступлений подобного рода, необходимость реализации эффективных мер, направленных на противодействия мошенничеству, связанному с использованием электронных платежных пластиковых карт определили необходимость проведения исследования способов подобного мошенничества, а также обоснования методики

¹ Безопасность банковских карт: взгляд потребителя и активность игроков рынка. Отчет по результатам исследования. М.: Национального агентства финансовых исследований, 2016. [Электронный ресурс] URL: http://nacfin.ru/wp-content/uploads/2015/01/moshennichestvo_bankovskie_karty.pdf. Проверено на 30.10.2016.

² Козловский В. Масштабы кибермошенничества растут // Российская газета. 2012. 29 ноября. URL: <http://www.rg.ru/2012/11/29/karti-site.html>, свободный.

расследования преступлений, связанных с незаконным использованием пластиковых банковских карт.

Данной проблеме посвящено значительное число работ, среди которых труды ученых-специалистов в области уголовного права, криминологии, гражданского и банковского права - Антонова И.О., Астапкиной С.М., Борзенкова Г.Н., Васюкова С.В., Вехова В.Б., Викулина А.Ю., Волженкина Б.В., Гаухмана Л.Д., Ефимовой Л.Г., Жалинского А.Э., Жукова Е.Ф., Ивасенко А.Г., Ларичева В.Д., Ляпунова Ю.И., Макаровой Г.Л., Максимова С.В., Новоселовой Л.А., Олейник О.М., Суханова Е.А., Тосуняна Г.А., Усоскина В.М., Шалимова А.Н., Южина А.А., Яни П.С., Яценко Б.В. и других. Данная проблема стала предметом исследования зарубежных авторов, среди которых Л.Джеймс, Дж. Т.Уэллс и др. Определенный вклад в решение проблемы противодействия этому виду преступлений внесли авторы инструктивных и аналитических материалов, размещенных на официальных сайтах кредитных организаций, которые направлены на формирование у держателей пластиковых карт соответствующих навыков пользования ими. В ходе исследования использованы нормы действующего уголовного законодательства РФ; постановления Пленума Верховного Суда РФ; статистические и аналитические данные, материалы судебно-следственной практики по делам о мошенничестве; результаты социологических исследований; научные публикации по теме исследования.

При написании параграфа 2.1 «Уголовно-правовая характеристика и проблемы квалификации мошенничества, совершаемого в банковской сфере с использованием электронных платежных пластиковых карт» использованы материалы диссертации Южина А.А. на тему: Мошенничество и его виды в российском уголовном праве. Диссертация на соискание ученой степени кандидата юридических наук. Специальность: 12.00.08 – уголовное право и криминология; уголовно-исполнительное право. Москва, Московский государственный юридический университет имени О.Е. Кутафина (МГЮА), 2016 г. При написании параграфа 2.3. «Криминалистическая характеристика мошенничества с использованием платежных карт» использованы материалы статьи: Антонов И.О., Шалимов А.Н. Способы мошенничества с использованием платежных карт как элемент криминалистической характеристики данного вида преступлений // Ученые записки Казанского университета. Гуманитарные науки. 2013. Том 155. Книга 4. С. 196-203. При написании параграфа 2.3 «Характеристика личности преступника, совершившего общественно опасные деяния в сфере проведения безналичных расчетов, производимых с использованием банковских карт» использованы материалы статьи: Васюков С.В. Криминологическая характеристика личности преступника, совершающего общественно опасные деяния в сфере проведения безналичных расчетов с использованием банковских карт // Ученые записки Орловского государственного университета. Серия гуманитарные и социальные науки. 2012. № 5 (49). С. 439-445.

Объектом данного исследования являются общественные отношения, возникающие в процессе предупреждения преступлений с использованием

банковских карт. Предмет исследования - криминологическая и уголовно - правовая характеристика преступлений, совершаемых с использованием банковских карт.

Целью написания данного научно-практического пособия выступает обоснование криминалистически значимых классификаций способов данного вида мошенничества, определение состава современных технологий, которые используют мошенники для получения конфиденциальной информации о реквизитах подлинных карт и их держателях. Наличие подобных исследований позволит сформулировать эффективный уголовно-правовой инструмент, ориентированный на конкретную разновидность мошенничества, который обеспечивает приемлемое качество процедуры ее выявления, расследования, привлечения к уголовной ответственности виновных лиц в подобного рода преступлениях. Цель исследования определила его задачи, включающие: определение факторов риска для системы экономической безопасности российской банковской системы, характеристику видов преступлений в банковской сфере и современного состояния в сфере обращения банковских платежных пластиковых карт в Российской Федерации, уголовно-правовую характеристику и обоснование проблем квалификации мошенничества, совершаемого в банковской сфере с использованием электронных платежных пластиковых карт, раскрытие способов мошенничества с использованием платежных карт как элемента криминалистической характеристики данного вида преступлений, разработку способов противодействия мошенничеству, связанному с использованием электронных платежных пластиковых карт.

Пособие рассчитано на банковских работников, работников подразделений УЭБ и ПК МВД по Республике Татарстан, а также может быть использовано в учебном процессе КЮИ МВД России.

ГЛАВА 1. ОБЕСПЕЧЕНИЕ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ БАНКОВСКОЙ СИСТЕМЫ РОССИИ В СОВРЕМЕННЫХ УСЛОВИЯХ

§1. Понятие экономической безопасности в банковской сфере

Одним из важнейших компонентов экономической безопасности страны является безопасность финансовой системы³. Без устойчивого функционирования финансовой системы и финансового рынка страны невозможно наращивание экономического и научно-технического потенциала России, который призван обеспечить достойное место страны в мире.

В начале 90-х гг. XX в. с началом экономических преобразований, в стране, на фоне практически отсутствующего законодательства, создалось большое количество коммерческих банков, которые по характеру своей деятельности зачастую были или фиктивными, или неконкурентоспособными. Это не способствовало формированию в России единой устойчивой национальной системы финансового рынка. В результате, большинство современных российских коммерческих банков не располагают достаточными собственными финансовыми средствами и надежным объемом сбережений и вкладов клиентов, достаточно слабы и не обладают нужным уровнем устойчивости, надежности и безопасности⁴.

Российская банковская система характеризуется рядом негативных факторов, к ключевым из которых относятся:

- неэффективная структура банковской системы;
- неопределенная и непредсказуемая правовая база;
- недостаточный уровень капитализации банков;
- высокая степень концентрации кредитных рисков и привлеченных средств;
- непрозрачность структуры собственности;
- высокая концентрация в категории наиболее крупных банков и значительная фрагментация в категории средних и мелких банков.

Агентство Standard&Poore при анализе российской банковской системы отметило следующие обстоятельства:

- ЦБ РФ очень быстро провел внедрение системы страхования вкладов, приняв в систему 835 банков (около 75% всех заявок), в результате он потерял возможность кардинально реструктурировать банковский сектор;
- соблюдение экономических нормативов ЦБ РФ носит посредственный характер: соблюдается буква, а не дух закона. Как следствие, ожидаемое ужесточение этих нормативов может и не дать желаемого результата;
- образование кредитных бюро призвано упростить рассмотрение кредитных заявок и снизить кредитные риски, но позитивный эффект от них пока

³ Архипов А., Городецкий А., Михайлов Б. Экономическая безопасность: оценки проблемы, способы обеспечения// Вопросы экономики. 2014. № 12. С.47.

⁴ Россия в глобализирующемся мире: Стратегия конкурентоспособности / Российская академия наук, отделение общественных наук, секция экономики; акад. Д.С. Львов [и др.]. М.: Наука, 2014. С.89.

не очевиден;

- создано хорошее законодательное обеспечение ипотечного кредитования. Но из-за высокой ставки рефинансирования, стоимость ипотечного кредита слишком высока для населения;

- доходность российских банков постепенно снижается.

Причинами этого являются:

- а) рост операционных затрат, которые опережают рост возобновленных доходов;

- б) усиление конкуренции, что снижает маржу;

- в) значительная зависимость банков от торгового дохода.

В конце XX-начале XXI века все более сильное влияние на устойчивость функционирования национальных финансовых систем и финансовых рынков многих стран, в том числе и России, оказывает процесс глобализации. Он принес с собой в экономику ряд новых аспектов:

- существенно возрастает международная мобильность факторов производства. В результате, финансовая сфера приобретает более значимую, чем ранее, роль в экономическом развитии, что представляет собой потенциальную угрозу для стабильности и устойчивости национальных финансовых систем;

- растущая взаимосвязь и взаимозависимость национальных финансовых рынков за счет упрощения условий мобильности капитала, появление новых финансовых инструментов увеличивают скорость движения финансовых потоков между странами;

- значительно возрастают объемы перемещаемых финансовых ресурсов в результате деятельности транснациональных корпораций и банков, крупных инвестиционных фондов, чьи действия зачастую не подконтрольны национальным правительствам или находятся в юрисдикции «оффшорных» зон;

- происходит отрыв финансовой сферы от реального сектора за счет усложнения ее инструментов и механизмов;

- увеличиваются возможности для проведения спекулятивных операций, не связанных с реальным производством. Хозяйственные операции приобретают все более глобальный характер, что расширяет возможности уклонения от уплаты налогов и легализации доходов, полученных преступным путем;

- развитие информационных и телекоммуникационных технологий приводит к росту объема и разнообразия финансовой информации и усугубляет характерную для рыночной экономики проблему асимметрии информации⁵.

Исходя из всего вышесказанного, можно сделать вывод о том, что глобализация экономики и внедрение технологических новаций в деятельность кредитных организаций несет с собой сразу несколько новых угроз как для всей банковской системы в целом, так и для отдельных банков. С другой стороны, ключевое изменение ситуации - это усиление конкуренции, поэтому банкам для

⁵ Россия в глобализирующемся мире: Стратегия конкурентоспособности / Российская академия наук, отделение общественных наук, секция экономики; акад. Д.С. Львов [и др.]. М.: Наука, 2014. С.89.

обеспечения своей экономической безопасности и устойчивости в новых, более жестких, конкурентных условиях, необходимо не только проводить меры, предупреждающие перечисленные угрозы, но и оптимизировать свои бизнес-процессы, снижать издержки и разрабатывать новые привлекательные банковские продукты и услуги, удобные для потребителей.

Современная экономика характеризуется тем, что вектор экономического развития часто зависит от ситуаций, складывающихся в финансовой сфере. Именно поэтому, ключевыми в международных отношениях являются валютно-кредитные и финансовые отношения⁶. Следовательно, одним из важнейших элементов национальной безопасности является безопасность финансовой системы государства. Экономическое развитие страны зависит от множества факторов: ресурсов, технологий, грамотной экономической политики, человеческого капитала. Но для того, чтобы все эти факторы могли эффективно взаимодействовать, обеспечивая экономический рост, необходим фактор финансовых ресурсов и финансовой инфраструктуры. Частью этого фактора «финансовой инфраструктуры» является банковская система страны, так как она служит источником финансирования и обеспечения движения капитала в стране. Поэтому, говоря об экономической безопасности отдельного банка, необходимо рассматривать ее и в ключе экономической безопасности страны, с учетом внешнеполитической и макроэкономической ситуации, кризисов в других регионах и динамик валютных курсов.

Последние несколько лет правительство страны декларирует необходимость реформирования экономики и внесения структурных изменений, в частности, в банковскую систему. Но банковская система не может существовать сама по себе, абстрагировавшись от реального сектора экономики, и экономическая безопасность банковского сектора России невозможна без решения проблемы восстановления всего воспроизводственного комплекса⁷. Экономика России на протяжении нескольких веков была «догоняющей», но необходимо отметить такие недостатки переноса опыта экономического и технологического развития других стран как неадекватность специфическим российским условиям и тот факт, что «заимствование» всегда будет оставлять Россию на догоняющих, а не на лидерских позициях. Под «реформированием» могут подразумеваться совершенно разные стороны жизни общества. С одной стороны, может иметься в виду развитие инновационного процесса, разработка и внедрение новых технологий. С другой стороны, модернизацию могут связывать с переменами, затрагивающими конкретные производства, государственные институты и экономические процессы. Не смотря на то, что несколько лет декларировался первый подход и было проведено несколько громких проектов (Сколково, создание государственных компаний, курирующих разработки и развитие технологий, например, РОСНАНО и т.д.),

⁶ Бочаров О.А. Формирование основ экономической безопасности банковской деятельности: Автореф. канд экон. наук. М., 2013. С.321.

⁷ Бочаров О.А. Формирование основ экономической безопасности банковской деятельности: Автореф. канд экон. наук. М., 2013. С.321.

достаточных инвестиций в научное развитие сделано не было (по сравнению с развитыми странами) и последнее время государство начало ориентироваться на второй подход к постиндустриальным преобразованиям.

Для проведения подобной политики необходимы большие средства, которые могут предоставить не только государство, но и банки. В общих чертах, взаимодействие банковского и промышленного капитала на данном этапе развития экономики происходит по следующим крупным направлениям:

- кредитование предприятий;
- прямое и портфельное финансирование крупных и стратегически важных инвестиционных проектов;
- факторинговые и лизинговые сделки;
- проведение процедуры банкротства;
- приобретение пакетов акций.

Итак, банковская сфера, являющаяся ключевой частью инфраструктуры, необходимой для нормального функционирования экономики, принимает на себя часть рисков от глобализации экономики и увеличения иностранно капитала в России, поэтому обеспечение экономической безопасности банковской системы страны становится стратегической задачей для государства. Без решения данной задачи обеспечивать поступательное развитие страны, укреплять ее безопасность невозможно.

§2. Виды преступлений в банковской сфере

Преступления в банковской сфере условно можно разделить на две группы:

- насильственные преступления (убийства, налеты, грабежи и т.д.);
- так называемые «беловоротничковые» преступления, к которым относятся всевозможные финансовые хищения и махинации.

Совершаемые в банковской сфере криминальные посягательства отличаются как особой изощренностью, многоплановостью, так и активной адаптацией преступности к новым формам и методам банковской деятельности и совершаются, как правило, организованными группами.

В настоящее время структура и динамика банковских преступлений претерпела серьезные изменения, они стали более организованными и профессиональными, повысился их интеллектуальный уровень. Преступники взяли на вооружение методы информационного обеспечения своей криминальной деятельности, все чаще используют современную технику и технологии, паразитируют на издержках и трудностях экономических реформ.

