

**МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ
РОССИЙСКОЙ ФЕДЕРАЦИИ**

КАЗАНСКИЙ ЮРИДИЧЕСКИЙ ИНСТИТУТ

БАНКОВСКАЯ БЕЗОПАСНОСТЬ

Учебное пособие

Составители

О.Г.Шмелева, Г.Н. Хадиуллина

Казань
КЮИ МВД России
2018

ББК 66.2 (2Рос)

Б 23

Одобрено редакционно-издательским советом КЮИ МВД России

Рецензенты:

Доктор юридических наук, доцент А.М. Хужин

(Нижегородская академия МВД России)

Кандидат юридических наук, доцент А.И. Попов

(Рязанский филиал Московского университета МВД России

имени В.Я. Кикотя)

Б 23

Банковская безопасность: учебное пособие / сост.

О.Г. Шмелева, Г.Н. Хадиуллина. – Казань: КЮИ МВД России,
2018. – 132 с.

ISBN 978-5-906977-42-7

Учебное пособие содержит основные понятия, способы и методы обеспечения банковской безопасности, алгоритм действий по выявлению и устранению угроз безопасности.

Адресовано преподавателям, курсантам и слушателям образовательных организаций системы МВД России, сотрудникам органов внутренних дел Российской Федерации.

ISBN 978-5-906977-42-7

ББК 66.2 (2Рос)

© Казанский юридический институт МВД России, 2018

© Шмелева О.Г., Хадиуллина Г.Н., 2018

Оглавление

	Введение	3
Глава 1	Обеспечение экономической безопасности банковской системы России в современных условиях	9
1.1.	Понятие экономической безопасности в банковской сфере	9
1.2.	Виды преступлений в банковской сфере	14
1.3.	Эволюция пластиковых карт и современное состояние в сфере обращения банковских платежных пластиковых карт в России	29
Глава 2	Методы предотвращения мошенничества, связанного с использованием электронных платежных пластиковых карт	49
2.1.	Анализ рисков в деятельности банков в целях предупреждения угроз экономической безопасности в финансово-кредитной сфере	49
2.2.	Уголовно-правовая характеристика и проблемы квалификации мошенничества, совершаемого в банковской сфере с использованием электронных платежных пластиковых карт	59
2.3.	Криминалистическая характеристика мошенничества с использованием платежных карт	81
2.4.	Способы противодействия мошенничеству, связанному с использованием электронных платежных пластиковых карт	118
	Заключение	128
	Список источников и литературы	132

ВВЕДЕНИЕ

Конституция равным образом защищает все формы собственности, и никто не может быть лишен своей собственности не иначе как по решению суда, так как собственность в нашей стране охраняется законом. Государство предусматривает различные способы её охраны, но наиболее существенным и действенным является охрана собственности нормами уголовного закона Российской Федерации. Глава 8 УК РФ "Преступления в сфере экономики" содержит главу 21 "Преступления против собственности", где законодатель раскрывает все виды и формы преступлений, совершаемых против собственности.

Согласно данным портала правовой статистики Генеральной прокуратуры РФ, на территории нашей страны в 2016 году всего совершено 2 160 063 преступления, почти половину которых (43,7 %) составляют хищения чужого имущества, совершенные путем краж - 871 084 (-14,5%), грабежей - 61 524 (-15,4%), разбоев - 11 416 (-16,3%). Количество преступлений, совершенных в форме мошенничества (статьи 159 - 159.6 УК РФ), по сравнению аналогичным периодом 2015 года, увеличилось на 4,2 % и составило 208 926 преступлений¹. Число предварительно расследованных дел данной категории снизилось на 8,2 %, что свидетельствует о том, что в настоящее время совершаемые криминальные посягательства стали отличаться значительным многообразием, динамикой, особой изощренностью, многоплановостью, профессионализмом, организованностью и весьма быстрой адаптацией и способностью к модернизации в зависимости от сферы проникновения.

Вопросы, связанные с противодействием преступности и, в частности, преступлениям против собственности, всегда находятся в поле зрения органов внутренних дел, поскольку именно они от имени государства призваны обеспечивать сохранность имущества, независимо от форм собственности, от преступных посягательств, а правильная квалификация преступлений выступает гарантом законности

¹Портал правовой статистики Генеральной прокуратуры РФ. URL: <http://www.crimesstat.ru>

их деятельности. Эффективность деятельности подразделений органов внутренних дел по противодействию преступлениям против собственности зависит в том числе и от верной квалификации преступного деяния.

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 карту, на которую перечисляется их заработная плата, 71% - дебетовую карту, 65% - кредитную карту¹. Согласно данным правоохранительных органов России, 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 трансформации и адаптации уголовного законодательства к новым реалиям. В связи с тем, что законодателю необходимо было решить проблему квалификации хищения с использованием карт, 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. 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 фор-

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

мы, 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, безусловно, приведет к росту числа преступлений в указанной сфере.

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

риалы судебно-следственной практики по делам о мошенничестве; результаты социологических исследований; научные публикации по теме исследования.

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 совершения 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.

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 её финансовой системы¹, так как без устойчивого функционирования финансовой системы и финансового рынка невозможно наращивание экономического и научно-технического потенциала России, который, в свою очередь, призван обеспечить достойное место страны в мире.

В начале 90-х гг. XX в. с началом экономических преобразований в стране, на фоне дефицита законодательства, которое должно было регулировать банковскую и иную коммерческую деятельность, создалось большое количество банков, которые по характеру своей деятельности зачастую были или фиктивными, или неконкурентоспособными. Безусловно, это не только не способствовало формированию в России единой устойчивой национальной системы финансового рынка, но и, как следствие, приводило к противоправным действиям. 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 безопасности².

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

¹ Архипов А., Городецкий А., Михайлов Б. Экономическая безопасность: оценки проблемы, способы обеспечения// Вопросы экономики. 2014. № 12. С.47.

² 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.

- 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&Poor's 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 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 и 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 информации¹.

Исходя из всего вышесказанного, можно сделать вывод о том, что глобализация экономики и внедрение технологических новаций в деятельность кредитных организаций несет с собой новые угрозы как для всей банковской системы в целом, так и для отдельных банков. С другой стороны, ключевое изменение ситуации - это усиление конкуренции, поэтому банкам для обеспечения своей экономической безопасности и устойчивости в новых, более жестких, конкурентных

¹ 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.

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 отношения¹. Следовательно, одним из важнейших элементов национальной безопасности является безопасность финансовой системы государства. Экономическое развитие страны зависит от множества факторов: грамотной экономической политики, ресурсов, технологий и 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 комплекса². Экономика России на протяжении нескольких веков была «догоняющей», но необходимо отметить такие недостатки переноса опыта экономического и технологического

¹ Бочаров О.А. Формирование основ экономической безопасности банковской деятельности: автореф. канд. экон. наук. М., 2013. С.321.

² Там же.

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. Несмотря 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.), 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.);
- и 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 склонения 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 отмыwanie 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.

То обстоятельство, что пластиковая карта как средство расчета являются относительно новым финансовым инструментом, применяемым на территории России, предопределило относительно небольшую историю уголовно-правовой охраны общественных отношений от криминальных посягательств, предметом которых являются указанные платежные средства. В частности, лишь с принятием действующего уголовного закона впервые было криминализировано деяние, конструктивным признаком которого является наличие предмета преступления, определяемого как «кредитные либо расчетные карты» (ст. 187 УК РФ).

Специфической особенностью преступлений, совершаемых в сфере оборота пластиковых карт, является их высокая латентность, что обусловлено не только вопросами процессуального и криминалистического характера (в частности, проблемы установления и фиксации следов преступления, определения места совершения пре-

ступления, подсудности уголовных дел и т.п.), но и проблемами технико-юридического конструирования норм уголовного закона, устанавливающих ответственность за различного рода посягательства с использованием пластиковых карт.

Квалификация хищений с использованием пластиковых карт, как правило, влечет необходимость уголовно-правовой оценки иных деяний, предметом которых являются указанные платежные документы, что свидетельствует о целесообразности рассмотрения в рамках настоящей работы не только вопросов завладения чужим имуществом, но и иные криминальные посягательства, характеризующиеся наличием специального предмета преступления – пластиковой карты, как финансового инструмента, посредством которого уполномоченный субъект распоряжается денежными средствами, находящимися на соответствующем расчетном счете.

Предваряя уголовно-правовую характеристику соответствующих составов преступлений, следует определиться с основными признаками, характеризующими пластиковую карту как финансовый инструмент.

Расчетная пластиковая карта является носителем информации, которая:

- определяет платежную систему, уполномоченного держателя карты и ее эмитента;
- устанавливает порядок и условия применения карты (например, алгоритм обработки транзакций, сроки действия карты, территориальные ограничения и т.п.);
- обеспечивает защиту карты от копирования и несанкционированных модификаций, в том числе посредством защиты информации, которая используется для аутентификации самой карты, а также лица, уполномоченного ее использовать (специальные логотипы, проверочные значения CVV/CVC, CVV2/CVC2, секретные ключи, используемые для идентификации карты и т.п.).

Информация, которая содержится на карте, наносится на магнитную полосу и (или) ее содержит микропроцессор, расположенный в карте. Считывание информации, которую содержит карта, происходит посредством применения специальных устройств – картридеров

(указанные устройства содержатся в так называемых POS-терминалах торговых и обслуживающих предприятий, а также в банкоматах).

Функционирование необходимой инфраструктуры применения той или иной пластиковой карты обеспечивает обслуживающий банк, который заключает договоры с торговыми предприятиями на обслуживание в них пластиковых карт, гарантируя торговому предприятию возврат средств за операции, совершенные в нем по картам любого банка - участника платежной системы.

Анализ статистических данных позволяет сделать вывод, что наиболее распространенными видами криминальных посягательств в сфере использования пластиковых карт являются:

- применение поддельных карт;
- противоправное использование подлинных карт (например, без санкции уполномоченного держателя);
- противоправное получение и использование конфиденциальной информации (например, скимминг – незаконное получение данных при помощи специального считывающего устройства (скиммера), фишинг – вид интернет-мошенничества с целью получения доступа к закрытой информации, в том числе содержащейся на расчетных пластиковых картах, и ряд других приемов).

Каждый из вышеприведенных видов противоправного поведения характеризуется различным содержанием, что влечет их различную уголовно-правовую оценку. В частности:

- противоправное получение информации по карте, а также данных держателя, осуществляется посредством скимминга, фишинга, распространения вредоносных программ либо осуществления хакерских атак. Указанные деяния, в зависимости от содержания объективной стороны, подлежат квалификации по следующим нормам уголовного закона: ст. 183 УК РФ «Незаконное получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну», ст. 272 УК РФ «Неправомерный доступ к компьютерной информации», ст. 273 УК РФ «Создание, использование и распространение вредоносных компьютерных программ», ст. 138.1 УК РФ «Незаконный оборот специальных технических средств, предназначенных для негласного получения информации»;

- изготовление поддельных расчетных карт. Уголовная ответственность за данное деяние установлена ст. 187 УК РФ «Изготовление или сбыт поддельных кредитных либо расчетных карт и иных платежных документов»;

- применение контрафактных пластиковых карт с целью получения наличных денежных средств в банкоматах либо осуществление операций по оплате товаров, работ либо услуг. Указанные действия, с учетом специфики конструктивных элементов состава, могут быть квалифицированы как «Кража» ст.158 УК РФ либо «Мошенничество с использованием платежных карт» ст. 159.3 УК РФ.

Тот факт, что большинство из рассмотренных выше деяний предваряют либо сопровождают факты хищений с использованием пластиковых карт, предопределяет необходимость анализа наиболее значимых признаков составов преступлений, описанных в рамках указанных норм уголовного закона.

Статья 187 УК РФ «Изготовление или сбыт поддельных кредитных либо расчетных карт и иных платежных документов -

Изготовление в целях сбыта или сбыт поддельных кредитных либо расчетных карт, а также иных платежных документов, не являющихся ценными бумагами, -

- наказывается...».

Предметом преступления, описанного в рамках ст. 187 УК РФ, являются кредитные либо расчетные карты. Нормативное определение требует от правоприменителя в каждом конкретном случае применения указанной нормы уголовного закона определять, какой вид карты изготавливается либо сбывается преступником. Несмотря на очевидное сходство указанных финансовых инструментов, они характеризуются различными признаками.

Кредитная карта предназначена для совершения ее держателем операций, расчеты по которым осуществляются за счет денежных средств, предоставленных кредитной организацией – эмитентом клиенту в пределах установленного лимита в соответствии с условиями кредитного договора ^[2].

Расчетная (дебетовая) карта – карта, предназначена для совершения операций ее держателем в пределах установленной кредитной

организацией – эмитентом суммы денежных средств (расходного лимита), расчеты по которым осуществляются за счет денежных средств клиента, находящихся на его банковском счете, или кредита, предоставляемого кредитной организацией – эмитентом клиенту в соответствии с договором банковского счета при недостаточности или отсутствии на банковском счете денежных средств (овердрафт).

Объективная сторона рассматриваемого преступления выражена в альтернативных действиях, определяемых законом как «изготовление» или «сбыт».

Изготовление карты в целях сбыта фактически означает ее подделку. Подделка карты может быть полной либо частичной. Полная подделка представляет собой изготовление карты не эмитентом и не платежной системой, но имеющей такие технические характеристики и внешний вид, которые позволяют ее использование в безналичных расчетах, и она может быть воспринята участниками платежной системы в качестве финансового инструмента. Частичной подделкой является карта, выпущенная эмитентом или платежной системой и переделанная таким образом, что позволяет ее применение как средства расчета.

Качество подделки пластиковой карты не имеет значения для квалификации. Это обусловлено тем, что даже при условии ненадлежащего качества расчетные карты, при наличии в них соответствующей информации, позволяют распоряжаться денежными средствами, находящимися на расчетных счетах (например, при использовании так называемого белого пластика производится получение наличных денежных средств в банкомате).

Статья 272 УК РФ «Неправомерный доступ к компьютерной информации

Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации, -
- наказывается...».

Применительно к пластиковым картам чаще всего деяние, ответственность за которое предусмотрено ст. 272 УК РФ, выражено в копировании информации посредством совершения скимминга (как

было указано, это процесс незаконного получения информации по карте, посредством ее копирования и переноса на другой материальный носитель). Однако для определения соответствующего копирования как уголовно наказуемого деяния (в рамках рассматриваемой нормы) необходимо установить режим правовой охраны соответствующей информации, являющейся предметом копирования.

Магнитная полоса пластиковой расчетной карты содержит два блока информации, в частности, на первом треке полосы содержится информация о держателе карты, а на втором треке – реквизиты самой карты.

В соответствии с содержанием Положения Банка России №382-П (пункт 2.1) защите подлежит «информация, необходимая для удостоверения клиентами права распоряжения денежными средствами, в том числе данных держателей платежных карт». Номер карты, как и данные о ее правомочном держателе, содержится на магнитной полосе, следовательно, информация, считываемая с карты, и копируемая на иной носитель, является охраняемой законом. Изложенное позволяет сделать вывод, что неправомерный доступ к информации, содержащейся на карте, соответствует признакам объективной стороны состава преступления ст. 272 УК РФ.

Статья 183 УК РФ «Незаконное получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну

Собирание сведений, составляющих коммерческую, налоговую или банковскую тайну, путем похищения документов, подкупа или угроз, а равно иным незаконным способом –

- наказывается...».

Детальный анализ содержания Положений Банка России № 266-П^[4] свидетельствует о том, что платежная карта является финансовым инструментом, который в числе прочего определяет соответствие реквизитов карты реквизитам корреспондирующего ей расчетного счета. Другими словами, расчетная карта содержит реквизиты банковского счета, информация о котором является банковской тайной. Изложенное свидетельствует о том, что получение сведений, касающихся

ся номеров банковских карт, фактически посягает на банковскую тайну и подлежит квалификации по ст. 183 УК РФ.

Нередко преступление, ответственность за которое предусмотрена ст. 183 УК РФ, совершается способом, образующим самостоятельный состав преступления. Речь идет о ситуациях, когда получение сведений о реквизитах расчетных пластиковых карт осуществляется посредством неправомерного доступа к охраняемой законом компьютерной информации. В таких случаях деяния соответствующих субъектов подлежат квалификации по совокупности преступлений, предусмотренных ст. 272 УК РФ и ст. 183 УК РФ. В качестве аргумента, свидетельствующего о необходимости именно такого подхода к уголовно-правовой оценке аналогичных деяний, проиллюстрируем следующий пример судебной практики.

Тверской районный суд г. Москвы, дело N 1-372/2012:

«Несостоятельна позиция стороны защиты об исключении из обвинения П. и К. ч. 3 ст. 272 УК РФ, основанная на том, что ч. 1 ст. 183 УК РФ включает копирование информации в качестве способа совершения указанного преступления, а также на том, что в данном случае, исходя из требований ст. 17 УК РФ, по мнению защиты, совокупность вышеуказанных преступлений исключается.

Так, собранные по делу доказательства в своей совокупности полностью подтверждают обстоятельства совершения подсудимыми двух преступлений в совокупности, поскольку П. и К. с помощью имеющегося у них считывающего устройства собирали сведения, содержащиеся на расчетных банковских картах граждан, составляющие в соответствии с требованиями ст. 857 ГК РФ, ст. 26 Федерального закона от 2 декабря 1990 г. № 395-1 «О банках и банковской деятельности» банковскую тайну. Данные сведения собирались подсудимыми путем неправомерного доступа к охраняемой законом компьютерной информации, что повлекло ее копирование, в связи с чем в соответствии с требованиями ч. 2 ст. 17 УК РФ вышеуказанные действия подсудимых безусловно являются способом совершения преступления, предусмотренного ч. 1 ст. 183 УК РФ, однако образуют самостоятельный состав преступления, предусмотренного ч. 3 ст. 272 УК РФ, а потому являются непосредственно идеальной совокупностью

двух указанных преступлений, учитывая, что путем неправомерного доступа к компьютерной информации подсудимые в данном случае посягали на информацию ограниченного доступа, а именно на банковскую тайну».

Статья 273 УК РФ «Создание, использование и распространение вредоносных компьютерных программ

Создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, -

- наказывается...».

Признаки преступления, уголовная ответственность за которое установлена ст. 273 УК РФ, нередко содержатся в деяниях, посредством которых осуществляется неправомерный доступ и копирование информации с расчетных карт (посредством применения скимминговых устройств). В частности, речь идет о ситуациях, когда в качестве средства достижения преступной цели (доступа либо копирования) используются компьютерные программы, заведомо предназначенные для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации.

Буквальное толкование рассматриваемой нормы уголовного закона свидетельствует о том, что преступление необходимо признавать оконченным составом с момента создания либо использования соответствующей программы. Под использованием понимается ее непосредственное применение в противоправных целях. В отличие от ст. 272 УК РФ особенностью диспозиции ст. 273 УК РФ является то, что в соответствии с ее содержанием, несанкционированное воздействие подразумевает таковое в отношении любой, а не только защищаемой законом информации.

Статья 138.1 УК РФ «Незаконный оборот специальных технических средств, предназначенных для негласного получения информации

Незаконные производство, приобретение и (или) сбыт специальных технических средств, предназначенных для негласного получения информации,

-наказываются ...».

Посредством введения в структуру Уголовного кодекса статьи 138.1 (Федеральный закон от 07.12.2011 г. № 420-ФЗ) законодатель установил уголовную ответственность за деяния, которые выражены в незаконном производстве, приобретении и (или) сбыте специальных средств, предназначенных, в числе прочего, и для негласного получения информации, содержанием которой являются данные о владельцах пластиковых карт, а также реквизитах самих карт, посредством использования которых впоследствии совершаются посягательства на собственность.

При установлении признаков состава, описанного в рамках анализируемой нормы, у правоприменителей может возникнуть проблема соотнесения скимминговых устройств с техническими средствами по смыслу ст. 138.1 УК РФ. Решение указанной проблемы возможно посредством изучения постановления Правительства РФ от 10.03.2000 г. №214^[6]. Указанный документ устанавливает список технических средств, посредством которых осуществляется негласное получение информации. Данный список определяет, что в числе прочих, к техническим средствам, специально предназначенным для негласного получения информации, относятся:

1. Телевизионные и видеокамеры, обладающие, по крайней мере, одним из следующих признаков: закамуфлированные под бытовые предметы; имеющие вынесенный зрачок входа (PIN-HOLE); работающие при низкой освещенности объекта (0,01 лк и менее) или при освещенности на приемном элементе 0,0001 лк и менее;

2. Комплекс аппаратуры передачи видеоизображения по кабельным, радио- и оптическим линиям связи.

Указанные средства применяются, в частности, для негласной записи и передачи по техническим каналам связи данных, содержащих PIN-коды держателей пластиковых карт.

3. Специальные технические средства для негласного получения (изменения, уничтожения) информации с технических средств ее хра-

нения, обработки и передачи. Применительно к сфере оборота пластиковых карт такими техническими средствами необходимо признавать скимминговые устройства (ридеры), используемые для копирования данных с магнитной полосы карт, а также накладные клавиатуры для считывания PIN-кодов.

Изложенные нормативные установления, обеспечивающие уголовно-правовую охрану общественных отношений непосредственно либо в числе прочих, в сфере оборота пластиковых карт, устанавливают ответственность за деяния, которые, как правило, являются приготовлением к хищению с использованием пластиковых карт.

При отсутствии признаков оконченного состава мошенничества и необходимости квалификации соответствующих деяний как приготовления, правоприменителям необходимо учитывать ограничения, установленные в рамках уголовного закона, касающиеся возможности привлечения к уголовной ответственности только за приготовление к тяжким и особо тяжким преступлениям. Изложенное делает необходимым установление умысла соответствующих субъектов на приготовление к соответствующим посягательствам на собственность, что на практике, как правило, реализовать не удастся, о чем свидетельствует отсутствие судебной практики по квалификации рассмотренных в рамках настоящего параграфа преступлений как приготовления к мошенничеству. Однако в любом случае соответствующие деяния должны получить самостоятельную уголовно-правовую оценку.

§3. Эволюция пластиковых карт и современное состояние в сфере обращения банковских платежных пластиковых карт в России

Рассматривая историю пластиковых карт, представляется необходимым проанализировать две важные функции пластиковых карт в системе денежного обращения: 1) функцию обналичивания средств и 2) функцию расчетов.