Основной целью организованных преступных группировок, внедряющихся в банковские структуры, является легализация незаконного капитала, проведение операций с преступными доходами, а также совершение мошенничества в отношении средств кредитных организаций.

Наиболее характерными действиями криминальных структур в банковской сфере являются:

- легализация преступно нажитых капиталов;
- незаконный вывоз капиталов за границу;
- организация банкротства или ликвидации кредитной организации путем дискредитации, инсценирования финансовой паники или востребования депозитов вкладчиками.

Причины разорения банковских структур внешне могут выглядеть как результат действия рыночных сил, но в действительности они могут быть вызваны спланированными действиями недобросовестных конкурентов. Подготовка таких акций оставляет материальные следы в виде «заказных» статей с целью дискредитации кредитной организации, попыток вербовки сотрудников и склонение их к предательству служебных интересов, образования лжефирм с целью хищения кредита у кредитной организации, взяток или поиска контактов с теми должностными лицами, которые правомочны осуществлять контрольные и распорядительные функции;

- создание для сотрудников кредитных организаций ситуаций, которые впоследствии используются для их шантажа, принуждения к сговору должностных лиц банковских структур;

- хищение конфиденциальной банковской информации, касающейся кредитования и иных видов деятельности кредитных организаций;

- незаконное получение и / или невозврат кредитов;

- внедрение членов организованных преступных группировок в банковские структуры, а также в число акционеров кредитных организаций, используя для этого фирмы, находящиеся под их контролем;

- силовое давление на кредитные организации по заказу конкурирующих организаций с использованием их «крыш», как правило, охранных фирм, состоящих из числа бывших сотрудников правоохранительных органов;

- решение зачастую криминальным способом гражданско-правовых конфликтов (например, связанных с возвратом долгов).

Наиболее характерными преступлениями, совершаемыми клиентами кредитно-банковских организаций являются преступления, связанные с выдачей и получением кредитов, поскольку кредитование является одной из наиболее массовых и одновременно уязвимых в криминологическом отношении банковских операций. Преступлениями, посягающими на интересы банка при осуществлении ссудных операций, являются: мошенничество, незаконное получение кредита. Рассмотрим подробнее основные способы и приемы совершения данных преступлений.

Мошенничество. Статья 159 Уголовного Кодекса (УК) РФ определяет мошенничество как хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием.

Мошенническое получение кредита основывается на представлении ложных сведений, заемщик при оформлении кредита уже предполагает не возвращать его, и имеет умысел на завладение имуществом или приобретение права на него в момент осуществления действий, повлекших передачу этого имущества.

Можно выделить несколько видов преступных посягательств сопряженных с мошенничеством при кредитовании в банковской сфере:

1) Хищений денежных средств банка путем оформления кредитов на подставных и несуществующих лиц.

2) Введение в заблуждение потенциальными ссудозаемщиками банковских служащих путем:

использования специально созданных для хищения кредитных средств фиктивных предприятий, фирм-однодневок (учредители и руководители такого предприятия присваивают полученный кредит и скрываются от кредиторов, фирма «исчезает»).

Наиболее распространенными способами создания таких предприятий являются:

- создание предприятия лицами, не намеревающимися заниматься хозяйственной деятельностью, регистрация таких предприятий на фиктивные адреса, по утраченным либо похищенным паспортам граждан.

- фальсификации документов, служащих обеспечением возврата кредитов, вследствие чего кредитное учреждение вводится в заблуждение относительно возможностей и перспектив возврата полученных средств и качества обеспечения кредита.

Под фальсификацией понимается подделка документов, служащих гарантией и обеспечением возврата по кредиту. Типичными примерами подобных действий являются следующие: представление в качестве залога неполноценного имущества, действительная стоимость которого не соответствует заявленной; предоставление в качестве залога имущества, не находящегося в собственности получателя кредита; предоставление в качестве залога имущества, на которое не может быть обращено взыскание; неоднократный залог одного и того же имущества.

- введение в заблуждение банка о финансовом состоянии и платежеспособности заемщика.

Создание видимости финансовой состоятельности предприятия происходит путем представления банку: недостоверной бухгалтерской и налоговой отчетности, бизнес-планов и технико-экономического обоснования предстоящих инвестиций за счет кредитных средств; оформление подложных документов в обоснование цели испрашиваемого кредита (например, представление договоров о якобы заключенных сделках); подложных документов на право получения кредита на льготных условиях, по заниженной процентной ставке.

Незаконное получение кредита. Действующим законодательством установлена уголовная ответственность за незаконное получение кредита - статья 176 УК РФ. Применительно к банку данным понятием охватывается четыре вида преступлений:

1) получение индивидуальным предпринимателем или руководителем организации кредита путем представления банку заведомо ложных сведений о хозяйственном положении либо финансовом состоянии, если это деяние

причинило крупный ущерб;

2) получение индивидуальным предпринимателем или руководителем организации льготных условий кредитования путем представления банку заведомо ложных сведений о хозяйственном положении либо финансовом состоянии, если это деяние причинило крупный ущерб;

3) незаконное получение государственного целевого кредита, если это деяние причинило крупный ущерб гражданам, организациям или государству;

4) использование государственного целевого кредита не по прямому назначению, если это деяние причинило крупный ущерб гражданам, организациям или государству.

Зачастую руководители организаций, получающих кредиты, имеют коррупционные связи с руководителями банковских учреждений. Основной причиной необоснованного предоставления кредитов и их расходования не по назначению является отсутствие при заключении договоров кредитования контроля и необходимости проверок со стороны коммерческих банков подлинности и достоверности документов заемщика, его платежеспособности, квалифицированных проводок, экономического обоснования кредитных проектов, а также дальнейшего использования полученных кредитов в соответствии с деятельностью, объявленной в Уставе заемщика.

Общественная опасность преступлений, совершенных в сфере кредитования, заключается в том, что приводит к очень тяжким последствиям как для самих банков (т.е. отзыв лицензии, банкротство и т.п.), так и для экономики страны в целом. К негативным последствиям можно отнести как банкротство заемщика, в т.ч. и преднамеренное, так и отмывание денежных средств или имущества, приобретенных незаконным путем. Опасность банкротства и незаконного вывода безналичных денежных средств юридических лиц в теневой наличный оборот очевидна – данные процессы ведут к нестабильности в экономике, а в худшем случае к кризису.

§3. Современное состояние в сфере обращения банковских платежных пластиковых карт в России

Пластиковая карта — обобщающий термин, который обозначает все виды карточек, различающихся по назначению, по набору оказываемых с их помощью услуг, по своим техническим возможностям и организациям, их выпускающим. Важнейшая особенность всех пластиковых карт, независимо от степени их совершенства, состоит в том, что на них хранится определенный набор информации, используемый в различных прикладных программах.

В настоящее время на территории России действуют десятки локальных, региональных и межрегиональных платежных систем. Количество держателей пластиковых карточек российских платежных систем исчисляется в совокупности многими сотнями тысяч. В исследовании А.В.Евстратова и А. И.Бережновой обозначена сильная зависимость между состоянием рынка электронных платежных систем и объемом продаж в РФ, что свидетельствует о

необходимости развития рынка электронных платежных систем, которые оказывают прямое влияние на рост экономики страны⁸.

В условиях введенных против России санкций бесперебойность и безопасность осуществления транзакций находятся под угрозой из-за подверженности международных платежных систем политическому влиянию со стороны США и Евросоюза. В этих условиях необходимым стало создание национальной платежной системы (НПС), не зависящей от внешних сил. С целью изучения состояния национальной платежной системы на современном этапе, анализа существующих проблем, поиска путей их решения и определения перспектив для начала рассмотрим российский рынок платежных систем⁹.

В 2014 году на одного гражданина Российской Федерации приходилось 1,6 банковской карты. Данный показатель имеет тенденцию к росту: так, с 2011 года он увеличился на 40%, при этом его значение стало сопоставимо с показателями, характерными для ведущих мировых держав (в 2014 году в США на человека приходилось 3,75 банковской карты, в Китае – 3,61, в Великобритании – 2,4, в Германии – 1,63, а в Италии – 1,22 карты¹⁰).

Российский рынок платежных систем, кроме всего прочего, можно охарактеризовать через такой показатель, как количество эмитированных карт. Динамика изменения значений данного показателя представлена на рис. 1.

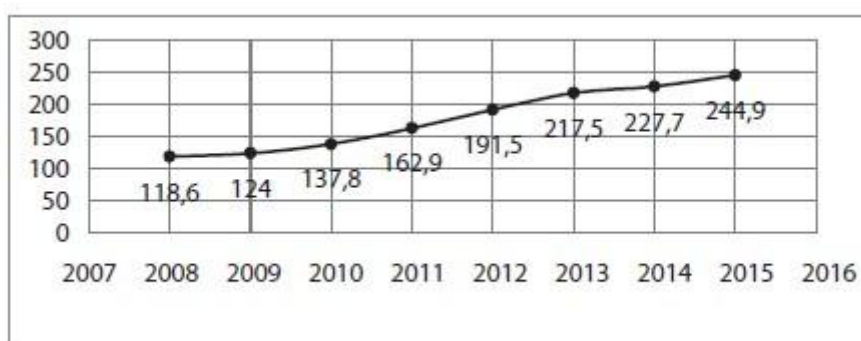


Рис. 1. Количество электронных платежных пластиковых карт, эмитированных в Российской Федерации, млн. ед., 2007-2015 гг.¹¹

Увеличение количества карт, эмитированных на территории России, свидетельствует о том, что российский рынок банковских карт находится в постоянном развитии. За период с 2008 по 2015 годы количество банковских карт увеличилось более чем в два раза, что свидетельствует о высоком и постоянно растущем спросе на данную банковскую услугу на российском рынке.

⁸ Евстратов А.В., Бережнова А.И. Развитие рынка электронных платежных систем и его роль в экономике Российской Федерации // Известия Волгоградского государственного технического университета. 2013. № 11 (144). С. 74-79.

⁹ Теряева А.С., Журавлева Т. А., Харитонюк Е. С. Национальная платежная система России: предпосылки возникновения и текущее состояние// Дискуссия. Выпуск №2 (65) февраль 2016. С. 54.

¹⁰ Отчет о платежных системах за 2014 год Банка международных расчетов [Электронный ресурс]. URL: <https://www.bis.org/cpmi/publ/d142a.pdf> (дата обращения: 27.01.2016).

¹¹ Центральный банк Российской Федерации [Электронный ресурс]. URL: <http://www.cbr.ru/> (дата обращения: 27.10.2016).

Количество эмитированных карт в США, рынок которых является самым развитым национальным рынком в данном аспекте, выше, чем в России: в 2014 г. – 1246,7 млн. карт, что в 5 раз больше аналогичного показателя в России¹².

Структура операций, совершаемых с использованием банковских карт, значительно изменилась с ростом объемов самих операций (рис. 2).

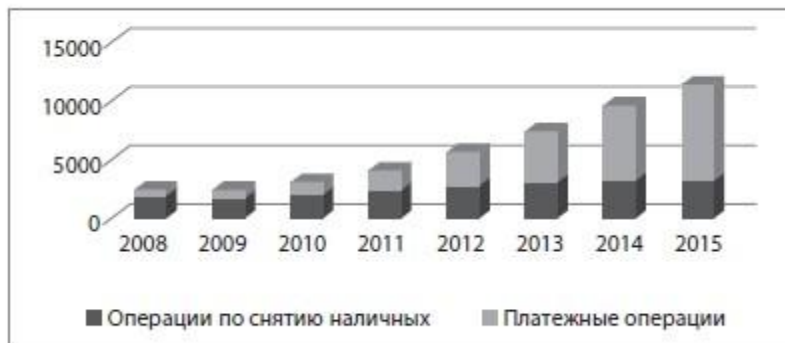


Рис. 2. Количество операций с электронными платежными пластиковыми картами, эмитированными в Российской Федерации, млн. ед., 2007-2015 гг.

В 2008 году доля платежных операций в России была равна 20,6 %, в 2015 году – 71,5 %, т. е. увеличилась практически в 3,5 раза. Число расчетных карт в общем объеме карт, эмитированных в России (87 %), значительно превышает число кредитных, что свидетельствует об использовании карт в основном с целью оплаты товаров и услуг. Таким образом, можно сделать вывод, что российский рынок платежных систем будет активно развиваться. Об этом также свидетельствуют такие факты, как постоянно увеличивающийся спрос и появление новых технологий, позволяющих использовать банковские карты максимально комфортно.

В связи с созданием в России национальной системы платежных карт (НСПК)¹³ одним из условий работы на российском рынке (с 1 июля 2016 года) для операторов платежных систем станет необходимость использования платежной инфраструктуры, находящейся на территории России. Передача информации по осуществляемым операциям по картам на территорию иностранного государства или доступ иностранцев к этой информации будут запрещены (если операции проводятся внутри страны)¹⁴.

Несмотря на быстрый рост данного рынка, существует ряд проблем, препятствующих его развитию. Эти проблемы могут быть разделены на две группы: проблемы, связанные с состоянием российской инфраструктуры, и проблемы, вызванные введением экономических санкций США, Евросоюзом и рядом других стран в 2014 году.

¹² Отчет о платежных системах за 2014 год Банка международных расчетов [Электронный ресурс]. URL: <https://www.bis.org/cpmi/publ/d142a.pdf> (дата обращения: 27.10.2016).

¹³ Федеральный закон "О национальной платежной системе" от 27.06.2011 N 161-ФЗ (действующая редакция, 2016) [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_115625/ (дата обращения: 27.10.2016).

¹⁴ Национальная система платежных карт Российской Федерации [Электронный ресурс]. URL: <http://www.nspk.ru/> (дата обращения: 27.10.2016).

К первой группе можно отнести следующие проблемы:

1. Слабое развитие инфраструктуры по приему безналичных платежей, особенно в разрезе мелких розничных магазинов и сетей. В России количество электронных терминалов (POS-терминалов), установленных в организациях торговли (услуг), в 2014 году составило 1288700 ед. (в США, для сравнения, их более 6 млн. ед.)¹⁵.

2. Недостаточно развитая по сравнению со странами Запада и Азиатско-Тихоокеанского региона сеть устройств самообслуживания. Лишь немногие банки могут позволить себе держать разветвленную сеть филиалов и банкоматов. Общее количество банкоматов в России в 2015 году составило 222,8 тыс. ед., в Китае – 614,9 тыс. ед., в США - 425 тыс. ед.¹⁶

3. Отторжение населением различных нововведений, в том числе использования платежных карт для совершения платежей. Несмотря на то, что банковские карты появились в России в 1991 году, их широкое применение началось только 5-7 лет назад.

Проблемы, относящиеся ко второй группе, связаны с введением экономических санкций в 2014 году. И хотя по состоянию на конец 2015 года санкции прямо не затрагивают взаимодействие российских банков и иностранных платежных систем в целом, имеют место быть несколько прецедентов. Так, платежные системы «Visa» и «Master Card» в 2014 году заблокировали операции по картам банка «Россия» и «СМП Банка» после того как они попали в «санкционный список». 22 декабря 2015 года, после решения США о расширении санкций в отношении России, еще шесть банков были отключены от международных платежных систем «Visa» и «Master Card»: «Генбанк», «Крайинвестбанк», банк «Верхневолжский», «Севастопольский морской банк» – в связи с работой в Крыму; «Инресбанк» и «Мособлбанк» – из-за причастности к «СМП Банку». Помимо этого, «Visa» и «Master Card» не работают на всей территории Крымской республики, т.е. эмиссия и обслуживание карт данных систем не осуществляется.

Следовательно, иностранные платежные системы могут быть использованы для давления на российскую экономику через отключение российских банков от них, что создаст коллапс в расчетах и предоставлении других финансовых услуг. Соответственно, создание национальной платежной системы было верным решением в сложившейся ситуации.

Национальная платежная система РФ была создана 23 июля 2014 года одновременно с учреждением АО «Национальная система платежных карт» (АО НСПК), 100% акций которого принадлежат Центробанку РФ. Деятельность АО НСПК регулируется Федеральным законом № 161 «О национальной платежной системе», «Стратегией развития Национальной платежной системы» и «Концепцией создания национальной системы платежных карт». Главными

¹⁵ Отчет о платежных системах за 2014 год Банка международных расчетов [Электронный ресурс]. URL: <https://www.bis.org/cpmi/publ/d142a.pdf> (дата обращения: 27.10.2016).

¹⁶ Национальная система платежных карт Российской Федерации [Электронный ресурс]. URL: <http://www.nspk.ru/> (дата обращения: 27.10.2016).

целями системы являются обеспечение суверенитета и безопасности платежного пространства России, а также бесперебойности осуществляемых на ее территории транзакций.

Для достижения вышеназванных целей всем иностранным платежным системам, работающим на территории России, было необходимо до 31 марта 2015 года передать НСПК обработку транзакций, проводимых внутри страны.

К концу 2015 года АО НСПК было реализовано следующее:

1. Все внутрироссийские транзакции международных платежных систем стали проходить через операционный процессинговый и клиринговый центр (ОПКЦ) НСПК.

2. Создана, протестирована и внедрена операционно-технологическая платформа, на которой базируется ОПКЦ НСПК.

3. Идет реализация унифицированных протоколов межбанковского взаимодействия.

4. Разработано и проходит сертификацию собственное платежное приложение для микропроцессорной карты на основе международного стандарта EMV.

5. Состоялся первый выпуск карт платежной системы «Мир», чьим оператором является АО НСПК, семью российскими банками: «Газпромбанком», «МДМ Банком», «Московским индустриальным банком», «Связь-Банком», РНКБ, банком «Россия» и «СМП Банком»¹⁷.

Предполагается, что в будущем карта «Мир» займет лидирующее положение на российском рынке, а затем выйдет и на мировой. Целевой аудиторией данной карты являются получатели бюджетных средств: пенсионеры; медицинские работники; лица, получающие социальные выплаты; студенты, получающие стипендии, и т.д. (охват данной аудитории должен составлять не менее 85%). И хотя 15 декабря 2015 года АО НСПК официально объявило о начале эмиссии платежных карт «Мир» семью российскими банками, фактически эмиссия состоялась не полностью. Банки выпускают данные карты в тестовом режиме, развивают эквайринговую систему, подходящую для «Мира».

На начальном этапе выпуск и использование карт платежной системы «Мир» осложнены некоторыми обстоятельствами:

1. Эквайринговая сеть «Мира» – система приема платежных карт для оплаты товаров, услуг, работ – недостаточно развита, что делает саму карту в некотором роде бесполезной, поскольку она почти не принимается к оплате. На начальном этапе платежная система «Мир» работает по мировому стандарту EMV, но с уникальными чипами российских производителей; однако в будущем, как только будет разработан отечественный стандарт, «Мир» перейдет на него. Поэтому данная проблема еще более усугубится из-за особого криптографического модуля карты, который будет отличаться от международных стандартов. Из чего следует, что для приема карт «Мир» к

¹⁷ Национальная система платежных карт Российской Федерации [Электронный ресурс]. URL: <http://www.nspk.ru/> (дата обращения: 27.01.2016).

оплате владельцам POS-терминалов придется обновить свое оборудование и поставить на него сертифицированный аппаратный криптографический модуль, стоимость которого может достигать нескольких тысяч долларов. Таким образом, эквайринговая сеть может не получить должного развития и распространения.

2. Большинство российских банкоматов не приспособлено для работы с картой «Мир», что также связано с ее технической уникальностью. В декабре 2015 года только 1,5 тыс. банкоматов из 213,5 тыс. принимали к обслуживанию данную карту. Это банкоматы 7 банков – эмитентов «Мира». По прогнозам АО НСПК, к концу третьего квартала 2016 года более 90% банкоматов и терминалов будут готовы к работе с картой «Мир». Эксперты считают, что с учетом будущей переориентации на отечественный стандарт переходный период займет 5-7 лет – в течение этого времени старые банкоматы и POS-терминалы будут заменяться на новые, поддерживающие отечественную криптографию.

3. Внедрение платежной системы «Мир» – дорогостоящий процесс. Все работы (создание эквайринговой сети, выпуск карт, а также оплата услуг вендора, запуск платежной системы «Мир») могут обойтись банку примерно в 100 тыс. долл., а сопровождение и обслуживание системы могут стоить около 5 млн долл. в год. Разница в цене эмиссии карт «Мир» и «Visa», «MasterCard» составляет около 35-40 % в пользу зарубежных. При необходимости несения банками таких расходов высока вероятность подорожания банковских услуг, поскольку банкам придется компенсировать возникшие расходы.

Несмотря на существующие проблемы, национальной платежной системе и карте «Мир» предрекают успешное будущее. АО НСПК планирует выпускать до 30 млн карт уже в 2016 году, а также надеется, что к концу третьего квартала того же года сеть приема платежной системы «Мир» будет сравнима с сетью приема других платежных систем. Более того, спектр услуг по данной карте будет существенно расширен: к концу 2016 года должны появиться карты с револьверным кредитованием, длинными grace-периодами, бесконтактные карты, мобильное приложение, защита «3D Secure». Успеху в распространении «Мира» на территории России также способствуют законодательные нормы, которые обязывают крупные, значимые банки эмитировать и обслуживать данные карты, а бюджетные учреждения – выдавать их своим сотрудникам в рамках зарплатных проектов¹⁸.

В сложившихся экономических и политических условиях создание российской платежной национальной системы является важным инструментом нейтрализации угроз и повышения эффективности функционирования системы национальной безопасности, поскольку международные платежные системы подвержены политическому влиянию со стороны. Благодаря переводу обработки транзакций международных платежных систем на НСПК на территории России обеспечиваются бесперебойность их осуществления, защита и суверенитет платежного пространства. Дальнейшее развитие НПС определяется

¹⁸ Там же.

необходимостью совершенствования законодательства, его правовых норм как основы: инновационного формирования расчетов; развития рынка платежных инструментов; создания более эффективной инфраструктуры и технико-технологической материальной базы; корректирования тарифной политики; стандартов надзора за розничными операторами услуг в этой системе.

Конкуренция и технологические особенности функционирования существующих в России систем препятствуют их интеграции в ближайшей перспективе, что, в целом, является сдерживающим фактором развития безналичных расчетов в сфере розничных платежей. Развитие российского рынка платежных карт является одним из важнейших факторов при решении задач по сокращению расчетов наличными деньгами и развитию безналичных расчетов в области розничных платежей. Для решения указанной задачи Банком России проводится работа по созданию условий для дальнейшего совершенствования современных инструментов розничных платежей, способствующих развитию в России карточной индустрии.

Развитие карточной индустрии обеспечивает повышение прозрачности финансовых операций, прирост налоговых поступлений, существенно снижает издержки, связанные с обслуживанием наличного денежного оборота, ведет к увеличению объема привлеченных денежных средств в банковскую сферу и, соответственно, кредитных возможностей банков, а также во многом способствует активному развитию смежных сфер деятельности, таких как производственная, социальная и сфера занятости.

ГЛАВА 2. МЕТОДЫ ПРЕДОТВРАЩЕНИЯ МОШЕННИЧЕСТВА, СВЯЗАННОГО С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННЫХ ПЛАТЕЖНЫХ ПЛАСТИКОВЫХ КАРТ

2.1. Уголовно-правовая характеристика и проблемы квалификации мошенничества, совершаемого в банковской сфере с использованием электронных платежных пластиковых карт¹⁹

Одним из самых распространенных видов высокотехнологичного мошенничества является мошенничество с использованием платежных карт, что обусловлено их обширным распространением среди населения, низкой культурой использования; сравнительной легкостью получения данных карты жертвы, сложность идентификации мошенника и сбора доказательств его вины. Это предопределило выделение мошенничества с использованием платежных карт в качестве разновидности мошенничества, что повлекло за собой включение в Уголовный кодекс Российской Федерации отдельной статьи, предусматривающей уголовную ответственность за совершение данного деяния (159.3 УК РФ).

Введение в Уголовный кодекс РФ статьи, предусматривающей ответственность за совершение мошенничества с использованием платежных карт, - это абсолютная новелла для российского права, несмотря на то, что в работах ряда исследователей киберпреступлений неоднократно указывалось на необходимость введения такого состава в российское уголовное право²⁰. Подобные составы давно включены в уголовное законодательство многих зарубежных государств.

Согласно статистике Центрального Банка РФ, общее количество эмитированных банковских карт за последние 7 лет возросло более чем на 50%. Так, если в 2008 г. количество банковских карт составляло 118 101, то уже по состоянию на 1 октября 2015 г. их количество возросло до 240 521, ежегодно их количество возрастало на 7%²¹. Как правило, платежная карта выпускается банком для клиентов с целью доступа к своим денежным средствам и осуществления иных услуг. Подобные карты привязываются напрямую к собственному расчетному счету клиента или к кредитному счету, связанному с использованием в определенном количестве денежных средств банка, на условиях возвратности. В соответствии с Положением Центрального Банка от 24.12.2004 № 266 «Об эмиссии платежных карт и об операциях, совершаемых с

¹⁹ При написании данного параграфа использованы материалы диссертации Южина А.А. на тему: Мошенничество и его виды в российском уголовном праве. Диссертация на соискание ученой степени кандидата юридических наук. Специальность: 12.00.08 – уголовное право и криминология; уголовно-исполнительное право. Москва, Московский государственный юридический университет имени О.Е. Кутафина (МГЮА), 2016 г. С. 153-164.

²⁰ См., например: Добрынин Ю. Классификация преступлений, совершаемых в сфере компьютерной информации [Электронный ресурс]. URL: http://www.russianlaw.net/law/computer_crime/a158/ (дата обращения: 04.11.2016).

²¹ По данным Центрального Банка Российской Федерации [Электронный ресурс] URL: <https://www.cbr.ru/>. Проверено на 30.10.2016.

их использованием» (далее положение ЦБ от 24.12.2004 № 266), кредитная организация осуществляет эмиссию расчетных (дебетовых) карт, кредитных карт и предоплаченных карт для физических лиц, юридических лиц и индивидуальных предпринимателей. Расчетная небанковская кредитная организация осуществляет эмиссию расчетных (дебетовых) карт для юридических лиц, индивидуальных предпринимателей, предоплаченных карт - для физических лиц, юридических лиц, индивидуальных предпринимателей²².

Платежная небанковская кредитная организация осуществляет эмиссию предоплаченных карт для физических лиц, юридических лиц, индивидуальных предпринимателей. В зависимости от условий предоставления банком-эмитентом платежной карты клиенту с помощью этого инструмента возможно: получать денежные средства как напрямую в кредитных организациях, так и через программно-технический комплекс, предназначенный для автоматизированной выдачи и приема наличных денежных средств (банкомат, банковский автомат); либо использовать ее в качестве средства платежа, в том числе и через сети Интернет. Платежная карта в диспозиции ст. 159.3 УК РФ выступает в качестве родового понятия, объединяющего конкретные виды карт: кредитные, расчетные и иные карты. Кредитная карта предполагает, что банк-эмитент обязуется предоставлять денежные средства клиенту в зависимости от установленных тарифов в течение определенного срока и в определенных пределах. В соответствии с положением ЦБ от 24.12.2004 № 266 предусматриваются два порядка осуществления операций с использованием кредитных карт. В первом случае денежные средства поступают непосредственно на банковский счет клиента, а во втором случае они предоставляются клиенту с использованием банковского счета. В случае, если клиент является нерезидентом РФ, то денежные средства ему предоставляются в валюте, в остальных случаях физическим лицам предусматривается выдача в валюте РФ²³.

Важным условием является обязательность возврата клиентом денежных средств кредитной организации. Расчетная карта (дебетовая карта) является средством платежа, привязанным напрямую к счету клиента и обеспечивает ему беспрепятственный доступ к своим денежным средствам (аналог дорожного чека). В качестве иных карт может выступать, например, предоплаченная платежная карта. Последняя является электронным средством платежа и используется для осуществления перевода электронных денежных средств, возврата остатка электронных денежных средств в пределах суммы предварительно предоставленных держателем денежных средств кредитной

²² См.: Положение об эмиссии платежных карт и об операциях, совершаемых с их использованием (утв. Банком России 24.12.2004 № 266-П) (ред. от 14.01.2015) (Зарегистрировано в Минюсте России 25.03.2005 № 6431) // Вестник Банка России. № 17. 30.03.2005.

²³ Положение об эмиссии платежных карт и об операциях, совершаемых с их использованием (утв. Банком России 24.12.2004 № 266-П) (ред. от 14.01.2015) (Зарегистрировано в Минюсте России 25.03.2005 № 6431) // Вестник Банка России. № 17. 30.03.2005.