Функция обналичивания - это древнейшая из функций обращения денежных средств. В XX в. до н. э. жители Вавилона могли сдать серебряные слитки, овец или зерно в храм бога Сина, получив за это

глиняный "вексель", который можно было обменять на те же ценности в других городах.

Подобные векселя существовали во многих странах Древнего мира. Чтобы их нельзя было украсть, в античной Греции придумали ноу-хау - документ с подписью владельца, которую он обязан был продублировать при получении денег. Он назывался "хирограф" (от cheir - "рука" и grapho - "пишу"). В эпоху Крестовых походов тот же принцип использовали рыцари-тамплиеры, создавшие сеть "отделений" ордена по всей Европе. Клиент ордена получал кусок пергамента со своим именем и отпечатком большого пальца, по которому мог получить деньги в любой из контор ордена.

Эстафету ордена подхватили возникшие в XIII в. в Италии банки, выдававшие клиентам кредитные обязательства - бумаги с печатью, которые можно было обменять на наличные деньги во всех отделениях банка. Поняв выгоду этого дела, к нему присоединилось государство, ставшее в итоге единственным эмитентом - изготовителем этих обязательств - всем известных бумажных денег¹.

Функция платежей по сравнению с обналичиванием развивалась с запозданием. В XVIII столетии деньги и их владельцы начали активно перемещаться по миру. Для помощи путешествующим на финансовом рынке появилось множество ценных бумаг, заменяющих реальные деньги (деривативов). Однако все они не имели отношения к банковским счетам. Для удобства платежей по ним были придуманы чеки - бумаги с подписью владельца счета. США стали первой страной, где чеками начали массово расплачиваться в ресторанах, отелях, магазинах. Чеки были удобны, но они имели ограниченный характер применения - деньги по ним трудно было получить в другом городе и практически невозможно - в другой стране.

Предшественником банковских карт явились первые карты лояльности - карточки, которые выпускали крупные американские отели, нефтяные компании и магазины в начале XX в. Эти товарные карточки имели два назначения - следить за счетом клиента и обеспечивать механизм записи его покупок. Их появление было логическим продолжением оплаты в рассрочку.

¹ Эрлихман В. Кошелек и жизнь // Gala Биография. 2012. № 11 (95). С. 96.

В 1914 г. компания Western Union выпустила для клиентов первую дебетовую карту (charge card¹). Затем торговые предприятия стали выпускать карточки для самых богатых клиентов, чтобы привязать их к своей сети магазинов и продавать им наиболее дорогие товары.

В начале 1920-х гг. нефтяные компании стали выпускать "карты учтивости" (courtesy cards), с помощью которых водители могли делать покупки на любой бензоколонке. Появились первые "бензиновые карты".

Первые карты были картонными и, следовательно, недолговечными. Надо было менять материал, и в 1928 г. бостонская компания Farrington Manufacturing выпустила первые металлические карты - Charga-Plates, пластинки с выбитым адресом. На них выдавливались (эмбоссировались) идентификационные данные, что позволило в некоторой степени автоматизировать процедуру приема карты.

Начало банковским кредитным картам положил Джон С. Биггинс, один из специалистов по потребительскому кредиту из Национального банка Flatbush в Бруклине. В 1946 г. он организовал работу по кредитной схеме Charge-it, которая предусматривала расписки, принимавшиеся местными магазинами от клиентов за мелкие покупки. По совершении покупки магазин сдавал эти расписки в банк, который оплачивал их со счетов покупателей.

В Национальном банке Flatbush была впервые опробована классическая цепочка расчетов, используемая сейчас повсеместно в банковском карточном бизнесе. Первой массовой платежной карточной системой была созданная в 1949 г. компания Diners Club. Главным отличием ее от предыдущих систем было то, что между клиентами и коммерческими компаниями существовал посредник, который взял на себя проведение расчетов. Именно это позволило Diners Club стать первой и очень массовой универсальной картой.

Идея создания такой карты родилась в центре Манхэттена, а именно в ресторане Major's Cabin Grill. Там встретились Альфред Блумингдейл, внук основателя одного из самых крупных американских универмагов, его давний друг Фрэнсис Макнамара, возглавлявший на тот момент финансовую компанию Hamilton Credit Corp., и

¹ Western Union / Our Rich History. URL: <http://corporate.westernunion.com/history.html>.

юрист Фрэнсиса - Ральф Снайдер. За обедом разговор зашел об одном клиенте Макнамары в Бронксе. Этот предприниматель позволял соседям пользоваться своим банковским счетом за проценты. Продавцы магазинов звонили ему по телефону и, получив разрешение, записывали стоимость покупок на его счет. В такой сделке новшеством являлось наличие посредника, который, используя свою кредитоспособность, предоставлял ссуду людям, не имеющим возможность получить ее по-другому.

Эта финансовая схема очень понравилась собеседникам. Изъян они увидели лишь в кредитовании людей, не имеющих в магазине кредитной линии. Ведь чаще всего именно с ними возникают проблемы. И поэтому ресторан показался им самым удачным местом для развития нового бизнеса. Макнамара, Блумингдейл и Снайдер поинтересовались у владельца ресторана, сколько он намерен платить за новых клиентов, которых они собираются к нему присылать. Владелец незамедлительно ответил: "Семь процентов". Так появилась ставка, которая установилась на десятилетия в области кредитных карт. Немного позднее, когда бизнес начал процветать, они задали вопросу же хозяину ресторана, откуда он взял эти известные "семь процентов". "Агент по путешествиям потребовал бы десять", - был ответ. Использовать в качестве идентификации клиентов соучредители решили эмбоссированные пластинки, которые к тому времени уже были довольно распространены и применялись во многих магазинах и бензиновых компаниях. К программе было привлечено 10 - 12 близлежащих ресторанов города.

Для развития бизнеса срочно требовались кредитные средства, и партнеры принимают решение об объединении своих компаний. Новая компания начала свою деятельность 28 января 1950 г. с начальным капиталом в 75 тыс. долл. и получила название Diners Club, дословно - "Клуб обедающих". Уже через год 285 торгово-сервисных организаций обслуживали 35 тыс. держателей карт компании. Diners Club регулярно взимала со своих клиентов плату за годовое обслуживание карты в размере 3 долл. К концу 1951 г. компания принесла владельцам прибыль в размере 61 222 долл. с оборота в 6,2 млн.

Далее вместе с развитием рынка Соединенных Штатов Америки операции с картами стали внедряться повсеместно. В 1951 г. Diners Club дала первую лицензию на использование своих схем и своего имени в Великобритании. И уже после этого появились такие известные платежные системы, как VISA, MasterCard и American Express.

В 1958 г. Bank of America выпустил карту Americard, которая стала очень успешным проектом - уже по итогам года было выдано 60 тыс. карт. В 1966 г. Bank of America начал выдавать лицензии другим банкам на проведение операций с картами BankAmericard. Решение о расширении операций на всю страну встретило противодействие других крупных банков и привело к образованию второй национальной системы карт, получившей название Interbank Cards Association (ICA). Ассоциация начала выпускать собственную карту - MasterCharge, после ряда переименований превратившуюся в MasterCard.

В середине 1970-х гг. платежные системы переросли национальный уровень, неизбежно возник вопрос о создании глобальных брендов. В 1976 г. Americard поменяла имя на VISA с целью мирового признания. В 1979 г. с той же целью ICA изменила свое название на MasterCard International и карта MasterCharge стала называться MasterCard. Несмотря на смену названия платежной системы, в логотипе пересекающиеся круги остались почти неизменными, поскольку компания не хотела потерять такой сильный носитель бренда. Аналогично, если посмотреть на историю эволюции бренда VISA, можно увидеть, что он не менялся 30 лет - с 1976 по 2006 г.

За период 1969 - 1981 гг. число банков, которые присоединились к MasterCard, возросло с 4461 по 12 504, а количество банков, присоединившихся к VISA, выросло с 3751 до 12 518¹. К 1984 г. 71% всех американцев в возрасте от 17 до 65 лет пользовались кредитными картами. В 1986 г. средний баланс на картах составлял 1472 долл. (для сравнения в 1970 г. он был 649 долл.).

В 1980-х гг. было дальнейшее расширение MasterCard в Азию и Латинскую Америку. В 1987 г. MasterCard стал первой картой оплаты в Китайской Народной Республике. В 1988 г. первая MasterCard была

¹ Распространение пластиковых карт по миру. URL: <http://www.belcard.by/cgi-bin/view.pl?topicid=feeb0ecf>.

выпущена в Советском Союзе.¹

Банкоматы появились позже банковских карт, причем как инфраструктура для банковских карт они стали работать только в конце 1960-х - начале 1970-х гг., таким образом, примерно с 1970 - 80-х гг. развиваясь наиболее активно. В таблице 1 отмечены наиболее важные события карточного бизнеса, разделенные на две части - собственно технологические изменения карт и эволюцию карточной инфраструктуры.

Таблица 1

Хроника технологической эволюции в карточном бизнесе 1900-2010 гг.

Период, годы	Эволюция карт	Эволюция банкоматов и иной карточной инфраструктуры
1900 - 1920	1914 г. - первая дебетовая карта Western Union. Первые карты лояльности (в основном VIP)	
1921 - 1930	Начало 1920-х гг. - нефтяные компании стали выпускать "карты учтивости" (courtesy cards). 1928 г. - металлические карты Charga-Plates	
1931 - 1940	1938 г. - кредитная схема American Airlines, Universal Air Travel Plan (UATP)	1939 г. - прототип первого банкомата (изобрел Лютер Джордж Симджян)
1941 - 1950	1946 г. - национальный банк Flatbush в Бруклине создал кредитную схему Charge-it. 1949 г. - появление Diners Club. 1950 г. - первая карта Diners Club (картонная)	1950 г. - появление импринтеров в точках продаж (первым изготовителем стала компания Addressograph)
1951 - 1960	1951 г. - Franklin National Bank of New York выпустил первую банковскую карту, которой можно было расплачиваться в несколь-	

¹ История платежной системы MasterCard International. Начало истории. URL: http://rbcard.com/history/hist_master.htm/, www.mastercard.com.

	ких соседних магазинах	
1961 - 1970	1966 г. - первые карты с магнитной полосой, которую считывало электронное устройство	1967 г. - первый банкомат по выдаче наличных денег в отделении британского банка Barclays. Изобретатель - шотландец Джон Шепард-Баррон. 1969 г. - американец Дон Ветцель изобрел уличный банкомат, принимающий карты с магнитной полосой
1971 - 1980	1974 г. - Arizona Bank в США выдает первую дебетовую карту к текущему счету. 1975 г. - Ролан Морено изобрел и запатентовал электронную карту памяти (чиповую карту)	1971 г. - Air Travel Card вводит платежные карты с магнитной полосой и первые в мире платежные терминалы. 1972 г. - Citibank начинает строить сеть банкоматов. 1972 г. - банк Lloyds ввел в Великобритании первые online-банкоматы под названием Cash-Point. 1972 - 1975 гг. - в США несколько сотен банкоматов 18 банков в штате Вашингтон были объединены в сеть под названием Exchange. 1979 г. - появились электронные платежные терминалы - EFTPOS
1981 - 1990	1983 г. - MasterCard поместила на карточке лазерную голограмму, что затруднило подделку и существенно повысило надежность карточек	1980-е гг. - в США, Японии и Европе появляются первые общенациональные сети банкоматов (Cirrus, Plus, Exchange и др.)
1991 - 2000	1993 г. - выпуск первой карты с CVV (трехзначным кодом проверки подлинности карты платежной системы). 1995 г. - моновалютная микропроцессорная карточка для мелких покупок (Proton).	В 1994 г. в США была реализована первая покупка через Интернет с использованием eCash (электронных денег). 1995 г. - платежная система Mondex разработала электронный кошелек.