организации-эмитенту в соответствии с требованиями ФЗ от 27.06.2011 № 161 «О национальной платежной системе»²⁴ (далее ФЗ от 27.06.2011 № 161) (телефонные карты, электронный проездной и т.д.).

При осуществлении платежей при помощи электронного средства платежа нет необходимости в заведении отдельного банковского счета. Перемещение электронных денежных средств происходит не по банковским информационным системам, а по специально предназначенным для этой карты сетям, где они хранятся на консолидированном счете. Электронные денежные средства представляют собой определенную информацию, которая была конвертирована в эквивалент, выраженный в стоимостной или натуральной единице (деньги, минуты, количество поездок, литры и т.д.). В зависимости от территории действия различают карты локального характера, использование которых возможно в офисах, банкоматах банка эмитента, как правило, в пределах одной страны (Оперативная российская платежная система Сберкарт), и международного характера, используемые в качестве универсального средства платежа на территории стран-участников, где принимаются данные карты (Visa, Master Card, Diners Club, American Express, JCB и China Unionpay).

В настоящий момент в РФ на основании ФЗ от 27.06.2011 № 161 создана российская национальная система платежных карт (НСПК). В качестве субъектов, участвующих в этих отношениях, можно выделить держателя карты, собственника карты и владельца. Держателем карты является лицо, на чье имя она непосредственно выпущена, т.е. тот, кто является субъектом права пользования данной карты. Как уже указывалось, денежные средства на счете карты принадлежат непосредственно держателю, и банк не имеет на них никаких прав. Основанием для приостановления операций по счету может являться наличие решения суда. В качестве собственника выступает банк-эмитент. При этом банк-эмитент не пользуется полномочиями собственника через признанную классическую триаду, установленную в ст. 209 ГК РФ. Эти права лишь распространяются на саму карту как физический предмет, но не в отношении ее содержимого, т.е. того счета, к которому она привязана, если это только не денежные средства самого банка или иной кредитной организации. В ряде случаев признано необходимым выделять владельца карты, т.е. то лицо в чьем владении находится карта. При этом в качестве такого владельца может выступать и не держатель карты. При выпуске платежной карты и в случаях ее использования кредитная организация обязана идентифицировать ее держателя в соответствии с ФЗ от 07.08.2001 № 115 «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма». Следовательно, каждая карта подлежит процедуре персонализации, в соответствии с которой ей присваивается определенный номер, имя держателя, срок действия. При этом все необходимые данные,

²⁴ См.: Положение об эмиссии платежных карт и об операциях, совершаемых с их использованием (утв. Банком России 24.12.2004 № 266-П) (ред. от 14.01.2015) (Зарегистрировано в Минюсте России 25.03.2005 № 6431) // Вестник Банка России. № 17. 30.03.2005.

связанные с информацией о держателе карты, наносятся на магнитную полосу и (или) в память микропроцессора карты, при наличии чипа. При совершении каких-либо операций с картой денежные средства могут поступать как с одного счета, к которому привязана карта (кредитная или расчетная), так и с нескольких счетов клиента, к которым эта карта также привязана. Для удобства клиента допускается также использование нескольких карт по одному счету, например, для членов семьи. Для юридических лиц и индивидуальных предпринимателей предусматриваются определенные ограничения на снятие наличных денежных средств в течение одного операционного дня. Для физических лиц банки и иные кредитные организации устанавливают собственные денежные лимиты. Норма о мошенничестве с использованием пластиковых карт (ст. 159.3 УК РФ) призвана обеспечивать помимо охраны собственности также и нормальную деятельность банков и иных кредитных организаций, связанную с беспрепятственным доступом клиентов к своим денежным средствам в необходимый момент.

Платежные карты сложно назвать предметом преступления, поскольку сама по себе карта никакой ценности не представляет, кроме как затрат по себестоимости при ее изготовлении. В результате завладения платежной картой субъект преступления стремится получить доступ к денежным средствам на счете, к которому привязана данная карта. Диспозиция части 1 статьи 159.3 УК сформулирована следующим образом: мошенничество с использованием платежных карт, то есть хищение чужого имущества, совершенное с использованием поддельной или принадлежащей другому лицу кредитной, расчетной или иной платежной карты путем обмана уполномоченного работника кредитной, торговой или иной организации. Непосредственным объектом указанного преступления, как видно из диспозиции, является собственность, то есть общественные отношения, связанные с владением, пользованием и распоряжением имуществом. Объективная сторона преступления заключается в обмане, в результате которого уполномоченный работник кредитной, торговой или иной организации (например, официант в ресторане), будучи введенным в заблуждение относительно того факта, что перед ним находится держатель карты, принимает предоставленную платежную карту в качестве средства платежа. Лицо, предоставляющее данную карту, в подтверждение своего обмана в личности, расписывается на товарном чеке, совершает иные юридически значимые действия, указывающие на то, что именно он якобы является держателем карты.

Мошенничество с использованием платежных карт рассматривается в ст. 159.3 УК РФ как форма хищения. Следовательно, преступление считается оконченным с момента, когда лицо, получив платежную карту, имело реальную возможность воспользоваться ей как средством платежа или обналичить денежные средства через уполномоченного сотрудника кредитной организации. В.В. Хилута подчеркивает, что ущерб причиняется собственнику, когда

имущество вышло из обладания субъекта²⁵. Если же деятельность субъекта этого вида мошенничества была пресечена при попытке использования платежной карты, то реальной возможности у лица воспользоваться ею не представилось. Такие действия необходимо квалифицировать как покушение на совершение преступления. Если же лицо просто владеет или приобрело поддельную карту, то речь может идти лишь о приготовлении к мошенничеству с использованием платежных карт. При этом сущность мошенничества как хищения чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием сохраняется и в рамках данного состава преступления. Под хищением, в соответствии с примечанием 1 к статье 158 УК, понимается совершенные с корыстной целью противоправные безвозмездное изъятие и (или) обращение чужого имущества в пользу виновного или других лиц, причинившие ущерб собственнику или иному владельцу этого имущества.

Согласно приговору Ленинского районного суда, г. Новосибирска, действия В. были квалифицированы как покушение на совершение мошенничества с использованием платежных карт, с использованием своего служебного положения в крупном размере. В. являясь менеджером по продажам ОАО «СБ», от имени клиентов банка, данными которых он обладал в силу его служебного положения, заполнял заявления на получение кредитных карт, после чего удостоверял эти документы у своего руководителя, вводя его в заблуждение относительно достоверности, и получал в свое распоряжение ПИН-коды для кредитных карт. Действуя по такой схеме, В. оформил на свое имя 72 кредитные карты с общей суммой кредитного лимита 3 886 000 руб. Полученные карты хранил у себя дома, однако воспользоваться ими не смог, поскольку его деятельность была пресечена сотрудниками полиции при обыске его квартиры²⁶.

Поскольку В., согласно материалам дела, не пытался воспользоваться данными картами, это представляет собой частный случай приискания орудия преступления (кредитная карта), что предполагает создание условий совершения преступления и относится в соответствии с ч.1 ст. 30 УК РФ к стадии приготовления, а не покушения. Если же рассматривать эту же ситуацию с другой точки зрения, то тут налицо коллизия со ст. 1591 УК РФ (мошенничество в сфере кредитования). В связи с тем, что денежные средства при оформлении заявления на получение кредитной карты предоставляются в определенных объемах и на определенный срок, при условии возвратности, то в соответствии со ст. 1591 УК РФ это предполагало бы оконченное преступление. Единственное, что их различает, - это средство преступления, в соответствии с которым им выступает кредитная карта, хотя объект преступления у этих составов

²⁵ См.: Хилюта В.В. Момент окончания хищения: практика применения теоретических концепций // Вестник БДУ. Сер. 3. 2010. № 3. С. 93.

²⁶ Приговор Ленинского районного суда г. Новосибирск от 04.03.2015. Дело № 1-39/2015 // http://sudact.ru/regular/doc/ejbXHqxAfVE/?regulartxt=%D1%87.3+%D1%81%D1%82.+30++%D1%81%D1%82.+159.3®ular-case_doc=®ulardoc_type=1008®ular-date_from=®ular-date_to=®ular-workflow_stage=®ular-area=®ularcourt=®ular-judge=&_id=1451391460487&snippet_pos=374#snippet

одинаковый, как основной, так и факультативный. Определенные вопросы возникают с однозначным отнесением настоящего деяния к видам мошенничества.

В соответствии с п.1 постановления Пленума Верховного Суда РФ от 27.12.2007 № 51 особенность мошенничества как формы хищения предполагает, что в результате обмана или злоупотребления доверием владелец имущества или иное лицо либо уполномоченный орган власти добровольно передают имущество или право на него. В описанной ситуации добровольно имущество никто не передает. Как уже было отмечено, платежная карта, выступает орудием преступления, с помощью которого субъект мошенничества пытается получить доступ к денежным средствам. Когда происходит обман представителя торговой организации (официанта), никто не удостоверяет, является ли данное лицо правомочным держателем карты или нет. Списание денежных средств происходит до того момента, как владелец карты ставит свою подпись на чеке.

Определенные вопросы возникают с однозначным отнесением настоящего деяния к видам мошенничества. В соответствии с п.1 постановления Пленума Верховного Суда РФ от 27.12.2007 № 51, особенность мошенничества как формы хищения предполагает, что в результате обмана или злоупотребления доверием владелец имущества или иное лицо либо уполномоченный орган власти добровольно передают имущество или право на него. Как уже было отмечено, платежная карта, выступает орудием преступления, с помощью которого субъект мошенничества пытается получить доступ к денежным средствам. Когда происходит обман представителя торговой организации (официанта), никто не удостоверяет, является ли данное лицо правомочным держателем карты или нет. Списание денежных средств происходит до того момента, как владелец карты ставит свою подпись на чеке. Наглядную аналогию проводит Л.В. Боровых, сравнивая банковскую карту с ключом от квартиры или иного помещения, где находится имущество. Самостоятельно ключ не представляет никакой ценности для преступника, большее значение имеет к чему может открыть доступ этот ключ²⁷. Однако определенную аналогию с мошенничеством с использованием платежных карт можно провести. Допустим, что держатель карты добровольно передает ее лицу, но при этом не передает соответствующие права на ее использование. В этом случае лицо не становится законным владельцем этой карты, когда пользуется ей в торговой организации, расписываясь за держателя. Подобные действия должны квалифицироваться аналогичным образом как кража по соответствующей части ст. 158 УК РФ. Определенные подтверждения этому можно найти и на практике. В соответствии с приговором Ленинского районного суда г. Новосибирска П. был признан виновным в совершении кражи с проникновением в жилище, с причинением значительного ущерба. Согласно материалам дела, у П. имелись ключи от квартиры, где она ранее проживала с потерпевшими Ф. и Х., которые сменили верхний замок, как только П. перестала

²⁷ Боровых Л.В., Корепанова Е.А. Проблема квалификации хищения с использованием банковских карт//Российский юридический журнал. 2014. № 2. С. 86.

совместно с ними проживать. Пытаясь проникнуть в квартиру в отсутствии Ф. и Х. и узнав, что ключ не подходит к одному из замков, П. попросила одного из соседей помочь ей открыть дверь, которая якобы захлопнулась, когда П. выходила на лестничную площадку, тем самым введя его в заблуждение. При помощи соседа П. проникла в квартиру и похитила денежные средства в сумме 15 000 рублей, а также определенное имущество и скрылась с места преступления²⁸.

В приведенном примере совершенно верно действия были квалифицированы как кража (п. «а», ч.3, ст. 158), поскольку способ совершения преступления был тайным²⁹. Однако определенную аналогию с мошенничеством с использованием платежных карт можно провести. Допустим, что держатель карты и добровольно передает ее лицу, но при этом не передает соответствующие права на ее использование. В этом случае лицо не становится законным владельцем этой карты, когда пользуется ей в торговой организации, расписываясь за держателя. Подобные действия должны квалифицироваться аналогичным образом как кража по соответствующей части ст. 158 УК РФ.

Определенные подтверждения этому можно найти и на практике. Так, П. был признан виновным в совершении кражи с причинением значительного ущерба гражданину (п. «в», ч. 2, ст.158 УК РФ). П. нашел банковскую карту, узнав, что на ней отсутствует ПИН код воспользовался ей при оплате покупок в ООО «АЗС»³⁰.

В случае совершения кражи и мошенничества выносится приговор по совокупности преступлений. Подобная ситуация подтверждается приговором Кировского районного суда г. Кемерово, согласно которому П., находясь в квартире у Ф. и воспользовавшись тем, что последняя находилась в ванной, похитил ее банковскую карту. Зная ПИН код от этой карты, П. получил через банкомат денежные средства. В продолжение умысла на хищение денежных средств он также воспользовался картой при оплате покупок в магазине, обманув кассиров, выдавая карту за собственную. В результате его действия квалифицировали по п. «в» ч.2 ст. 158, ч.2 ст. 159.3 УК РФ³¹.

В соответствии с п.16 постановлением Пленума Верховного Суда РФ от 27.12.2002 № 29 разграничиваются понятия совокупности и продолжаемого

²⁸ Приговор Ленинского районного суда г. Новосибирска от 08.12.2015. Дело № 1-1128/2015 // <http://sudact.ru/regular/doc/F5Kun42Viw5w/>

²⁹ Как тайное хищение чужого имущества (кража) следует квалифицировать действия лица, совершившего незаконное изъятие имущества в отсутствие собственника или иного владельца этого имущества, или посторонних лиц либо хотя и в их присутствии, но незаметно для них (Постановление Пленума Верховного Суда РФ от 27.12.2002 № 29 (ред. от 03.03.2015) «О судебной практике по делам о краже, грабеже и разбое» // «Российская газета». № 9. 18.01.2003).

³⁰ Приговор Ленинского районного суда г. Новосибирска от 05.05.2015. Дело № 1-420/2015 // <http://sudact.ru/regular/doc/n1gmRVeglg/>

³¹ Приговор Кировского районного суда г. Кемерово, кемеровской области от 12.11.2015. Дело № 1-395/15 // <http://sudact.ru/regular/doc/Y1E4KZB0MKoV/>

хищения³². По мнению специалистов по вопросам мошенничества в банковской сфере с использованием электронных платежных пластиковых карт³³, вышеприведенный пример указывает на тот факт, что виновный дважды стремился получить денежные средства Ф., при этом источник этих денежных средств был в обоих случаях одинаковый. Поэтому несмотря на несколько эпизодов хищения дополнительная квалификация по ст. 159.3 УК РФ является излишней. Так, С. совершил хищение денежных средств с банковской карты, принадлежащей К., совершив 123 разные операции и его действия были квалифицированы по ч. 3 ст. 159.3 УК РФ³⁴.

Ряд авторов считает, что ввиду вышесказанного представляется излишним относить данный вид хищения к специальным видам мошенничества, а п. 13 абз. 2, п. 14 постановления Пленума Верховного Суда РФ от 27.12.2007 № 514 следует пересмотреть, чтобы специально подчеркнуть, что любое хищение чужих денежных средств путем использования заранее похищенной или поддельной кредитной (расчетной) карты следует квалифицировать по соответствующей части ст. 158 УК РФ³⁵. Исполнение объективной стороны мошенничества с использованием платежных карт идет в разрез с концепцией добровольности передачи имущества собственником или иным владельцем.

Субъект преступления общий - вменяемое физическое лицо, достигшее возраста наступления уголовной ответственности (16 лет). Субъективная сторона преступления характеризуется прямым умыслом. Злоумышленник осознает общественную опасность мошеннических операций с использованием платежных карт, предвидит наступление общественно опасных последствий и желает их наступления. Части вторая-четвертая указанной статьи содержат квалифицирующие признаки преступления, полностью совпадающие с закрепленными в статье 159 УК.

2.2. Криминалистическая характеристика мошенничества с

³² От совокупности преступлений следует отличать продолжаемое хищение, состоящее из ряда тождественных преступных действий, совершаемых путем изъятия чужого имущества из одного и того же источника, объединенных единым умыслом и составляющих в своей совокупности единое преступление (Постановление Пленума Верховного Суда РФ от 27.12.2002 № 29 (ред. от 03.03.2015) «О судебной практике по делам о краже, грабеже и разбое» // «Российская газета», № 9. 18.01.2003).

³³ Южин А.А. Мошенничество и его виды в российском уголовном праве. Диссертация на соискание ученой степени кандидата юридических наук. Специальность: 12.00.08 – уголовное право и криминология; уголовно-исполнительное право. Москва, Московский государственный юридический университет имени О.Е. Кутафина (МГЮА), 2016 г. С. 153-162.

³⁴ Приговор Кировского районного суда г. Кемерово, кемеровской области от 12.11.2015. Дело № 1-395/15 // <http://sudact.ru/regular/doc/Y1E4KZB0MKoV/>

³⁵ Южин А.А. Мошенничество и его виды в российском уголовном праве. Диссертация на соискание ученой степени кандидата юридических наук. Специальность: 12.00.08 – уголовное право и криминология; уголовно-исполнительное право. Москва, Московский государственный юридический университет имени О.Е. Кутафина (МГЮА), 2016 г. С. 161.

Способ совершения преступления является основополагающим, системообразующим элементом, характеризующим любое преступление, в том числе и мошенничество с использованием платежных карт. Следует согласиться с позицией В.Д. Ларичева, который считает, что при объяснении логики построения криминалистической характеристики преступлений и выделении ее элементов целесообразно использовать в качестве основы механизм разбора совершения преступлений, а центральным элементом этого механизма определить именно способ совершения преступления³⁷. При владении информацией о способе совершения преступления появляется возможность выдвигать обоснованные версии о содержании других элементов криминалистической характеристики по конкретному уголовному делу.

В криминалистическом смысле мошенничество с использованием платежных карт можно определить как систему действий по подготовке, совершению и сокрытию хищения чужого имущества, основным содержанием которой (системы) является использование поддельной или принадлежащей другому лицу кредитной, расчетной или иной платежной карты для осуществления обмана уполномоченного работника кредитной, торговой или иной организации. Фактически в этом случае, как и в других видах мошенничества, содержанием мошеннических действий остается в той или иной степени качественная или количественная замена предмета и средств совершения мошенничества³⁸.

Классификации способов мошенничества с использованием платежных карт по самым различным основаниям представлены в работах ряда авторов, среди которых труды В.Б.Вехова, М.Н.Филиппова, Н.Н.Федотова и др.³⁹ Анализируя действующее законодательство с учетом произошедших изменений, вышеуказанные работы, а также сложившуюся практику расследования данной разновидности криминального обмана, можно выделить ряд классификаций, которые имеют наибольшее значение в криминалистическом смысле.

В самой статье 159.3 УК РФ фактически представлен ряд оснований для классификации способов мошенничества с использованием платежных карт.

³⁶ Данный раздел работы основан на материалах статьи: Антонов И.О., Шалимов А.Н. Способы мошенничества с использованием платежных карт как элемент криминалистической характеристики данного вида преступлений // Ученые записки Казанского университета. Гуманитарные науки. Казань, 2013. Том 155. Книга 4. С. 196-203

³⁷ Ларичев В.Д. Криминалистическая характеристика экономических преступлений и методика её построения // Научный портал МВД России. 2009. № 1. С. 111.

³⁸ Волохова О.В. Расследование преступлений, связанных с обманом. М.: Юрлитинформ, 2008. С.33.

³⁹ Вехов В.Б. Особенности расследования преступлений, совершённых с использованием пластиковых карт и их реквизитов. Волгоград: ВА МВД России, 2005. 276 с.; Филиппов М.Н. Расследование краж и мошенничеств, совершённых с использованием банковских карт и их реквизитов: Автореф. дис. ... канд. юрид. наук. М., 2012. 30 с.; Федотов Н.Н. Форензика – компьютерная криминалистика. М.: Юрид. мир, 2007. 359 с.

Так, их можно классифицировать в зависимости от того, какая разновидность платежной карты была задействована мошенниками для совершения преступления. Соответственно, имеет смысл говорить о способах, в которых были использованы: а) кредитная карта; б) расчетная карта; в) иная платежная карта (УК РФ).

Другим основанием для классификации способов является характеристика лица, на которое были направлены обманные действия при совершении преступления. По данному основанию способы мошенничества с использованием платежных карт могут быть ранжированы на три категории:

- 1) криминальный обман уполномоченного работника кредитной организации;
- 2) криминальный обман уполномоченного работника торговой организации;
- 3) криминальный обман уполномоченного работника иной организации (ст. 159.3 УК РФ).

Криминалистическое значение имеет также разделение способов совершения мошенничества с использованием платежных карт в зависимости от количества лиц, участвующих в реализации умысла на хищение путем обмана. Соответственно, можно выделить криминальный обман, совершенный в одиночку либо в составе группы. Среди мошенничеств с использованием платежных карт особую опасность представляют преступления, совершенные организованными преступными группами.

Организованные преступные группы кардеров нередко совершают несколько эпизодов мошенничества. Так, в городе Ухта были задержаны участники преступной группы, состоящей из трех человек, занимавшихся мошенничеством с использованием поддельных платежных карт (23 эпизода хищений). Члены организованной преступной группы по фальшивой банковской карте приобрели на одной АЗС 900 л бензина на 22140 руб., а на другой – 3658 л дизельного топлива на 100960 руб. Эмитентами пластиковых карт, которые были задействованы при совершении преступления, являлись банки США, Испании, Франции и Швейцарии. Для совершения мошенничества преступники использовали специальное оборудование по изготовлению поддельных пластиковых карт⁴⁰. Несколько эпизодов мошенничества было на счету группы лиц, которая использовала похищенную у владельца банковскую карту для приобретения товаров в магазинах⁴¹.

Специалисты отмечают, что, как и другие киберпреступления, преступления с использованием платежных карт нередко совершаются членами разветвленных, хорошо организованных преступных групп, участники которых

⁴⁰ Попова Н. Российские банкоматы оказались в ливанской петле // АН-online. – 2012. – 11 фев. – URL: <http://argumenti.ru/crime/2012/02/156477>, свободный.

⁴¹ Приговор Верхнепышминского городского от 21 фев. 2012 г. по уголовному делу № 1-50/12 <http://docs.pravo.ru/document/view/22393765/>.

имеют свою преступную специализацию⁴². Криминальная специализация в группе может выглядеть следующим образом: одни члены группы осуществляют сбор информации по платежным картам, другие – обрабатывают собранную информацию и передают их тем, кто занимается изготовлением поддельных карт. Подготовленное таким образом хищение осуществляют лица, специализирующиеся на «вещевом» кардинге – именно они используют платежную карту для обмана работников торговой организации.

Уже очень давно хищения, совершаемые с использованием платежных карт, являются одной из составляющих транснациональной организованной киберпреступности. Показательным в этом отношении является задержание и последующая экстрадиция из Франции в США Владислава Хорохорина (известного также под ником BadB), имеющего гражданство Украины, Израиля и России. Его криминальная деятельность заключалась в продаже при помощи Интернета украденных данных о платежных картах, в том числе на форумах CarderPlanet и carder.su. Правоохранительные органы пришли к выводу, что Хорохорин является создателем криминальной схемы, которая позволила преступникам похитить более девяти миллионов долларов США. Помощник Генерального прокурора США Лэнни Брюер (Lanny A. Breuer) считает В.Хорохорина одним из наиболее известных во всем мире мошенников, занимающихся преступной деятельностью с использованием кредитных карт⁴³.

Еще одним основанием для классификации способов мошенничества с использованием платежных карт является технологическое решение, задействованное преступниками при совершении преступления. В статье 159.3 УК РФ указано два способа совершения такого мошенничества: с использованием поддельной (1) или принадлежащей другому лицу (2) платежной карты (УК РФ). Примером последнего является дело, в ходе расследования которого было установлено, что К., совершив тайное хищение имущества, завладел платежной картой потерпевшего и решил использовать ее для осуществления мошенничества. С целью реализации своего умысла К. неоднократно использовал похищенную платежную карту для приобретения различных товаров⁴⁴.

По данному основанию, кроме указанных выше способов, исследователи выделяют и другие разновидности криминального обмана в зависимости от того, используется ли для его реализации конфиденциальная информация о реквизитах подлинных карт и их держателях (3) или несовершенство аппаратно-программного обеспечения технологии обращения платежных карт (4)⁴⁵.

⁴² Козловский В. Масштабы кибермошенничества растут // Российская газета. 2012. 29 нояб. URL: <http://www.rg.ru/2012/11/29/karti-site.html>, свободный

⁴³ Франция избавилась от российского кибервора и отправила его в США // АН-online. 2012. 17 июня. URL: <http://argumenti.ru/crime/2012/06/184343>, свободный.

⁴⁴ Приговор Верхнепышминского городского от 7 июня 2011 г. по уголовному делу № 1-152/11 <http://docs.pravo.ru/document/view/18392970/>.

⁴⁵ Вехов В.Б. Особенности расследования преступлений, совершённых с использованием пластиковых карт и их реквизитов. Волгоград: ВА МВД России, 2005. с. 91–162

Следует отметить, что в рамках каждой из четырех указанных разновидностей через сравнительно небольшой промежуток времени появляются новые криминальные схемы. Мошенники учитывают изменения, происходящие в технологии защиты платежных карт, и совершенствуют свои преступные методики. Так, достаточно вспомнить, какие приемы они задействуют для получения конфиденциальной информации о реквизитах подлинных платежных карт и их держателях.

Наиболее распространенными схемами мошенничества с банковскими картами являются следующие: оглашение сведений о ПИН-коде самим держателем карты; дружественное мошенничество (использование в своих целях карты с предварительной осведомленностью о ПИН-коде членами семьи, близкими друзьями, коллегами по работе); подглядывание из-за плеча (мошенник вполне может узнать ПИН-код держателя банковской карты, подглядывая из-за его плеча, пока тот вводит код в банкомате; затем злоумышленник осуществляет кражу карты и использует ее в своих целях); «Ливанская петля» (мошенник использует техническое устройство, препятствующее извлечению карты из банкомата, затем он советует держателю карты обратиться в банк и пользуется его отсутствием для кражи карты); фальшивые банкоматы (мошенники разрабатывают и производят фальшивые банкоматы, либо переделывают старые; после введения карты и ПИН-кода обычно на дисплее фальшивого банкомата появляется надпись, что денег в банкомате нет или, что банкомат не исправен; во время использования банкомата информацию о счете данного лица и его персональный идентификационный номер копируются с магнитной полосы карты); ограбление держателей банковских карт.

Считывание секретной информации, хранящейся на карте, может производиться разными способами. Наиболее распространенный из них – сговор мошенников с сотрудниками магазинов, отелей, ресторанов, других торговых и развлекательных предприятий. Через такие компании проходит большое количество транзакций с пластиковыми картами, информация о которых сохраняется в компьютерных базах данных компании или на слипах (бумажных документах, подтверждающих факт осуществления платежа). Результатом такого сговора является передача информации о реквизитах карточек представителям криминальных структур. В этом случае происходит так называемый скиминг. Настоящую платежную карту пропускают через специальное устройство (скимер) и считывают данные, которые хранятся на ее магнитной полосе. Скиммеры (от англ. *skimming* – снятие сливок) – приборы, монтируемые на банкомат для несанкционированного считывания конфиденциальной информации непосредственно с карты; накладные клавиатуры, размещаемые на клавиатуре банкомата и используемые для копирования вводимых на настоящую клавиатуру данных; миниатюрные видеокамеры, установленные таким образом, что в их объектив попадает

информация, которая вводится в банкомат посредством клавишного набора⁴⁶.

Довольно распространен способ, когда криминальные структуры организуют свои собственные магазины. Цель существования подобных «торговых точек» проста – получить как можно больше данных о пластиковых картах клиентов. Часто мошенники используют для этого и Интернет- сайты. Воспользовавшись один раз услугами такого сайта (например, купил товар или скачал видеоролик), владелец карты с удивлением выясняет, что стал его подписчиком, и, таким образом, с него ежемесячно взимается плата за подписку, отказаться от которой довольно проблематично.

Новейшие технологии, взятые на вооружение преступниками, позволили им модернизировать устройства, используемые для скимминга. Речь идет о шимминге (англ. *shimming*) – использовании гибких, очень тонких плат, внедряемых преступниками в банкомат через щель приемника пластиковых карт. Плата при помощи специальной карты носителя присоединяется к контактам, считывающим данные с платежных карт. Толщина платы сопоставима с толщиной человеческого волоса (0.1 мм). Принципиальным отличием технологии шимминга от использования скимерских устройств является ее большая визуальная незаметность.