	1996 г. - Europay, MasterCard и VISA выпускают международный стандарт для банковских чиповых карт под названием EMV	В конце 1990-х гг. появился первый банкомат с функцией приема денег - cash-in. 2000 г. - платежные терминалы обеспечивают коммуникацию с помощью GPRS, радиочастот или bluetooth
2001 - 2010	2002 г. - MasterCard тестирует бесконтактную чиповую карту PayPass и вводит мини-карту SideCard. 2005 г. - выпуск первой карты VISA с CVV2 (трехзначным кодом проверки подлинности карты платежной системы). 2005 г. - MasterCard и VISA пришли к соглашению по стандарту для бесконтактных чиповых карт	В 2000-х гг. при производстве банкоматов начали применять технологию Cash Recycling

Прототип первого банкомата был изобретен Лютером Джорджем Симджяном еще в 1939 г. Устройство выдавало наличные, но при этом не могло списать их со счета: аппарат не был связан с банком.

Интересно отметить, что изобретатель банкомата Джон Шепард-Баррон впоследствии пророчески заявил: "Скоро все покупки мы будем совершать с помощью мобильных телефонов. Вы просто отправляете СМС, и деньги списываются с вашего счета".

Пластиковых карточек в то время не существовало, и для снятия денег использовались специальные ваучеры, которые надо было заранее получить в банке. Спустя несколько лет другой шотландец - Джеймс Гудфеллоу - придумал использовать секретный PIN-код для защиты от несанкционированного доступа к банковским счетам, а первые пластиковые карточки с магнитной полосой появились в США.

Однако широкое распространение банкоматы получили только в конце 1980-х гг., до этого они особенным спросом не пользовались. Можно назвать две основные причины такой ситуации. Прежде всего,

банковское дело является одним из самых консервативных видов бизнеса.

Важная проблема заключалась в технологической отсталости самих банкоматов. В отличие от современных машин первые банкоматы работали в режиме офлайн, т.е. не имели постоянной связи с банком.

Логично, что однажды производители банкоматов задумались над вопросом, а почему банкомат только выдает деньги. Снять деньги с кредитной карты легко, но, чтобы погасить кредит, приходится идти в отделение банка. В итоге в конце 1990-х гг. появился первый банкомат с функцией приема денег - cash-in.

В России в силу нашего исторического отставания от мирового банковского бизнеса подавляющее большинство банкоматов, приняв деньги от клиента, не могут их тут же выдать другому клиенту. Собранные деньги распределяются по отдельным кассетам и хранятся там до тех пор, пока их не пересчитает инкассация. Только после этого банк сможет распоряжаться этими деньгами по своему усмотрению, в том числе выдавать их через банкоматы.

В ряде зарубежных стран банкоматы с ресайклингом применяются уже много лет. Наибольшую распространенность они получили в Азии - в Японии первые банкоматы с такой функцией появились еще в 1980-х гг. В Европе банкоматы с ресайклингом начали получать широкое распространение в начале 2000-х гг. В отличие от России там они подлежат обязательной сертификации. Пионером в области использования банкоматов с замкнутым оборотом наличных в России, пожалуй, можно назвать Альфа-Банк. Он начал присматриваться к таким устройствам еще в 2009 г., запуская их в пилотном режиме. Полноценная эксплуатация ресайклинг-банкоматов в банке началась в 2011 г.¹

Другое направление эволюции банкоматов - биометрические технологии. В Малайзии и Японии банки активно используют карты,

¹ Лаврентьева Н. Российские банки внедряют технологию, отбирающую "хлеб" у инкассаторов // Cnews.ru. 16 марта 2012г. URL: <http://www.cnews.ru/news/top/index.shtml?2012/03/16/481803>.

на чип которых записаны биометрические данные человека - отпечаток пальца или радужная оболочка глаза.

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.

Классифицировать карты можно по различным признакам: по материалу изготовления (бумажные, пластиковые, металлические), по способу записи информации (магнитные и микропроцессорные), по территориальной принадлежности (международные, национальные, локальные), а также по многим и многим другим признакам. Платежные системы также используют свою классификацию карточных продуктов применительно к клиентским группам, разделяя виды карт по сфере применения и социальному статусу держателя.

Положение об эмиссии платежных карт и об операциях, совершаемых с их использованием (утв. Банком России 24 декабря 2004 г. N 266-П; ред. от 15 ноября 2011 г., с изменениями от 10 августа 2012 г.; далее - Положение Банка России N 266-П), также классифицирует платежные карты по системе проведения расчетов (расчетные карты, кредитные карты и предоплаченные карты), что отражено в п. 1.5: кредитная организация вправе осуществлять эмиссию банковских карт следующих видов: расчетных (дебетовых) карт, кредитных карт и предоплаченных карт.

Расчетная (дебетовая) карта предназначена для совершения операций ее держателем в пределах установленной кредитной организацией - эмитентом суммы денежных средств (расходного лимита), расчеты по которым осуществляются за счет денежных средств клиента, находящихся на его банковском счете, или кредита, предоставляемого кредитной организацией - эмитентом клиенту в соответствии с договором банковского счета при недостаточности или отсутствии на банковском счете денежных средств (овердрафт).

Кредитная карта предназначена для совершения ее держателем операций, расчеты по которым осуществляются за счет денежных средств, предоставленных кредитной организацией - эмитентом клиенту в пределах установленного лимита в соответствии с условиями кредитного договора.

Предоплаченная карта предназначена для совершения ее держателем - физическим лицом операций, расчеты по которым осуществляются кредитной организацией - эмитентом от своего имени за счет денежных средств, предоставленных держателем - физическим лицом, или денежных средств, поступивших в кредитную организацию - эмитент в пользу держателя - физического лица, если возможность использования поступивших денежных средств от третьих лиц предусмотрена договором между держателем - физическим лицом и кредитной организацией - эмитентом. Предоплаченная карта удостоверяет право требования ее держателя - физического лица к кредитной организации - эмитенту по оплате товаров (работ, услуг, результатов интеллектуальной деятельности) или выдаче наличных денежных средств".

Расчетная (дебетовая) карта - это может быть дебетовая карта или карта с разрешенным овердрафтом. В первом случае клиент может использовать только средства, которые он внес на карту, и после того, как он их израсходует, то уже не сможет использовать карту (более подробно дебетовые карты будут описаны далее). Карта с разрешенным овердрафтом позволяет как пользоваться средствами клиента, которые он внес на счет, так и получать кредит по карте, когда средства клиента заканчиваются. Далее мы подробно опишем карты с разрешенным овердрафтом.

Кредитная карта. По кредитной карте клиент может пользоваться только кредитом, предоставленным банком, по ней не может быть "положительного" остатка, т.е. или держатель карты должен банку, или не должен. Даже если клиент внесет сумму, превышающую долг, то сумма превышения будет использована только на очередное погашение кредита, но не для платежей по карте.

Предоплаченная карта. По предоплаченной карте не открывается счет физическому лицу - это обязательства банка перед клиентом,

данный продукт по своей сути является переводом без открытия счёта, который временно до распоряжения клиента, куда его направить, находится в банке.¹

В настоящее время на территории России действуют десятки локальных, региональных и межрегиональных платёжных систем. Количество держателей пластиковых карточек российских платёжных систем исчисляется в совокупности многими сотнями тысяч. В исследовании А.В.Евстратова и А. И. Бережной обозначена сильная зависимость между состоянием рынка электронных платёжных систем и объёмом продаж в РФ, что свидетельствует о необходимости развития рынка электронных платёжных систем, которые оказывают прямое влияние на рост экономики страны².

В условиях введенных против России санкций бесперебойность и безопасность осуществления транзакций находятся под угрозой из-за подверженности международных платёжных систем политическому влиянию со стороны США и Евросоюза. В этих условиях необходимым стало создание национальной платёжной системы (НПС), не зависящей от внешних сил. С целью изучения состояния национальной платёжной системы на современном этапе, анализа существующих проблем, поиска путей их решения и определения перспектив для начала рассмотрим российский рынок платёжных систем³.

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 бан-

¹ Бизнес-энциклопедия "Платёжные карты" / И.М. Голдовский, М.Ю. Гончарова, А.Н. Грачев и др.; ред.-сост. А.С. Воронин. 2-е изд., перераб. и доп. М.: КНОРУС, ЦИПСИР, 2014. 560 с.

²Евстратов А.В., Бережная А.И. Развитие рынка электронных платёжных систем и его роль в экономике Российской Федерации // Известия Волгоградского государственного технического университета. 2013. № 11 (144). С. 74-79.

³Теряева А.С., Журавлева Т. А., Харитонюк Е. С. Национальная платёжная система России: предпосылки возникновения и текущее состояние// Дискуссия. 2016. Вып. №2 (65). С. 54.

ковской карты, в Китае – 3,61, в Великобритании – 2,4, в Германии – 1,63, а в Италии – 1,22 карты¹).

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.

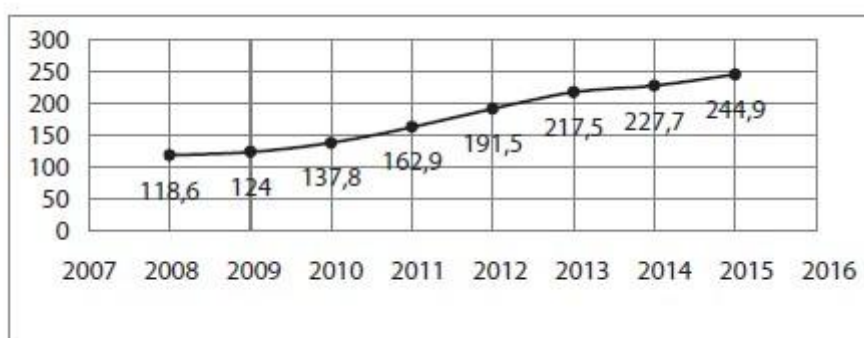


Рис. 1. Количество электронных платежных пластиковых карт, эмитированных в Российской Федерации, млн ед., 2007-2015 гг.²

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. 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 России³.

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

¹Отчет о платежных системах за 2014 год Банка международных расчетов. URL: <https://www.bis.org/cpmi/publ/d142a.pdf> (дата обращения: 27.01.2016).

²Центральный банк Российской Федерации [Электронный ресурс]. URL: <http://www.cbr.ru/> (дата обращения: 27.10.2016).

³Отчет о платежных системах за 2014 год Банка международных расчетов...

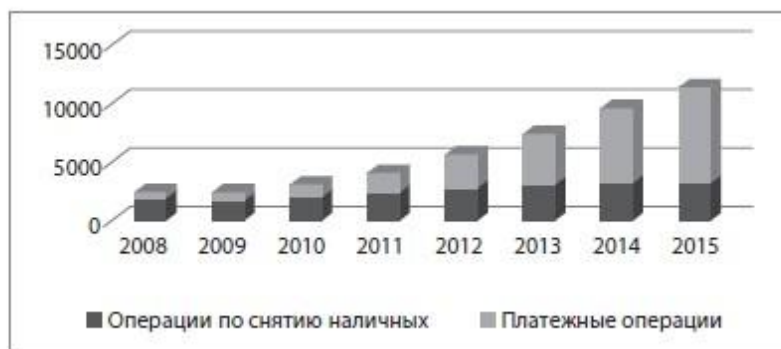


Рис. 2. Количество операций с электронными платежными пластиковыми картами, эмитированными в Российской Федерации, млн ед., 2007-2015 гг.