Помимо названных достаточно миниатюрных высокотехнологичных приспособлений, мошенники могут использовать и гораздо более громоздкие по размерам, но не менее технологичные устройства – фальшивые банкоматы. Методы социальной инженерии востребованы в процессе так называемого фишинга (англ. *phishing* – производное от *phone* и *fishing*), результатом которого нередко становится доступ преступников к важной конфиденциальной информации владельца платежной карты. Для выведывания используются различные приемы: отправка электронных сообщений, подделанных под официальные письма, совершение ложных телефонных звонков от имени банка и т. д. Сравнительно новым приемом сбора мошенниками конфиденциальной информации является так называемый вишинг (англ. *vishing* – *voice phishing*) – голосовой фишинг, реализуемый посредством мобильной телефонной связи.

Широкое общественное информирование о ставших известными способах выведывания мошенниками конфиденциальной информации снизило эффективность фишинговых атак, что привело к изобретению преступниками так называемого фарминга (англ. *pharming* – производное от *phishing* и *farming*). Этот вид интернет-мошенничества представляет собой процедуру скрытого перенаправления потенциальных жертв мошенничества на ложные IP-адреса в сети Интернет. Для фарминга может быть использован компьютер владельца платежной карты, на который незаметно для пользователя размещается специальная про-грамма («троян»). Фарминг может быть осуществлен и непосредственно на DNS сервере интернет-провайдера владельца карты. Для

⁴⁶ Антонов И.О., Шалимов А.Н. Способы мошенничества с использованием платежных карт как элемент криминалистической характеристики данного вида преступлений // Ученые записки Казанского университета. Гуманитарные науки. Казань, 2013. Том 155. Книга 4. С. 196-203

получения конфиденциальной информации мошенники делают все возможное, чтобы потенциальная жертва была в полной уверенности, что пользуется услугами банка. После того как владелец карты выполнит стандартную процедуру ввода платежных реквизитов, он перенаправляется на официальный сайт банка.

Самым распространенным мошенничеством по данным международной платёжной системы является мошенничество с утерянными картами. Ущерб от него составляет почти половину от всех случаев мошенничества с кредитными картами. Ведь, вовремя не заблокированная потерянная или украденная карта, может послужить преступнику отличным средством для оплаты по счету там, где не требуется ввода никаких паролей⁴⁷. С 1 января 2014 года вступила поправка в Федеральный закон от 27 июня 2011 г. № 161-ФЗ «О национальной платёжной системе». В частности, теперь гражданам предоставляется десять дней вместо ранее установленного одного дня для того, чтобы обнаружить пропажу денежных средств и обратиться с заявлением в банк. По вступившим поправкам в закон банки обязаны сообщать клиентам обо всех операциях, которые проводятся с их картами, теми средствами, которые указаны в договоре.

Мошенничества с использованием платежных карт, совершаемые перечисленными выше способами, нередко очень тесно связаны с предусмотренными уголовным законодательством РФ преступлениями в сфере компьютерной информации (ст. 272–274 УК РФ), мошенничеством в сфере компьютерной информации (ст. 159.6 УК РФ), а также изготовлением или сбытом поддельных кредитных или расчетных карт и иных платежных документов (ст. 187 УК РФ)⁴⁸.

Представленные классификации способов мошенничества с использованием платежных карт позволяют более точно оценить возможные корреляционные связи между элементами криминалистической характеристики этого рода мошенничества. Не подлежит сомнению, что среди закономерностей криминальной деятельности особенно большое значение должно уделяться изучению зависимости вида, способа и механизма преступного поведения от особенностей связи правонарушителя с предметом преступного посягательства, обстановкой, сложившейся в месте совершения преступления и вокруг него; следует также учитывать влияние на эту связь личностно-типологических свойств субъекта преступления, степени организованности, разветвленности и состава преступной группы (при наличии таковой) и др.⁴⁹

Исследование современных способов мошенничества с использованием платежных карт имеет конечной целью поддержание в актуальном работоспособном состоянии криминалистической характеристики данного вида мошенничества. Она является составной частью методики расследования

⁴⁷ Кривошапова С.В., Литвинов Е.А. Оценка и способы борьбы с мошенничеством с банковскими картами в России [Текст]/ Кривошапова С.В., Литвинов Е.А. // Международный журнал прикладных и фундаментальных исследований. 2015. № 4-1. С. 116-120.

⁴⁸ Там же.

⁴⁹ Криминалистика / Под ред. Н.П. Яблокова. М.: Норма: ИНФРА-М, 2010. С.546.

указанных преступлений и во многом предопределяет качество предварительного расследования. Результаты изучения способов совершения преступлений указанного вида также могут быть востребованы при разработке оптимального методического обеспечения механизма противодействия мошенническим посягательствам в национальной платежной системе.

2.3. Характеристика личности преступника, совершившего общественно опасные деяния в сфере проведения безналичных расчетов, производимых с использованием банковских карт⁵⁰

Криминологическая характеристика субъектов преступлений, совершаемых в сфере проведения безналичных расчетов, производимых с использованием банковских карт, основана на анализе социально-демографических признаков, социального статуса личности и ее нравственно-психологических свойств. Их использование позволило предложить следующую типологию личности преступника, совершившего преступление в сфере проведения безналичных расчетов, производимых с использованием банковских карт:

- лица, устойчиво ориентированные на совершение преступлений в сфере проведения безналичных расчетов, производимых с использованием банковских карт, готовые не только использовать, но и создавать необходимые обстановку и условия, убежденные в предпочтительности этого варианта поведения любому другому;

- лица, ориентированные на совершение преступлений в сфере проведения безналичных расчетов, производимых с использованием банковских карт и готовые для этого использовать сложившуюся обстановку и условия, но обычно не склонные к активным действиям по их созданию;

- лица, втянутые в совершение преступлений в сфере проведения безналичных расчетов, производимых с использованием банковских карт в силу неблагоприятной ситуации и в результате того, что попали в среду активных носителей антиобщественных взглядов.

Проведенные исследования показали, что личность преступника, совершающего преступления в этой сфере отличается рядом характерных особенностей. Данные уголовной статистики и материалов уголовных дел свидетельствуют о том, что среди преступников достаточно высок удельный вес мужчин – около 78%. Доля женщин среди лиц, совершивших хищения и мошенничества с банковскими картами значительно ниже и составляет всего около 22%, и в отличие от обычного мошенничества (где они выполняют роли организаторов и непосредственных исполнителей) их роль чаще всего сводится

⁵⁰ При написании данного раздела использованы материалы статьи: Васюков С.В. Криминологическая характеристика личности преступника, совершающего общественно опасные деяния в сфере проведения безналичных расчетов с использованием банковских карт // Ученые записки Орловского государственного университета. Серия гуманитарные и социальные науки. 2012. № 5 (49). С. 439-445.

к оказанию содействия при совершении преступлений (например, помощи в обналичивании денежных средств). Вместе с тем указанный показатель значительно выше среднестатистического показателя удельного веса преступниц женского пола в целом, который в последние годы колеблется от 12 до 15%⁵¹

В структуре лиц, совершивших экономические преступления, в сфере проведения безналичных расчетов, производимых с использованием банковских карт, достаточно высок удельный вес иностранных граждан (около 20%), представленных гражданами стран ближнего и дальнего зарубежья (КНР, КНДР и др.). Среди всех иностранцев, совершивших преступления с помощью банковских карт, удельный вес последних составил не более 15%⁵².

Наиболее криминогенной возрастной категорией являются лица 26-39 лет: их доля в структуре преступности доходит до 54%, далее следует возрастная группа осужденных за данное деяние: 39-50 (около 26%), от 18 до 26 лет (около 18%), 50 и старше (2%). Преобладание в структуре организованного мошенничества более зрелого контингента преступников обуславливается наличием жизненного опыта, свидетельствующего о способности лица максимально использовать свои физические и интеллектуальные возможности для обеспечения результативности и скрытности осуществления преступной деятельности. Весьма неблагоприятные прогнозы олицетворяет собой группа лиц в возрасте до 29 лет. Практически это молодые, но уже вполне профессиональные преступники, связавшие повышение уровня своего материального благосостояния, да и положение в обществе в целом, с криминалом⁵³.

Изучаемый вид преступного поведения требует наличие определенного уровня знаний, умений и навыков в области информационных технологий, а также способности оказать психологическое воздействие. Изучение статистических и фактологических данных, характеризующих субъектный состав осужденных за мошеннические действия по уровню образования, показывает, что он не изменяется в последние годы. Анализ материалов уголовных дел показало, что около 34% мошенников имели среднее общее образование, 25% – среднее специальное, 27% – высшее и неоконченное высшее, 14 % – неполное среднее. При этом отдельные лица (около 2%) имели по два высших образования⁵⁴.

⁵¹ Так, по итогам 2011 года удельный вес женщин в структуре лиц, совершивших преступления составил 15,3%. См. Состояние преступности в России за 2011 год. Сборник ГИАЦ МВД России. М., 2012. С. 35.

⁵² Васюков С.В. Автореферат диссертации на соискание ученой степени кандидата юридических наук на тему: «Предупреждение преступлений, совершаемых в сфере проведения безналичных расчетов, проводимых с использованием банковских карт». Специальность 12.00.08 - Уголовное право и криминология; уголовно-исполнительное право. М., 2013. С. 20-23.

⁵³ Там же.

⁵⁴ Там же.

Анализ субъектного состава осужденных за совершение преступлений, предусмотренных ст. 159 УК РФ по роду профессиональной деятельности показал, что среди них: трудоспособные без определенных занятий составляют 49,3%, государственные и муниципальные служащие - 3,7 %, служащие коммерческих или иных организаций - 10,3%, частные предприниматели - 2,5%, учащиеся и студенты - 2,9%, рабочие (21,8%), лица прочих занятий - 9,5%⁵⁵.

Анализ материалов судебно-следственной практики показывает, что 45% мошенников, совершивших уголовно наказуемые деяния в составе организованной группы или преступного сообщества, в браке не состояли. В законных отношениях находились 55% участников мошеннических организованных структур, из них представители мужского пола составили 75%⁵⁶.

Изучение абсолютных показателей лиц, совершивших организованные мошенничества, позволяет сделать вывод о том, что уровень ранее судимых лиц, совершивших мошенническое посягательство, изменяется практически пропорционально числу привлеченных к ответственности за данное уголовно наказуемое деяние. В среднем каждый пятый (около 20%), привлеченный к ответственности за мошенничество ранее был судимым, из них подавляющее большинство были осуждены условно. При этом большинство мошенников (около 85%) процентов осужденных были подвержены определенному «своему» способу совершения⁵⁷.

2.4. Способы противодействия мошенничеству, связанному с использованием электронных платежных пластиковых карт

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)⁵⁸ 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

⁵⁵ Там же.

⁵⁶ Там же.

⁵⁷ Там же.

⁵⁸ Справочно: адрес в сети Интернет: www.tk122.ru 13

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 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.

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.

Для эффективного предотвращения мошеннических операций необходимо учитывать российскую специфику:

- низкая техническая подготовка клиента, граничащую с технической и финансовой безграмотностью;
- правовой нигилизм и халатность клиентов.

По имеющимся оценкам, из общего числа фактов, мошенничество в сфере электронных платежей возможно из-за потери данных. Утечка информации из финансово-кредитной сферы происходит с помощью подкупа, шантажа, переманивания служащих в 43 % случаях, копирования программного продукта – 24 %, проникновения в компьютер – 18 %, кражи документации – 10 %, подслушивания телефонных переговоров – 5 %⁵⁹.

Сегодня до 80 % обращений через интернет-сайт МВД РФ посвящены мошенничеству при покупке товаров через социальные сети и интернет-магазины. Также продолжает расти разнообразие вредоносных программ для мобильных устройств.

Целью злоумышленников может быть получение доступа к мобильному банку жертвы и к конфиденциальным сведениям.

В 2014 г. зафиксировало увеличение числа программ, используемых для реализации мошеннических схем. Они имеют широкий функционал – от получения данных банковских карт до снятия наличных денег и несанкционированного проникновения во внутреннюю сеть банка. Не теряет популярность и «классический» скимминг. Обобщенные данные в области разработки безопасных приложений и оценки уязвимостей показывают следующую статистику:

1. В 2015 году злоумышленник оказался способен получить доступ к узлам внутренней сети субъекта национальной платежной системы в 9 случаях из 10, а в 2012 году аналогичное соотношение составляло 7 из 10;

⁵⁹ Выборнов А. Устранение уязвимостей // BIS journal. 2014. № 4.

2. Для проведения атаки в 82 % случаев достаточно иметь среднюю или низкую квалификацию;

3. Факторы уязвимости web-приложений обнаружены в 93 % исследованных систем;

4. Причинами возникновения уязвимостей в АБС являются ошибки (недостатки) разработки (23 %) и отсутствие эффективных защитных механизмов (43 %);

5. Уязвимости приложений – один из распространенных факторов, способствующих проникновению в корпоративные сети⁶⁰.

Рассмотрим основные приемы мошеннических действий, следующие из российской специфики. Самый распространенный способ – халатность и правовой нигилизм клиентов, которые разглашают PIN-код путем его записи на карту или путем так называемого «дружественного мошенничества» – разглашения PIN-кода членам семьи, близким друзьям, коллегам.

Еще пример – когда из-за фактора технической неграмотности клиенты впадают в панику при получении SMS-сообщения «Ваша банковская карта заблокирована» со всеми вытекающими для них последствиями.

Также распространенной схемой является помощь прохожего, называемая «ливанской петлей». Суть в том, что при блокировке карты банкоматом на помощь клиенту приходит «добрый» мошенник, изображая опытного пользователя банкоматов⁶¹. Но несмотря на такое разнообразие мошеннических схем, большая часть краж обусловлена человеческим фактором.

Согласно статистике, на 10 инцидентов в области информационной безопасности только 1 приходится на внешнего «хакера», еще 1 – на озлобленного, обиженного сотрудника и остальные 8 – на нерадивых, безответственных и плохо обученных сотрудников предприятия.

Эффективность обеспечения безопасности по отношению к пластиковым платежным средствам может быть повышена путем технологических и организационных методов.

К первым относятся совершенствование выпуска карт и повышение уровня безопасности использования банкоматов.

В России банкоматы широко используются для снятия наличных денег, а также в качестве платежных терминалов, в отличие от европейских стран.

Учитывая это, банкам необходимо прилагать наибольшие усилия в противодействии использованию мошенниками банкоматов в качестве технических средств получения/ дублирования секретной информации (ее носителя).