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)¹ 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)².

Несмотря на быстрый рост данного рынка, существует ряд проблем, препятствующих его развитию. Эти проблемы могут быть раз-

¹ 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).

²Национальная система платежных карт Российской Федерации. URL: <http://www.nspk.ru/> (дата обращения: 27.10.2016).

делены на две группы: проблемы, связанные с состоянием российской инфраструктуры, и проблемы, вызванные введением экономических санкций США, Евросоюзом и рядом других стран в 2014 году.

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.)¹.

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.²

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 «MasterCard» 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 «MasterCard»: «Генбанк», «Крайинвестбанк», банк «Верхневолжский», «Севастопольский морской банк» – в связи с работой в Крыму; «Инресбанк» и

¹Отчет о платежных системах за 2014 год Банка международных расчетов.
URL: <https://www.bis.org/cpmi/publ/d142a.pdf> (дата обращения: 27.10.2016).

²Национальная система платежных карт Российской Федерации.
URL: <http://www.nspk.ru/> (дата обращения: 27.10.2016).

«Мособлбанк» – из-за причастности к «СМП Банку». Помимо этого, «Visa» и «MasterCard» 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 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»¹.

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 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.

¹Национальная система платежных карт Российской Федерации. URL: <http://www.nspk.ru/> (дата обращения: 27.01.2016).

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 проектов¹.

¹ Там же.

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 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. Анализ рисков в деятельности банков в целях предупреждения угроз экономической безопасности в финансово-кредитной сфере

На современном рубеже становления экономики в условиях обострения конкурентной борьбы внимание к банковским рискам возрастает. В условиях нестабильности экономической конъюнктуры руководство любого банка понимает, что банковской деятельности, как и любой другой, присущ риск¹.

В соответствии с Положением Центрального Банка России от 16 декабря 2003 года №242-П «Об организации внутреннего контроля в кредитных организациях и банковских группах» под банковским риском понимается свойственная банковской деятельности возможность (вероятность) несения кредитной организацией потерь и (или) смещения в худшую сторону ликвидности вследствие наступления неблагоприятных событий, связанных с внутренними причинами (сложность организационной структуры, уровень и степень профессиональной квалификации служащих, организационные изменения и конфигурации, текучесть сотрудников и т.д.) и (или) внешними причинами (изменение экономических условий деятельности кредитной организации, используемых технологий и т.д.).

Банковский риск – это не имманентно присущее банку свойство, не столько неизбежность негативного хода событий, сколько деятельность, которая может привести к достижению отрицательного результата.

Далее рассмотрим оценку банковских рисков в соответствии с принятой методикой оценки соответствия безопасности банковской системы Российской Федерации требованиям СТО БР ИББС-1.0-2014.

¹ Бочаров О.А. Формирование основ экономической безопасности банковской деятельности: автореф. дис. ... канд: экон. наук. М., 2013. С.83.

Оценка текущего уровня безопасности организации определяется с помощью групповых и частных показателей безопасности, позволяющих оценить степень выполнения требований безопасности ИБ СТО БР ИББС-1.0 для следующих областей:

- обеспечение безопасности при назначении и распределении ролей и обеспечении доверия к персоналу;
- обеспечение безопасности на стадиях жизненного цикла АБС;
- обеспечение безопасности при управлении доступом и регистрацией;
- обеспечение безопасности средствами антивирусной защиты;
- обеспечение безопасности при использовании ресурсов сети Интернет;
- обеспечение безопасности при использовании средств криптографической защиты информации;
- обеспечение безопасности банковских платежных технологических процессов;
- обеспечение безопасности банковских информационных технологических процессов;
- обработка персональных данных в организации БС РФ;
- обеспечение безопасности банковских технологических процессов, в рамках которых обрабатываются персональные данные.

Специализация банка на определенных видах услуг оказывает значительное влияние на его профиль рисков. К примеру, банк, активно работающий на рынке кредитования компаний нефинансового сектора, на межбанковском рынке, на рынке потребительского кредитования, будет подвержен в большей степени кредитным рискам, а банк, вкладывающий значительные ресурсы в фондовый рынок, – рыночному риску. Минимизировать риски с учетом влияния внешней среды и специфики работы банка обязана система управления рисками, наличие которой является неотъемлемым условием успешной деятельности кредитной организации.

О.И. Лаврушин отмечает, что оценка деловой репутации банка клиентами и партнерами имеет самое непосредственное и прямое от-

ношение к деловым связям банка. При этом деловая репутация считается наиболее уязвимой из числа его нематериальных активов.

Деловая репутация банка – это качественная оценка заинтересованными сторонами финансовой устойчивости, качества и свойств предоставляемых услуг и иной деятельности банка, а также деятельности его реальных владельцев и аффилированных лиц, способная оказать воздействие на финансовый результат банка¹.

Возникновение правового риска может быть обусловлено как внешними, так и внутренними факторами.

К внутренним причинам относятся:

- нарушение кредитной организацией законодательства РФ, в том числе по идентификации и изучению клиентов, установлению и идентификации выгодоприобретателей (лиц, к выгоде которых действуют клиенты), учредительных и внутренних документов кредитной организации;

- несоответствие внутренних документов кредитной организации законодательству РФ, а также неспособность кредитной организации своевременно приводить свою деятельность и внутренние документы в соответствие изменениям законодательства;

- неэффективная организация правовой работы, приводящая к правовым ошибкам в деятельности кредитной организации вследствие действий сотрудников или органов управления кредитной организации;

- нарушение или несоблюдение кредитной организацией условий и обозначенных критериев в договорах;

- недостаточная проработка кредитной организацией правовых вопросов при разработке и внедрении новых технологий и условий проведения банковских операций и других сделок, финансовых инноваций и технологий.

К внешним причинам возникновения правового риска относятся:

¹ Лясковский Е.Н. Организационно методические основы обеспечения экономической безопасности банковской сферы // Проблемы управления рисками в техносфере. 2009. № 1(9) 2(10). С.90.

– несовершенство правовой системы (отсутствие достаточного правового регулирования, противоречивость законодательства РФ, пробелы и коллизии в праве, частая подверженность изменениям, в том числе в части несовершенства методов государственного регулирования и (или) надзора, некорректное применение законодательства иностранного государства и (или) норм международного права), невозможность решения отдельных вопросов путем переговоров и как результат – обращение кредитной организации в судебные инстанции для их урегулирования;

– нарушения клиентами и контрагентами кредитной организации условий договоров;

– нахождение кредитной организации, ее филиалов, дочерних и зависимых организаций, клиентов и контрагентов под юрисдикцией различных государств.

Допустимый размер рисков различного вида должен фиксироваться через стандарты (лимиты и нормативные показатели), отражаемые в документе о политике банка на предстоящий период. Эти стандарты определяются на основе бизнес-плана. К их числу можно отнести:

– долю отдельных сегментов в портфеле активов банка, кредитном портфеле, торговом и инвестиционных портфелях;

– соотношение кредитов и депозитов;

– уровень показателей качества кредитного портфеля;

– долю просроченных и пролонгированных ссуд;

– долю МБК в ресурсах банка;

– уровень показателей ликвидности баланса и достаточности капитальной базы;

– стандартные требования к заемщикам банка (по длительности участия в данной сфере бизнеса, соответствию среднеотраслевым экономическим показателям, ликвидности баланса и т.д.) .

Критерии оценки степени риска могут быть как общими, так и специфичными для отдельных видов риска.

Наиболее разработаны в экономической литературе критерии оценки кредитного риска.

Оценка финансового состояния заемщика перед принятием решения о предоставлении ссуды, а также для проведения текущего мониторинга финансового положения проводится банками на основании бухгалтерской отчетности в полном объеме, составленной в соответствии с образцами форм приказа Минфина РФ от 02.07.2010 г. №66н «О формах бухгалтерской отчетности организаций».

Положение №254-П «О порядке формирования кредитными организациями резервов на возможные потери по ссудам, по ссудной и приравненной к ней задолженности» определяет лишь минимальные требования к подходам оценки финансового положения заемщика, а разработку самих методик возлагает на саму кредитную организацию.

Согласно требованиям действующей редакции Положения №254-П и Указания №2155-У применяемая кредитной организацией методика анализа и оценки финансового положения заемщиков – юридических лиц должна обеспечивать комплексность и объективность проводимого анализа, учитывать отрасль (сферу) деятельности заемщика, содержать перечень сведений, необходимых для оценки рисков заемщика (включая функционирование рынка (рынков), на котором (которых) работает заемщик), основных используемых источников информации и критерии оценки ее достоверности, а также предусматривать порядок расчета и оценки показателей:

- стабильности производства;
- чистых активов;
- рентабельности;
- платежеспособности (включая порядок осуществления анализа причин возникновения неплатежеспособности);
- дебиторской и кредиторской задолженности (включая оценку безнадежной к погашению дебиторской задолженности, внешних обязательств заемщика, включая просроченную кредиторскую задолженность, а также критерии существенности допущенной просрочки);
- скрытых потерь (неликвидных запасов готовой продукции и др.);
- других показателей, устанавливаемых кредитной организацией самостоятельно.

При анализе отчетности и иной информации с целью оценки финансового положения заемщика следует учитывать также рекомен-

дации Банка России, данные в письме №43-Т от 04.04.2011 г. «О некоторых вопросах оценки качества ссуд».

В соответствии с положениями данного письма, при анализе банком информации и отчетности заемщика в целях оценки его финансового положения целесообразно рассматривать наличие фактов, свидетельствующих об отсутствии у заемщика - юридического лица реальной деятельности в сфере производства, выполнения работ / услуг, либо осуществления такой деятельности в объемах незначительных и не сопоставимых с размером предоставляемой ссуды¹.

В условиях конкуренции банку не всегда приходится иметь дело только с надежными и материально состоятельными клиентами. Как правило, наоборот, среди кредитополучателей банка преобладают люди, которые испытывают финансовые затруднения.

Поэтому умение кредитных специалистов проанализировать и оценить сильные и слабые стороны заемщика в отношении принятых долговых обязательств – основная задача любого банка, т.к. процесс кредитования неразрывно связан с действием всевозможных факторов риска, способных доставить банку финансовые затруднения, в том числе и мошенничество при получении кредита.

Введение в заблуждение потенциальными ссудозаемщиками сотрудников банка осуществляется разными методами, которые могут быть объединены в две группы:

А) путем использования специально созданных для хищения кредитных ресурсов фиктивных организаций².

Выделяют следующие типичные приемы создания фиктивных организаций:

1. Создание организации по подлинным документам лицами, не намеревающимися заниматься хозяйственной деятельностью. Руководители такой организации после получения кредита и его присвоения скрываются от кредиторов.

2. Внесение в учредительные документы, необходимые для регистрации организации, искаженных сведений об учредителях (руко-

¹ Кирюшин А.В., Плотников С.В. Правовые аспекты обеспечения экономической безопасности Российской Федерации //История государства и права. 2014. № 9. С.69.

² Там же.

водителях). Часто для этих целей используются утраченные либо похищенные паспорта граждан. После регистрации фирмы и получения кредита мошенник скрывается.

3. Изготовление подложных уставов, регистрационных и иных документов с использованием подлинных печатей, ксерокопий действительных документов и иным образом.

4. Регистрация организаций на фиктивные адреса. Возможны различные модификации данного приема: при регистрации лжефирм указывается несуществующий адрес; указанная в качестве адреса квартира меняется, продается; перемена арендуемых в качестве офисов помещений без уведомления регистрационных, налоговых органов, контрагентов по сделкам; заключение за денежное вознаграждение устных соглашений с владельцами квартир об использовании их адреса в качестве юридического адреса фиктивного предприятия.

5. Использование реквизитов ликвидированных организаций с получением путем обмана согласия их руководителей.

6. Похищение регистрационных документов действующих организаций и открытие по ним расчетных счетов в банке.

7. Создание либо использование в целях хищения кредита легальных организаций под давлением организованных преступных групп. Руководители подобных организаций, получив по требованию преступников банковскую ссуду, передают ее преступникам либо непосредственно, либо под видом выполнения обязательств по сделке.

8. Регистрация организаций по ненадлежаще оформленным, недействительным документам по сговору с должностными лицами государственных органов, осуществляющих регистрацию организаций.

9. Использование для хищения кредитных ресурсов специально созданных организаций, находящихся под контролем руководителя фирмы-ссудополучателя или связанных с ним лиц. Одна из возможных схем хищения кредита выглядит следующим образом: деньги тратятся не на цели, обозначенные в кредитном договоре (например, на развитие производства), а на приобретение различных ценностей для фирмы – получателя кредита (машин, дорогой оргтехники и т.п.). В дальнейшем руководитель фирмы, имея намерение присвоить полученные средства, учреждает ряд новых коммерческих структур на

свое имя или на имя своих соучастников и передает эти ценности с баланса структуры – получателя кредита на балансы новых структур. Тем самым затрудняется установление принадлежности ценностей и их изъятие в целях возмещения ущерба.

С целью избежания ответственности на должности руководителей организаций или главных бухгалтеров подбираются некомпетентные лица, часто судимые либо страдающие психическими заболеваниями, которые за определенное вознаграждение подписывают документы, необходимые для реализации преступных схем:

Б) путем фальсификации документов и применения иных приемов обмана, вследствие чего кредитные офицеры вводятся в заблуждение относительно возможностей и перспектив возврата полученных средств и качества обеспечения кредита.

Важным элементом преступных схем по присвоению кредитных ресурсов банков является введение банковских служащих в заблуждение относительно наличия либо качества обеспечения кредита и, тем самым, относительно возможности исполнения должником своих обязательств в случае невозврата кредита.

Можно выделить следующие способы злоупотреблений при использовании банковских гарантий и поручительств¹:

1. Фальсификация. Объектом фальсификации часто являются гарантийные письма. Для изготовления поддельных гарантийных писем используются следующие приемы:

1) использование похищенных бланков организаций с оттисками печатей;

2) использование похищенных либо утерянных печатей;

3) выполнение через сообщников оттисков настоящей печати на подложное гарантийное письмо одновременно с подделкой подписей руководителей организаций;

4) использование смонтированных ксерокопий бланков документов, оттисков печатей и подписей руководящих лиц;

¹ Волженкин Б.В. Преступления, связанные с нарушением установленного порядка осуществления предпринимательской и иной экономической деятельности // Новое уголовное право России. Особенная часть: учеб. пособие. М., 2011. С.47.

5) использование подложных писем, заверенных оттисками печатей со старыми названиями, реквизитами банком или их филиалов.

2. Злоупотребления при использовании залога в качестве обеспечения кредита. Типичными вариантами подобных действий являются:

1) представляется в качестве залога непомноценного имущества, действительная стоимость которого не соответствует заявленной;

2) предоставление в качестве залога имущества, не находящегося в собственности получателя кредита;

3) предоставление в качестве залога имущества, на которое не может быть

обращено взыскание;

4) неоднократный залог одного и того же имущества.

Используются также иные приемы обмана при осуществлении ссудных операций:

1) при заключении кредитных договоров изготавливаются подложные документы, создающие видимость финансовой состоятельности (в частности, представляются ложные балансы), недостоверные бизнес-планы и технико-экономические обоснования предстоящих инвестиций за счет кредитных средств;

2) фабрикуются подложные документы в обоснование кредитного запроса, договоры о якобы заключенных сделках;

3) представляются подложные документы на право получения кредита на льготных условиях, по заниженной процентной ставке.

Таким образом, мошенничество организаций с финансовыми и учредительными документами не позволяет кредитным организациям достоверно оценить риски кредитования.

2.2. Уголовно-правовая характеристика и проблемы квалификации мошенничества, совершаемого в банковской сфере с использованием электронных платежных пластиковых карт¹

Как указывалось выше, мошенничество, совершаемое с использованием пластиковых платежных карт, входит в главу 21 УК РФ, где указаны все виды и формы преступлений против собственности. Далее немного остановимся на общей характеристике преступлений против собственности. Родовым объектом преступлений против собственности, представленных в гл. 21 УК РФ, являются законные права и интересы физических и юридических лиц в экономической сфере. Видовым объектом преступлений против собственности выступают правоотношения в сфере собственности в части владения, пользования и распоряжения имущественными ценностями (благами). Непосредственным объектом преступлений против собственности выступают конкретные правоотношения в сфере собственности, имущественных благ и интересов. Объективная сторона рассматриваемой категории преступлений выражается в форме противоправного деяния, влекущего или создающего угрозу причинения имущественного вреда, материального ущерба собственнику или иному владельцу имущества. По своей юридической конструкции большая часть составов преступлений против собственности являются материальными, т. е. считаются оконченными с момента наступления общественно опасных последствий. К числу материальных относятся составы преступлений, предусмотренных ст. 158–161, 164, 165, 167, 168 УК РФ. Формальной юридической конструкцией отличается такое преступление, как неправомерное завладение автомобилем или иным транспортным средством (ст. 166 УК РФ). Усеченными признаются составы разбоя (ст. 162 УК РФ) и вымогательства (ст. 163 УК РФ).

¹При написании данного параграфа использованы материалы: Южин А.А. Мошенничество и его виды в российском уголовном праве: дис. ... на соискание ученой степени кандидата юридических наук: 12.00.08 – уголовное право и криминология; уголовно-исполнительное право. М: МГЮУ им. О.Е. Кутафина (МГЮА), 2016 С. 153-164.

Субъективная сторона данной категории преступлений всегда отличается умышленной формой вины и в большинстве случаев предполагает наличие корыстной цели и соответствующей мотивации.

Субъектом преступлений, предусмотренных ст. 159–159⁶, 160, 164, 165, 168, ч. 1 ст. 167 УК РФ, выступает вменяемое физическое лицо, достигшее 16 лет. Применительно к деяниям, названным в ст. ст. 158, 161, 162, 163, 166, ч. 2 ст. 167 УК РФ, возрастной предел уголовной ответственности снижен законодателем до 14 лет.

Термин «хищение» определяется законом как противоправное безвозмездное изъятие и (или) обращение чужого имущества в пользу виновного или других лиц, совершаемое с корыстной целью (примечание 1 к ст. 158 УК РФ). Хищение характеризуют следующие признаки: предмет, чужеродность похищаемого имущества, сложный механизм хищения, противоправность, безвозмездность, а также причинение ущерба собственнику или иному владельцу имущества.

Объектом хищений выступают отношения собственности в части реализации правомочий по владению, пользованию и распоряжению имущественными ценностями (благами). Предметом хищения выступает чужое имущество, понятие которого, в свою очередь, складывается из двух компонентов: материального (вещного) и экономического. Материальный компонент заключается в том, что чужое имущество должно обладать признаками вещи, предмета материального мира. Экономический компонент предполагает наличие у предмета хищения определенной товарно-денежной стоимости.

Сложность механизма хищения заключается в осуществлении преступником таких противоправных действий, как изъятие и обращение чужого имущества.

Термин «изъятие» означает противоправное отторжение, обособление части имущества от общей имущественной массы, находящейся в обладании собственника или лица, в ведении которого оно находится.

Термин «обращение» в данном контексте определяется как незаконное использование или владение виновным или третьими лицами имуществом собственника, т. е. фактическое осуществление ука-

занными лицами правомочий собственника в отношении чужого имущества.

Термин «противоправность» характеризуется следующими чертами: во-первых, осуществлением хищения противозаконным способом, т. е. запрещенным действующим законодательством; во-вторых, отсутствием у виновного каких-либо законных прав на похищаемое имущество.

Термин «безвозмездность» означает, что собственнику взамен изымаемой вещи не предоставляется равноценный эквивалент стоимости похищаемого имущества. Частичное возмещение его стоимости собственнику является недостаточным для исключения состава хищения.

Причинение ущерба собственнику или иному владельцу имущества заключается в фактическом уменьшении в результате хищения общего количества имущества, принадлежащего собственнику или иному законному владельцу.

Хищения разграничивают в зависимости от такого критерия, как способ совершения данного противоправного деяния. Существует 6 форм хищения: кража, мошенничество, присвоение, растрата, грабеж, разбой. Составы всех этих хищений, за исключением разбоя, по своей юридической конструкции являются материальными, т. е. оконченными в момент наступления общественно опасных последствий в виде причинения имущественного ущерба.

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 персональных данных держателя карты; сложностью 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 мошенничество с использованием платежных карт (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 право¹. Подобные составы давно включены в уголовное законодательство многих зарубежных государств.

Согласно статистическим данным Центрального банка РФ, за последние 7 лет число эмитированных банковских карт возросло вдвое. 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%². 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 их использованием» (далее положение ЦБ от 24.12.2004 № 266), кредитная организация осуществляет эмиссию расчетных (дебетовых) карт, кредитных карт и предоплаченных для следующих категорий лиц: физических и юридических лиц, индивидуальных предпринимателей. Расчетная небанковская кредитная организация осуществляет эмиссию расчетных (дебетовых) карт для юридических лиц, индивидуальных предпринимателей, предоплаченных карт - для физических лиц, юридических лиц, индивидуальных предпринимателей³. Платежная небанковская кредитная организация осуществляет эмиссию предоплаченных карт для физических лиц, юридических

¹Добрынин Ю. Классификация преступлений, совершаемых в сфере компьютерной информации. URL: http://www.russianlaw.net/law/computer_crime/a158/ (дата обращения: 04.11.2016).

²По данным Центрального Банка Российской Федерации [Электронный ресурс] URL: <https://www.cbr.ru/>. Проверено на 30.10.2016.

³Положение об эмиссии платежных карт и об операциях, совершаемых с их использованием утв. Банком России 24.12.2004 № 266-П: ред. от 14.01.2015 // Вестник Банка России. 2005. № 17.

лиц, индивидуальных предпринимателей, с помощью инструментария которого возможно выполнять следующие действия: получать денежные средства на руки как в кредитных учреждениях, так и через программно-технический комплекс, предназначенный для автоматизированной выдачи и приема наличных денежных средств, так называемых банкоматов и банковских автоматов; а также возможно использовать ее в качестве средства платежа, в том числе и через сеть Интернет.