Банкам следует совершенствовать механизмы защиты банкоматов:

- периодически изменять настройки,
- увеличивать количество штатных видеокамер,

⁶⁰ Выборнов А. Устранение уязвимостей // BIS journal. 2014. № 4.

⁶¹ Смольянинова Е.Н., Фурманов Д.В. Проблемы безопасности расчетов при использовании пластиковых карт // Актуальные вопросы экономических наук. – 2012. – С. 46–50.

- устанавливать банкоматы исключительно в людных общественных местах и крупных учреждениях.

Также можно вводить ограничения на суммы, снимаемые в банкомате клиентами по зарплатным проектам, в зависимости от месторасположения банкомата.

Если говорить о совершенствовании информационных систем, можно выделить следующие требования:

1. Построение модели и ее параметров для выявления подозрительных операций. Принятие решение об отклонении операции и занесении карты в стоп-лист.

2. Возможность управления (блокировка) подозрительными точками обслуживания (банкоматы, терминалы, точки продаж, торговцы).

3. Статистический анализ истории операций. Выявление карт, которые были обслужены в подозрительных точках.

4. Оповещение операторов системы о фактах мошенничества для принятия соответствующих мер (SMS и E-mail информирование, генерация оповещений)⁶².

Банки активно развивают свои системы безопасности. С технической точки зрения они имеют достаточно возможностей для построения надежной системы информационной защиты.

Однако применение технических устройств не исключает присутствия индивидов. В этой связи наибольший удельный вес мошенничества в дистанционном банковском обслуживании (ДБО) приходится на социальный инжиниринг, т.е. мошеннические схемы, в основе которых лежит невнимательность и доверчивость клиента, его неосведомленность, пренебрежение правилами безопасной работы в интернете. Именно поэтому донесение до клиента необходимой информации и приучение его к соблюдению этих правил не менее важно, чем совершенствование и внедрение новых технологий обеспечения безопасности в ДБО. Данная проблема более актуальна, чем нехватка на рынке IT-решений. Не менее насущная проблема – недостаток законодательной базы в части борьбы с мошенничеством – недостаток в актах, регулирующих ответственность за мошеннические действия, формирование доказательной базы.

Отметим наиболее существенные проблемы предупреждения мошенничества, совершаемого с использованием пластиковых карт:

– умалчивание коммерческими структурами информации о совершении мошенничества в целях сохранения престижа и видимости его благополучности перед клиентами;

– отсутствие слаженной кооперации и взаимодействия служб безопасности банков и правоохранительных органов (МВД, ФСБ, СК, прокуратуры), их недостаточная активность⁶³. Важно отметить эффективность организационных

⁶² Смольянинова Е.Н., Фурманов Д.В. Проблемы безопасности расчетов при использовании пластиковых карт //Актуальные вопросы экономических наук. 2012. С. 46–50.

⁶³ Эволюция карточного мошенничества в Европе 2013. [Электронный ресурс]. URL: <http://www.fico.com/landing/fraudeurope2013>

методов защиты, о которых забывают в погоне за техническими средствами.

Необходимо организовать грамотное реагирование на сообщения держателей карт о неправомерных списаниях денежных средств, вести правильный учет и анализ этих сообщений.

Важной задачей является определение оптимальных параметров системы, позволяющих минимизировать риск банка – опыт и интуиция оператора может работать эффективней компьютерной системы и сотрудника службы безопасности. Для повышения эффективности защитных механизмов следует проводить работу и с владельцами карт, ведь их внимательность – главный способ избежать мошенничества.

В заключение можно отметить, что качество обеспечения безопасности банковской системы зависит от уровня «честности» участников финансовых отношений, эффективности работы службы безопасности кредитных организаций, профессионализма сотрудников правоохранительных органов, занимающихся предупреждением и выявлением мошенничества в банковской сфере, а также объема разъяснительной работы, проводимой с держателями легитимных пластиковых карт. Перед банком и клиентом стоят общие цели, они решают одни и те же задачи. Развитие информационных технологий требует развития взаимодействия и совершенствования системы банк – клиент – банк.

Итак, противодействие мошенничеству с использованием пластиковых карт - это реализация системы противодействия как внешнему, так и внутреннему мошенничеству, так называемые решения антифрод, работающие в реальном времени. Другими словами, это комплекс организационных и технических мер, обеспечивающих дополнительную защиту автоматизированных банковских систем и систем дистанционного банковского обслуживания. Такие системы содержат наборы правил, позволяющие с высокой долей вероятности обнаружить транзакции, сформированные мошенниками. Это, например, «черные» и «белые» списки. В «черные» списки попадают те получатели платежей, которые уже были уличены в участии в мошеннических схемах, в «белые» – те, которым клиент платил и не обжаловал этот платеж⁶⁴. Возможно также создание профиля пользователя, учитывающего различные параметры выполняемых операций: запрашиваемую сумму, дату и время, географию – и определяющего уровень риск для каждой транзакции по этому профилю. Транзакции с высоким уровнем рисков можно запрещать или ограничивать по сумме, или требовать дополнительной авторизация для выполнения операции⁶⁵.

⁶⁴Корякин В.М., Саенко А.Ю. Некоторые вопросы безопасности использования банковских карт [Текст]// Право в вооруженных силах. № 2. 2012. С. 75.

⁶⁵ Мокрушина А.Л., Рустамова Э.О. Интернет-банкинг - новая форма старых услуг: понятие, безопасность, перспективы развития системы // Проблемы и перспективы развития современного законодательства: сборник материалов межкафедральной научно-практической конференции юридического факультета Российской таможенной академии. М.: Изд-во Рос. тамож. акад., 2013. С.63-66.

В комплексе с программно-аппаратными средствами противодействия компания «АСТ» применяет методику оценки защищенности системы ДБО. «АСТ» как аудитор систем ДБО осуществляет следующие виды технологических аудитов:

- аудит внешнего периметра – проверки правил фильтрации, типовых конфигураций сервисов, тестирование на известные удаленные уязвимости в ОС и сервисах;

- аудит архитектуры системы – проверки парольной политики, ролей пользователей, правил логики системы;

- аудит защищенности web-приложений – поиск известных и новых уязвимостей в приложениях,

 - проверки на наличие скрытых скриптов и шифрования web-соединений;

- аудит защищенности на уровне СУБД – контроль парольной политики СУБД, проверки на уязвимости и ошибки конфигурации, шифрование критичных данных и др.;

- аудит защищенности клиентской части системы – поиск уязвимостей, анализ работы клиента с криптографией, проверка настроек и конфигураций клиентского ПО, системы хранения паролей на клиентской части и др.

По результатам проведенных проверок и выявленных уязвимостей определяются возможные векторы атак как на клиентов системы, так и на серверы ДБО.

Снижение рисков мошенничества в системах дистанционного банковского обслуживания (ДБО) за счет дополнительного анализа типового поведения клиентов, анализа аномального поведения и введение дополнительных проверок позволяют снизить прямые финансовые потери банков, связанные с мошенничеством. Повысить репутацию и уровень доверия к банку в глазах клиентов, инвесторов и партнеров.

ЗАКЛЮЧЕНИЕ

Одним из важнейших компонентов экономической безопасности страны является безопасность финансовой системы. Без устойчивого функционирования финансовой системы и финансового рынка страны невозможно наращивание экономического и научно-технического потенциала России, который призван обеспечить достойное место страны в мире.

Банковская сфера, являющаяся ключевой частью инфраструктуры, необходимой для нормального функционирования экономики, принимает на себя часть рисков от глобализации экономики и увеличения иностранно капитала в России, поэтому обеспечение экономической безопасности банковской системы страны становится стратегической задачей для государства. Без решения данной задачи обеспечивать поступательное развитие страны, укреплять ее безопасность невозможно.

Преступления в банковской сфере условно можно разделить на две группы:

- насильственные преступления (убийства, налеты, грабежи и т.д.);
- так называемые «беловоротничковые» преступления, к которым относятся всевозможные финансовые хищения и махинации.

Совершаемые в банковской сфере криминальные посягательства отличаются как особой изощренностью, многоплановостью, так и активной адаптацией преступности к новым формам и методам банковской деятельности и совершаются, как правило, организованными группами.

В настоящее время структура и динамика банковских преступлений претерпела серьезные изменения, они стали более организованными и профессиональными, повысился их интеллектуальный уровень. Преступники взяли на вооружение методы информационного обеспечения своей криминальной деятельности, все чаще используют современную технику и технологии, паразитируют на издержках и трудностях экономических реформ.

Основной целью организованных преступных группировок, внедряющихся в банковские структуры, является легализация незаконного капитала, проведение операций с преступными доходами, а также совершение мошенничества в отношении средств кредитных организаций.

Безусловно, с развитием высоких технологий традиционные формы преступных посягательств приобрели новый характер. В частности, говоря о банковских картах, целью преступников стало завладение указанными инструментами (либо связанной с ними идентифицирующей информацией) для того, чтобы иметь возможность распоряжаться средствами на карточных счетах. Такие хищения осуществляются не непосредственно у держателя карты, а с его банковских счетов, что зачастую предполагает использование преступником схем. Применительно к рассматриваемой категории преступлений предлагаются следующие способы совершения хищений:

- Использование найденной или украденной карточки для оплаты товаров и услуг или/ и получения наличных денег из банкоматов,
- Подделка самой пластиковой карты или ее оттисков,

- Получение незаконным путем оттисков настоящей пластиковой карты,
- Мошенничество с картами, не полученными законным держателем,
- Получение преступниками настоящих пластиковых карт путем оформления заявок на подставных лиц,
- Использование слабых мест технологии обработки платежей, совершенных с помощью «пластиковых» денег,
- Мошенничества, совершаемые законными держателями пластиковых карт».

Для эффективного предотвращения мошеннических операций необходимо учитывать российскую специфику:

- низкая техническая подготовка клиента, граничащую с технической и финансовой безграмотностью;
- правовой нигилизм и халатность клиентов.

В России банкоматы широко используются для снятия наличных денег, а также в качестве платежных терминалов, в отличие от европейских стран.

Учитывая это, банкам необходимо прилагать наибольшие усилия в противодействии использованию мошенниками банкоматов в качестве технических средств получения/ дублирования секретной информации (ее носителя).

Банкам следует совершенствовать механизмы защиты банкоматов:

- периодически изменять настройки,
- увеличивать количество штатных видеокамер,
- устанавливать банкоматы исключительно в людных общественных местах и крупных учреждениях.

Также можно вводить ограничения на суммы, снимаемые в банкомате клиентами по зарплатным проектам, в зависимости от месторасположения банкомата.

Если говорить о совершенствовании информационных систем, можно выделить следующие требования:

1. Построение модели и ее параметров для выявления подозрительных операций. Принятие решение об отклонении операции и занесении карты в стоп-лист.
2. Возможность управления (блокировка) подозрительными точками обслуживания (банкоматы, терминалы, точки продаж, торговцы).
3. Статистический анализ истории операций. Выявление карт, которые были обслужены в подозрительных точках.
4. Оповещение операторов системы о фактах мошенничества для принятия соответствующих мер (SMS и E-mail информирование, генерация оповещений)⁶⁶.

Итак, противодействие мошенничеству с использованием пластиковых карт - это реализация системы противодействия как внешнему, так и внутреннему мошенничеству, так называемые решения антифрод, работающие в

⁶⁶ Смольянинова Е.Н., Фурманов Д.В. Проблемы безопасности расчетов при использовании пластиковых карт //Актуальные вопросы экономических наук. 2012. С. 46–50.

реальном времени. Другими словами, это комплекс организационных и технических мер, обеспечивающих дополнительную защиту автоматизированных банковских систем и систем дистанционного банковского обслуживания.

Снижение рисков мошенничества в системах ДБО за счет дополнительного анализа типового поведения клиентов, анализа аномального поведения и введение дополнительных проверок позволяют снизить прямые финансовые потери банков, связанные с мошенничеством. Повысить репутацию и уровень доверия к банку в глазах клиентов, инвесторов и партнеров.

Таким образом, норма о мошенничестве с использованием платежных карт (ст. 1593 УК РФ) призвана обеспечивать помимо охраны собственности также и нормальную деятельность банков и иных кредитных организаций, связанную с беспрепятственным доступом клиентов к своим денежным средствам в необходимый момент. В результате завладения платежной картой субъект преступления стремится получить доступ к денежным средствам на счете, к которому привязана данная карта. Объективная сторона преступления заключается в обмане, в результате которого уполномоченный работник кредитной, торговой или иной организации (например, официант в ресторане), будучи введенным в заблуждение ²⁰³ относительно того факта, что перед ним находится держатель карты, принимает предоставленную платежную карту в качестве средства платежа. С другой точки зрения, между ст. 1591 и ст. 1593 УК РФ существует конкуренция. Денежные средства при оформлении заявления на получение кредитной карты предоставляются в определенных объемах и на определенный срок, при условии возвратности, то в соответствии со ст. 1591 УК РФ это предполагало бы оконченное преступление. Единственное, что их различает, - это средство преступления, в соответствии с которым при мошенничестве с использованием платежной карты выступает кредитная карта. Определенные вопросы возникают с однозначным отнесением настоящего деяния к видам мошенничества. В соответствии с п.1 постановления Пленума Верховного Суда РФ от 27.12.2007 № 51 особенность мошенничества как формы хищения предполагает, что в результате обмана или злоупотребления доверием владелец имущества или иное лицо либо уполномоченный орган власти добровольно передают имущество или право на него. В описанной ситуации добровольно имущество никто не передают. Как уже было отмечено, платежная карта, выступает орудием преступления, с помощью которого субъект мошенничества пытается получить доступ к денежным средствам. Когда происходит обман представителя торговой организации (официанта), никто не удостоверяет, является ли данное лицо правомочным держателем карты или нет. Списание денежных средств происходит до того момента, как владелец карты ставит свою подпись на чеке.

Таким образом, предпосылками мошенничества в сфере дистанционных платежей выступают:

1. Отсутствие необходимости личного присутствия владельца средств для осуществления платежа или передачи денег другому лицу.

2. Использование технических средств для осуществления платежных операций в автоматическом режиме.

3. Движение денежных средств на основе единых принципов и правил коммуникации и платежей.

4. Пробелы и неточности в правилах платежных систем, недочеты в законодательстве о платежах и услугах связи.

5. Отсутствие единой системы мониторинга мошеннических транзакций и противодействия хищениям электронных денег.

Мошеннические группы характеризуются следующими признаками:

1. Несколько участников группы имеют высшее образование и обладают навыками в области ИТ.

2. Для хищения используются компьютеры, мобильные телефоны, современные средства коммуникации.

3. Организация строится по распределенному принципу, в связи с чем практически невозможно вычислить всех участников группы.

4. Задания передаются через анонимные сетевые сервисы или по СМС, деньги переводятся на карты преступников через цепочку посредников.

5. Как правило, преступление совершается в несколько этапов, реализация которых зачастую осуществляется участниками группы в различных странах.

6. Существует значительное число каналов незаконной торговли похищенной финансовой информацией и обмена сведениями о действиях служб безопасности банков и правоохранительных органов.

К мероприятиям, направленным на предупреждение и пресечение мошенничества, относятся:

1. Совершенствование законодательной базы электронного денежного оборота, в том числе усиление ответственности за преступления в области высоких технологий.

2. Формирование единых правил для всех операторов электронных денежных средств, установление ответственности за бездействие при мошенничестве с использованием оборудования или программного обеспечения оператора.

3. Укрепление взаимодействия между службами мониторинга и предотвращения мошенничества участников рынка.

4. Укрепление технологической базы служб фрод-мониторинга участников рынка.

5. Развитие взаимодействия между банками и правоохранительными органами в деле пресечения и предотвращения преступлений в области высоких технологий

6. Повышение грамотности населения в части безопасного поведения при использовании электронных денежных средств.

7. Создание в России федеральной системы мониторинга в области электронного денежного оборота.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

Нормативные акты и судебные решения

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 N 6-ФКЗ, от 30.12.2008 N 7-ФКЗ, от 05.02.2014 N 2-ФКЗ, от 21.07.2014 N 11-ФКЗ) // Собрание законодательства РФ. 2014. N 31. Ст. 4398.
2. О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации: Федеральный закон Российской Федерации от 29 нояб. 2012 г. № 207-ФЗ // Рос. газ. 2012. 3 дек. № 5951.
3. УК РФ – Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ. – URL: <http://www.consultant.ru/popular/ukrf/>, свободный.
4. О банках и банковской деятельности: Федеральный закон от 2 декабря 1990 г. N 395-I [Текст]// Ведомости съезда народных депутатов РСФСР от 6 декабря 1990 г. N 27 Ст. 357
5. О Центральном банке Российской Федерации (Банке России): Федеральный закон от 10 июля 2002 г. N 86-ФЗ [Текст]// Собрание законодательства Российской Федерации. 2002. N 28. Ст. 2790.
6. О страховании вкладов физических лиц в банках Российской Федерации: Федеральный закон от 23 декабря 2003 г. N 177-ФЗ [Текст]// Собрание законодательства Российской Федерации. 2003. N 52 (часть I). Ст. 5029.
7. О национальной платежной системе: Федеральный закон от 27.06.2011 N 161-ФЗ (действующая редакция, 2016) [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_115625/ (дата обращения: 27.10.2016).
8. О безопасности: Федеральный закон от 28.12.2010 N 390-ФЗ (действующая редакция, 2016) [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_108546/ (дата обращения: 27.10.2016).
9. О полиции: Федеральный закон от 07.02.2011 N 3-ФЗ (действующая редакция, 2016) [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_110165/ (дата обращения: 27.10.2016).
10. Доктрина информационной безопасности Российской Федерации Утверждена Президентом Российской Федерации 9 сентября 2000 г. № Пр – 1895.
11. Положение ЦБ РФ от 16.12.2003 г. № 242-П «Порядок обеспечения и защиты банковской информации» (с изменениями и дополнениями). [Электронный ресурс]. URL: <http://base.garant.ru/584330/> (дата обращения: 27.10.2016).
12. Положение Банка России от 9 июня 2012 года № 382-П “О требованиях к обеспечению защиты информации при осуществлении переводов

денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств” в редакции Указания Банка России от 5 июня 2013 года № 3007-У.

13. обработке в информационных системах персональных данных”.

14. Положение об эмиссии платежных карт и об операциях, совершаемых с их использованием (утв. Банком России 24.12.2004 № 266-П) (ред. от 14.01.2015) (Зарегистрировано в Минюсте России 25.03.2005 № 6431) // Вестник Банка России. № 17. 30.03.2005.

15. Стандарт Банка России СТО БР ИББС -1.0 – 2010 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения».

16. Заявление Правительства РФ и ЦБР от 5 апреля 2011 г. NN 1472п-П13, 01-001/1280 "О Стратегии развития банковского сектора Российской Федерации на период до 2015 года" [Электронный ресурс]. URL: <http://base.garant.ru/591345/#ixzz3uNoqGaTJ>

17. Постановление Пленума Верховного Суда РФ от 27.12.2002 № 29 (ред. от 03.03.2015) «О судебной практике по делам о краже, грабеже и разбое» // Российская газета. № 9. 18.01.2003).

18. Приговор Ленинского районного суда г. Новосибирска от 05.05.2015. Дело № 1-420/2015 // <http://sudact.ru/regular/doc/n1gmRVegiglgl/>

19. Приговор Кировского районного суда г. Кемерово, кемеровской области от 12.11.2015. Дело № 1-395/15 // <http://sudact.ru/regular/doc/Y1E4KZB0MKoV/>

20. Приговор Верхнепышминского городского суда (Свердловская область) от 7 июня 2011 г. по уголовному делу № 1-152/11//СПС Право.ru.– URL:<http://docs.pravo.ru/document/view/18392970/>.

21. Приговор Верхнепышминского городского суда (Свердловская область) от 21 февр. 2012 г. по уголовному делу № 1-50/12 //СПС Право.ru.– URL: <http://docs.pravo.ru/document/view/22393765/>.

Специальная литература

22. Акимов В.Е. Методика расследования преступлений, связанных с хищением денеж-ных средств, совершенных с использованием банковских пластиковых карт: Авто-реф. дис. ... канд. юрид. наук. – М., 2008. – 20 с.

23. Алексанов А.К., Демчев И.А., Доронин А.М. и др. Безопасность карточного бизнеса: бизнес-энциклопедия. – М.: Моск. фин.-пром. акад.: ЦИПСИР, 2012. – 432 с.

24. Антонов И.О., Шалимов А.Н. Способы мошенничества с использованием платежных карт как элемент криминалистической характеристики данного вида преступлений // Ученые записки Казанского университета. Гуманитарные науки. Казань, 2013. Том 155. Книга 4. С. 196-203

25. Архипов А., Городецкий А., Михайлов Б. Экономическая безопасность: оценки проблемы, способы обеспечения// Вопросы экономики.

2014. № 12. Безопасность банковских карт: взгляд потребителя и активность игроков рынка. Отчет по результатам исследования. М.: Национального агентства финансовых исследований, 2016. [Электронный ресурс] URL: http://nacfin.ru/wpcontent/uploads/2015/01/moshennichestvo_bankovskie_karty.pdf. Проверено на 30.10.2016.

26. Боровых Л.В., Корепанова Е.А. Проблема квалификации хищения с использованием банковских карт // Российский юридический журнал. 2014. № 2. Бочаров О.А. Формирование основ экономической безопасности банковской деятельности: Автореф. канд экон. наук. М., 2013.

27. Васюков С.В. Криминологическая характеристика личности преступника, совершающего общественно опасные деяния в сфере проведения безналичных расчетов с использованием банковских карт // Ученые записки Орловского государственного университета. Серия гуманитарные и социальные науки. 2012. № 5 (49). С. 439-445.

28. Васюков С.В. Автореферат диссертации на соискание ученой степени кандидата юридических наук на тему: Предупреждение преступлений, совершаемых в сфере проведения безналичных расчетов, проводимых с использованием банковских карт. Специальность 12.00.08 - Уголовное право и криминология; уголовно-исполнительное право. М., 2013. С. 20-23.

29. Вехов В.Б. Особенности расследования преступлений, совершенных с использованием пластиковых карт и их реквизитов. Волгоград: ВА МВД России, 2005. 276 с.;

30. Волохова О.В. Расследование преступлений, связанных с обманом. М.: Юрлитинформ, 2008.

31. Выборнов А. Устранение уязвимостей // BIS journal. 2014. № 4.

32. Горова Н. Туз в кошельке // Коммерсантъ. Юг России. Ростов-на-Дону. 2013. 30 апр. URL: <http://kommersant.ru/doc/2179379?isSearch=True>, свободный.

33. Джеймс Л. Фишинг: Техника компьютерных преступлений / Пер. с англ. Р.В. Гадицкого. М.: НТ Пресс, 2008. 314 с.

34. Добрынин Ю. Классификация преступлений, совершаемых в сфере компьютерной информации [Электронный ресурс]. URL: http://www.russianlaw.net/law/computer_crime/a158/ (Проверено 04.11.2016).

35. Евстратов А.В., Бережнова А.И. Развитие рынка электронных платежных систем и его роль в экономике Российской Федерации // Известия Волгоградского государственного технического университета. 2013. № 11 (144). С. 74-79.

36. Заячковский О.А., Эльзесер В.В. Способы совершения мошенничества с использованием банковских пластиковых карт // Сб. ст. аспирантов, соискателей и молодых ученых юрид. фак. КГУ. Калининград: КГУ, 2005. С. 57-62.

37. Звезда И.И. Расследование хищений в банковской сфере, совершенных путем мошенничества: Автореф. дис. ... канд. юрид. наук. М., 2008. 22 с.

38. Киселев А. Кражи с пластиковых карт часто происходят с участием сотрудников банков // Коммерсантъ FM. 2013. 23 мая. URL: <http://kommersant.ru/doc/2195462?isSearch=True>, свободный.
39. Козловский В. Масштабы кибермошенничества растут // Российская газета. 2012. 29 нояб. URL: <http://www.rg.ru/2012/11/29/karti-site.html>, свободный
40. Компьютерное мошенничество. Битва байтов / Под ред. Дж. Т. Уэллса; Пер. с англ. С.А. Филина. – М.: Маросейка, 2010. – 354 с.
41. Корякин В.М., Саенко А.Ю. Некоторые вопросы безопасности использования банковских карт [Текст]// Право в вооруженных силах. № 2. 2012.
42. Кривошапова С.В., Литвинов Е.А. Оценка и способы борьбы с мошенничеством с банковскими картами в России // Международный журнал прикладных и фундаментальных исследований. 2015. № 4-1. С. 116-120.
43. Криминалистика / Под ред. Н.П. Яблокова. – М.: Норма: ИНФРА-М, 2010. – 751 с.
44. Ларичев В.Д. Криминалистическая характеристика экономических преступлений и методика ее построения // Научный портал МВД России. 2009. № 1.
45. Малов А. Исповедь кардера. М.: ЦИПСИР: Альпина Паблишерз, 2010. 198 с.
46. Мещеряков В.А. Преступления в сфере компьютерной информации: основы теории и практики расследования. Воронеж: Изд-во Ворон. гос. ун-та, 2002. 408 с.
47. Мишина И.М. Расследование мошенничества, совершенного с использованием банковских карт: криминалистические и уголовно-процессуальные аспекты: Автореф. дис. ... канд. юрид. наук. М., 2009. 26 с.
48. Мокрушина А.Л., Рустамова Э.О. Интернет-банкинг - новая форма старых услуг: понятие, безопасность, перспективы развития системы // Проблемы и перспективы развития современного законодательства: сборник материалов межкафедральной научно-практической конференции юридического факультета Российской таможенной академии. М.: Изд-во Рос. тамож. акад., 2013. С.63-66.
49. Национальная система платежных карт Российской Федерации [Электронный ресурс]. URL: <http://www.nspk.ru/> (дата обращения: 27.10.2016).
50. Отчет о платежных системах за 2014 год Банка международных расчетов [Электронный ресурс]. URL: <https://www.bis.org/cpmi/publ/dl42a.pdf> (дата обращения: 27.01.2016).
51. Официальный сайт Центрального Банка Российской Федерации [Электронный ресурс] URL: <https://www.cbr.ru/>. Проверено на 30.10.2016.
52. Попова Н. Российские банкоматы оказались в ливанской петле // АН-online. 2012. 11 фев. – URL: <http://argumenti.ru/crime/2012/02/156477>, свободный.
53. Россинская Е.Р. Криминалистика. М.: НОРМА: ИНФРА-М, 2012. 464 с.

54. Россия в глобализирующемся мире: Стратегия конкурентоспособности / Российская академия наук, отделение общественных наук, секция экономики; акад. Д.С. Львов [и др.]. М.: Наука, 2014.
55. Смольянинова Е.Н., Фурманов Д.В. Проблемы безопасности расчетов при использовании пластиковых карт //Актуальные вопросы экономических наук. 2012. С. 46–50.
56. Состояние преступности в России за 2011 год. Сборник ГИАЦ МВД России. М., 2012.
57. Теряева А.С., Журавлева Т. А., Харитонюк Е. С. Национальная платежная система России: предпосылки возникновения и текущее состояние// Дискуссия. Выпуск №2 (65) февраль 2016.
58. Федотов Н.Н. Форензика – компьютерная криминалистика. М.: Юрид. мир, 2007. 359 с.
59. Филиппов М.Н. Расследование краж и мошенничеств, совершенных с использованием банковских карт и их реквизитов: Автореф. дис. ... канд. юрид. наук. М., 2012. 30 с.;
60. Фирсов Е. П. Расследование изготовления или сбыта поддельных денег или ценных бумаг, кредитных либо расчетных карт и иных платежных документов. М. : Юрлитинформ, 2004. 155 с.
61. Франция избавилась от российского кибервора и отправила его в США // АН-online. 2012. 17 июня. URL: <http://argumenti.ru/crime/2012/06/184343>, свободный.
62. Хилюта В.В. Момент окончания хищения: практика применения теоретических концепций // Вестник БДУ, сер. 3. 2010. № 3. С. 93.
63. Эволюция карточного мошенничества в Европе 2013. [Электронный ресурс]. URL: <http://www.fi.co.com/landing/fraudeurope2013>
64. Южин А.А. Мошенничество и его виды в российском уголовном праве. Диссертация на соискание ученой степени кандидата юридических наук. Специальность: 12.00.08 – уголовное право и криминология; уголовно-исполнительное право. Москва, Московский государственный юридический университет имени О.Е. Кутафина (МГЮА), 2016 г.