Платежная карта в диспозиции ст. 159.3 УК РФ выступает в качестве родового понятия, объединяющего конкретные виды карт: расчетные кредитные 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 обозначенных пределах. В соответствии с положением Центробанка от 24.12.2004 № 266 предусматриваются два порядка осуществления операций с использованием таких карт. В первом случае денежные средства поступают непосредственно на банковский счет клиента. Во втором же случае последние предоставляются клиенту с использованием банковского счета. В случае, если получатель кредитной карты не является гражданином России, то денежные средства ему предоставляются в иностранной валюте, в остальных случаях физическим лицам предусматривается выдача в валюте РФ¹. Важным условием предоставления такой карты является обязательность возврата клиентом денежных средств кредитной организации.

Расчетная карта, или по - другому 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 предостав-

¹Положение об эмиссии платежных карт и об операциях, совершаемых с их использованием ...

ленных держателем денежных средств кредитной организации-эмитенту в соответствии с требованиями ФЗ от 27.06.2011 № 161 «О национальной платежной системе»¹ (далее ФЗ от 27.06.2011 № 161) (телефонные карты, электронный проездной и т.д.).

Для осуществления платежей при помощи электронных средств платежа не нужно заводить отдельный банковский счет. 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, MasterCard, DinersClub, AmericanExpress, JCB и ChinaUnionpay).

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 и владельца карты. В качестве держателя карты выступает 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-эмитент не имеет на них никаких прав. Вступившее в законную силу решение суда является легитимным основанием для приостановления операций по счету. В качестве собственника, выступает банк-эмитент. При этом банк-эмитент не пользуется полномочиями собственника, обозначенными в ст. 209 ГК РФ, то

¹Положение об эмиссии платежных карт и об операциях, совершаемых с их использованием...

есть у него нет права пользования, распоряжения и владения в отношении денежных средств, находящихся на банковском счете. Эти права распространяются лишь на саму карту как на предмет материального мира, но не в отношении ее содержимого, т.е. того счета, к которому она привязана, если это только на счете этой карты не находятся собственные средства данной кредитной организации. В ряде случаев признано необходимым выделять владельца карты, т.е. то лицо, в чьем владении находится карта, так как держатель и владелец карты могут быть разными лицами. 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». Существует специальная процедура, в соответствии с которой каждой банковской карте присваивается определенный номер, имя держателя и срок действия. Вся необходимая информация о держателе карты, наносится 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. Следовательно, норма о мошенничестве с использованием пластиковых карт (ст. 159.3 УК РФ) призвана обеспечивать не только охрану собственности, а также нормальную деятельность банков и иных кредитных организаций, связанную с беспрепятственным доступом клиентов к своим денежным средствам в необходимый момент.

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. Так, ст. 159.3 УК РФ призвана защитить отношения собственности, имущественные интересы потерпевшего, а также отношения, обеспечивающие нормальный порядок функционирования расчетов по операциям с использованием платежных карт.

Диспозиция рассматриваемой нами нормы имеет бланкетный характер, так как сфера противоправного использования платежных карт - это область специальных познаний.

Специалистами указывается, что данный состав преступления характеризуется специальным предметом - поддельной или принадлежащей другому лицу платежной картой.¹ Однако нам ближе точка зрения, согласно которой предметом посягательства в анализируемой норме выступает чужое имущество, включающее денежные средства, находящиеся на банковском счете, наличные денежные средства, товары, оплаченные с предоплаченной карты,² 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, а не саму карту, которая представляла бы для него какую -нибудь ценность. В данном случае карта, по нашему мнению, выступает необходимым средством совершения преступления.

Как уже было отмечено, платежная карта выступает средством совершения преступления, с помощью которой субъект мошенничества пытается получить доступ к денежным средствам. Когда происходит обман представителя какой-либо организации, никто не удостоверяет, является ли данное лицо правомочным держателем карты или нет. Списание денежных средств происходит до того момента,

¹ Аналитический обзор статей об ответственности за мошенничество // Официальный сайт справочной правовой системы «КонсультантПлюс» URL: <http://www.consultant.ru/law/review/1657522.html>.

² Александрова И.А. Новое уголовное законодательство о мошенничестве // Юридическая наука и практика. Вестник Нижегородской академии МВД России. 2013. № 21. С.54-62.

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 то, к чему он может открыть доступ¹. Определенную аналогию с мошенничеством с использованием платежных карт тоже можно провести.

Как было указано выше, объективная сторона преступления включает в себя обман, в результате которого уполномоченный работник кредитной, торговой или иной организации, будучи введенным в заблуждение относительно того факта, что перед ним находится законный 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.

Объективная сторона преступления включает в себя пять обязательных признаков.

Первый признак – общественно опасное действие, выражающееся в хищении чужого имущества.

Второй признак – средство совершения преступления, в качестве которого могут выступать:

- 1) поддельная кредитная, расчетная или иная платежная карта;
- 2) кредитная, расчетная или иная платежная карта, принадлежащая другому лицу (указанный вид мошеннических действий имеет место, например, в случаях, когда лицо, используя банковскую карту для оплаты товаров или услуг в торговом или сервисном центре, ставит подпись в чеке на покупку вместо законного владельца карты либо предъявляет поддельный паспорт на его имя).

Определение в рамках ст. 159³ УК РФ средства преступления как конструктивного признака влечет необходимость при квалификации устанавливать, что соответствующее противоправное деяние было совершено посредством использования расчетной или иной пла-

¹Боровых Л.В., Корепанова Е.А. Проблема квалификации хищения с использованием банковских карт // Российский юридический журнал. 2014. № 2. С. 86.

тежной карты. Изложенное исключает возможность квалификации по рассматриваемой норме уголовного закона деяния, содержанием которых является неправомерное использование данных, содержащихся на пластиковых картах.

Например, нередко злоумышленники посредством применения скимминговых устройств получают информацию по карте и впоследствии распоряжаются находящимися на ее счете средствами при оплате товаров и услуг через Интернет без непосредственного использования пластиковой карты. В таких ситуациях отсутствие применения предмета преступления, указанного в ст. 159³ УК РФ, влечет квалификацию деяния по ст. 159⁶ УК РФ «Мошенничество в сфере компьютерной информации». Еще одним аргументом, свидетельствующим о необходимости квалификации действия злоумышленников в ситуациях, аналогичных изложенному примеру, является отсутствие обмана уполномоченного работника торговой или обслуживающей организации, так как операция совершается удаленно.

Третий признак – способ совершения преступления, состоящий в обмане уполномоченного работника кредитной, торговой или иной организации.

Под обманом понимается способ извлечения имущества или права на него посредством намеренного искажения истины, сознательного сообщения заведомо ложных сведений (утверждения о фактах отсутствующих или отрицания обстоятельств существующих) с целью завладения чужим имуществом (активный обман). При активном обмане заблуждение собственника (или иного владельца) может быть вызвано также предоставлением фальсифицированного товара или иного предмета сделки, использованием обманных приемов при расчете за товары или услуги, игрой в азартные игры, имитацией кассовых расчетов либо иными умышленными действиями, направленными на введение владельца имущества или иного лица в заблуждение. Обман может выражаться и в умолчании об истинных фактах (сокрытии истины), сообщение о которых по обстоятельствам дела вменяется виновному в обязанность. В этом случае именно бездействие виновного (пассивный обман) приводит жертву в состояние заблуждения об истинных его целях.

Мошеннический обман состоит в воздействии на сознание потерпевшего и требует участия самой жертвы (личного или через представителей) в передаче имущественного блага виновному. При уголовно-правовой оценке соответствующих деяний, предметом которых являются пластиковые карты, необходимо учитывать, что в соответствии с правилами квалификации в случаях, когда работник кредитной, торговой или иной организации не задействован в расчетной операции с похищенной или поддельной платежной картой, то содеянное виновным подлежит квалификации по ст. 158 УК РФ («Кража»). При этом нужно руководствоваться разъяснением постановления Пленума Верховного Суда РФ, данным им в п. 13 «О судебной практике по делам о мошенничестве, присвоении или растрате», согласно которому «...не образует состава мошенничества хищение чужих денежных средств путем использования заранее похищенной или поддельной кредитной (расчетной) карты, если выдача наличных денежных средств осуществляется посредством банкомата без участия уполномоченного работника кредитной организации. В этом случае содеянное следует квалифицировать по соответствующей части статьи 158 УК РФ. Хищение чужих денежных средств, находящихся на счетах в банках, путем использования похищенной или поддельной кредитной либо расчетной карты следует квалифицировать как мошенничество только в тех случаях, когда лицо путем обмана или злоупотребления доверием ввело в заблуждение уполномоченного работника кредитной, торговой или сервисной организации...».

Сам обман как способ совершения указанного преступления не имеет каких-либо особенностей по сравнению с общим понятием, характеризующим любое мошенническое хищение.

Четвертый признак – общественно опасное последствие в виде прямого ущерба, причиненного собственнику.

При квалификации содеянного необходимо устанавливать наличие реального ущерба, являющегося следствием противоправного изъятия чужого имущества, так как он в соответствии с примечанием к ст. 158 УК РФ является конструктивным признаком любой формы хищения, в том числе мошенничества.

Пятый признак – наличие причинно-следственной связи между противоправным действием и наступившим в результате этого имущественным вредом.

К уполномоченным работникам кредитной, торговой или иной организации относятся лица, являющиеся работниками соответствующих организаций и фактически от её имени осуществляющие различного рода операции. Например, такие как продажа товаров, оплата работ (услуг), прием и выдача денежных средств с использованием контрольно-кассовой или банковской техники, оснащенной возможностью принимать к обслуживанию платежные карты. Не имеет значения то, были ли они назначены на свою должность с нарушением закона или локальных актов организации. Даже если уполномоченный работник не совершил действий с целью идентификации владельца карты (не попросил поставить подпись на чеке, предоставить паспорт и т.п.), совершенное деяние все равно квалифицируется как мошенничество с использованием платежных карт.

Общественная опасность рассматриваемого преступления выражается в том, что оно посягает не только на отношения собственности, в частности, имущественные интересы потерпевшего, но и на отношения, обеспечивающие нормальный порядок расчетов по операциям с использованием платежных карт.

Основным непосредственным объектом преступления являются общественные отношения, обеспечивающие охрану прав собственности кредитной, торговой или иной организации, а также владельцев кредитных, расчетных или иных платежных карт.

В соответствии с положениями действующего законодательства кредитными организациями являются юридические лица, которые для извлечения прибыли как основной цели своей деятельности на основании специального разрешения (лицензии) Центрального банка Российской Федерации (Банка России) имеют право осуществлять банковские операции^[8].

Торговые организации представляют собой совокупность упорядоченных и взаимодействующих между собой организационных элементов (торговых предприятий, организаций, подсистем), образующих

целостную систему, а также комплекс целенаправленных организующих действий, обеспечивающих функционирование торговли.

Под иными организациями следует понимать структуры, не относящиеся ни к кредитным, ни к торговым организациям (например, сервисные центры, рекламные агентства и т. п.).

Дополнительным непосредственным объектом преступлений, выраженных в мошенничестве с использованием платежных карт, выступают общественные отношения, регулирующие стабильное функционирование национальной платежной системы

Субъектом преступления является достигшее возраста (16 лет) наступления уголовной ответственности вменяемое физическое лицо. Следовательно, в данной статье предусмотрен общий субъект преступления.

Субъективная сторона преступления характеризуется прямым умыслом, так как злоумышленник осознает общественную опасность совершаемым им мошеннических операций с использованием платежных карт, предвидит наступление общественно опасных последствий и желает их наступления.

Законом предусмотрены квалифицированные составы мошенничества с использованием платежных карт. Часть 2 комментируемой статьи включает в себя совершение мошенничества группой лиц по предварительному сговору и с причинением значительного ущерба гражданину. В части 3 и 4 указаны особо квалифицированные составы данного преступления: это, во-первых, деяния, совершенные с использованием виновными своего служебного положения, а равно в крупном размере; и во-вторых, деяния, совершенные организованной группой либо в особо крупном размере.

Согласно примечанию к ст. 159.1 УК РФ крупным размером в ст. 159.3 УК РФ признается стоимость похищенного имущества, превышающая 1500000 рублей, а особо крупным размером – превышающая 6 000 000 рублей.¹

¹ Теоретические основы квалификации преступлений, предусмотренных ст. 159-159.6 УК РФ: методические рекомендации / М.Р. Гарафутдинов и др. Казань: КЮИ МВД России, 2014. – 75 с.

Стоит отметить, что в случае хищения незначительной суммы и при отсутствии квалифицирующих признаков действия правонарушителей не могут рассматриваться как уголовно наказуемое деяние ввиду его малозначительности и подлежат квалификации по ст. 7.27 КоАП РФ.

Статья 7.27 КоАП РФ «Мелкое хищение, -

Мелкое хищение чужого имущества путем кражи, мошенничества, присвоения или растраты при отсутствии признаков преступлений, предусмотренных частями второй, третьей и четвертой статьи 158, частями второй, третьей и четвертой статьи 159, частями второй, третьей и четвертой статьи 159.1, частями второй, третьей и четвертой статьи 159.2, частями второй, третьей и четвертой статьи 159.3, частями второй и третьей статьи 159.4, частями второй, третьей и четвертой статьи 159.5, частями второй, третьей и четвертой статьи 159.6 и частями второй и третьей статьи 160 Уголовного кодекса Российской Федерации.

Примечание. Хищение чужого имущества признается мелким, если стоимость похищенного имущества не превышает одну тысячу рублей».

Мошенничество с использованием платежных карт рассматривается в ст. 159.3 УК РФ как форма хищения. Состав преступления носит материальный характер. Следовательно, преступление считается оконченным с момента, когда лицо, получив платежную карту, имело реальную возможность воспользоваться ею как средством платежа или обналичить денежные средства через уполномоченного сотрудника кредитной организации. В.В. Хилюта подчеркивает, что ущерб причиняется собственнику, когда имущество вышло из обладания субъекта¹. 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 приоб-

¹Хилюта В.В. Момент окончания хищения: практика применения теоретический концепций // Вестник БДУ. Сер. 3. 2010. № 3. С. 93.

рело поддельную карту, то речь может идти лишь о приготовлении к мошенничеству с использованием платежных карт.

Момент окончания данного вида мошенничества должен определяться правилом о моменте окончания мошенничества-хищения, т.е. если руководствоваться господствующей в настоящее время теорией «реальной возможности», виновное лицо должно путем обмана банковского или иного работника изъять денежные средства и получить возможность пользоваться или распоряжаться ими по своему усмотрению. Естественно, мы можем констатировать такую возможность, если лицо с похищенным имуществом выйдет за пределы организации (хотя вопрос о расстоянии, на которое необходимо скрыться, остается открытым, поскольку судебная практика не признает оконченное хищение в случае задержания на крыльце, вблизи и т.д.) либо распорядиться им внутри организации (например, произведет оплату каких-либо услуг).

Однако если представить ситуацию, что виновное лицо переведет данные деньги на счет, а по прошествии определенного времени (это могут быть минуты, часы, месяцы и т.д.) при выяснении обстоятельств счет будет заблокирован, сможем ли мы говорить об оконченном хищении? Думается, ответ на поставленный вопрос, судебная практика при использовании теории «реальной возможности» так и не даст, поскольку, с одной стороны, виновный произвел перевод денежных средств, с другой стороны, в случае блокировки счета он никогда данные деньги не получит.

Помимо изложенной проблемы разграничения состава кражи и мошенничества, казуистичной является сама формулировка диспозиции ст. 159.3 УК, предусматривающая сопряженность использования платежной карты с обманом. В правоприменительной практике появились трудности в разграничении и применении статьи в отношении определенных действий мошенничества с использованием платежных карт и мошенничества в сфере кредитования.

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 квартиры¹. 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. 159.1 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. 159.1 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 одинаковый, как основной, так и факультативный.

Определенные вопросы возникают с однозначным отнесением настоящего деяния к видам мошенничества.

В уголовном праве советского периода законодатель определял мошенничество как завладение личным имуществом граждан или приобретение права на имущество путем обмана или злоупотребления доверием. В п. 12 постановления от 5 сентября 1986 г. N 11 "О

¹ Приговор Ленинского районного суда г. Новосибирск от 04.03.2015. Дело № 1-39/2015 // URL: http://sudact.ru/regular/doc/ejbXHqxArFVE/?regularartxt=%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

судебной практике по делам о преступлениях против личной собственности" Пленум Верховного Суда СССР указал, что неотъемлемым признаком мошенничества является добровольная передача потерпевшим имущества или права на имущество виновному под влиянием обмана или злоупотребления доверием¹, когда у потерпевшего возникало чувство правомерной передачи своего имущества злоумышленнику. Те есть характерна была внешняя "добровольность" такой передачи.

В 1996 г. российский законодатель в ст. 159 УК РФ закрепил отличное от советского понятие мошенничества, под которым понимается хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием. Но все же, как и раньше, обман и злоупотребление доверием остаются обязательными признаками состава мошенничества. И поскольку вслед за принятием Уголовного кодекса РФ от Пленума Верховного Суда новых разъяснений по составу мошенничества не последовало, то на практике презюмировалась направленность обмана на потерпевшего.

С развитием экономики и технологий преступники стали использовать для незаконного изъятия имущества обман в отношении не только потерпевшего, но и третьих лиц, не обладающих правомочием распоряжения имуществом.

Для того чтобы разрешить возникшие противоречия, Пленум Верховного Суда РФ в постановлении от 27 декабря 2007 г. N 51 расширил содержание понятия обмана в составе мошенничества. Так, он разъяснил, что мошенничество совершается путем обмана или злоупотребления доверием, под воздействием которых владелец имущества или иное лицо либо уполномоченный орган власти передают имущество или право на него другим лицам либо не препятствуют изъятию этого имущества или приобретению права на него другими лицами. Заметим, что указанный круг лиц, на который согласно позиции Пленума ВС РФ может быть направлен обман при совершении мошенничества, выходит за рамки понятия потерпевшего, указанного

¹ О судебной практике по делам о преступлениях против личной собственности: Постановление Пленума Верхов. Суда СССР от 5 сентября 1986 г.: в ред. от 30.11.1990 // СПС "КонсультантПлюс" (док. недейств.).

в ст. 42 Уголовно-процессуального кодекса Российской Федерации, в соответствии с которым потерпевшим в преступлениях против собственности признается собственник либо владелец имущества. Следовательно, теперь обман в мошенничестве имеет более широкое содержание, в соответствии с которым он может быть направлен не только на потерпевшего, но и на третьих лиц, не обладающих правом распоряжения имуществом. Таким образом, на сегодняшний день судебная практика не придерживается традиционного подхода в понимании сущности мошенничества, согласно которому обман при совершении мошенничества должен быть направлен на потерпевшего и именно под его воздействием потерпевший должен сам добровольно передать свое или находящееся у него на законном основании имущество виновному.

Следовательно, с декабря 2012 г. законодатель официально, вопреки традиционному пониманию мошенничества и сложившейся практике, закрепил возможность направленности обмана при совершении мошенничества не только на потерпевшего, имеющего право распоряжения имуществом, но и на третьих лиц, которые таким правом не обладают, а выступают лишь в роли лиц, присутствующих при совершении преступления. Заметим, что на сегодняшний день это единственный состав мошенничества, в котором законодатель определил возможность направленности обмана не только на потерпевшего.

Представляется, что законодатель поспешил принимать статью в такой редакции, поскольку, как уже было указано выше, если при мошенничестве обман не направлен на потерпевшего, но при этом используется как средство облегчения доступа к имуществу и направлен на третьих лиц, то он не обуславливает передачу имущества. А поскольку он не обуславливает передачу имущества и не воздействует на волю лица, которое имеет право распоряжаться имуществом, то изъятие имущества происходит тайно или открыто, помимо воли собственника или иного владельца имущества и такие действия нельзя признать мошенничеством.

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. 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 совместно с ними проживать. Пытаясь проникнуть в квартиру в отсутствие 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 преступления¹.

В приведенном примере совершенно верно действия были квалифицированы как кража (п. «а», ч.3, ст. 158), поскольку способ совершения преступления был тайным². 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

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

²Как 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 (О судебной практике по делам о краже, грабеже и разбое: (постановление Пленума Верховного Суда РФ от 27.12.2002 № 29: ред. от 03.03.2015// Российская газета. 2003. № 9).

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 ею при оплате покупок в ООО «АЗС»¹.

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 РФ².

В соответствии с п. 16 постановления Пленума Верховного Суда РФ от 27.12.2002 № 29 разграничиваются понятия совокупности и продолжаемого хищения³. По мнению специалистов по вопросам мошенничества в банковской сфере с использованием электронных платежных пластиковых карт⁴, вышеприведенный пример указывает на тот факт, что виновный дважды стремился получить денежные средства Ф., при этом источник этих денежных средств был в обоих слу-

¹Приговор Ленинского районного суда г. Новосибирска от 05.05.2015. Дело № 1-420/2015 // URL: <http://sudact.ru/regular/doc/n1gmRVegiglg/>

²Приговор Кировского районного суда г. Кемерово, кемеровской области от 12.11.2015. Дело № 1-395/15 // URL: <http://sudact.ru/regular/doc/Y1E4KZB0MKoV/>

³От 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 (О судебной практике по делам о краже, грабеже и разбое: постановление Пленума Верховного Суда РФ от 27.12.2002 № 29: ред. от 03.03.2015 // Российская газета. № 9).

⁴Южин А.А. Мошенничество и его виды в российском уголовном праве: дис. ... на соискание ученой степени кандидата юридических наук: 12.00.08 – уголовное право и криминология; уголовно-исполнительное право. М.: МГЮУ им. О.Е. Кутафина, 2016. С. 153-162.

чаях 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 РФ¹.

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 РФ². Исполнение объективной стороны мошенничества с использованием платежных карт идет вразрез с концепцией добровольности передачи имущества собственником или иным владельцем.

Изложенные примеры наглядно свидетельствуют о том, что действующая редакция диспозиции ст. 159.3 УК дезориентирует правоприменителей, порождает избыточность уголовно-правового запрета, в связи с чем, на наш взгляд, подлежит исключению из УК.

Ввиду отсутствия единого мнения между судебными инстанциями, органами прокуратуры и органами, производящими предварительное следствие по данной категории дел, и достаточно определенной и регламентированной правовой базы, вследствие неоднозначности принимаемых решений правоприменитель Республики Татарстан старается не квалифицировать деяния по статье 159.3, чаще определяя их как кражу.

В заключение необходимо остановиться на вопросах рассогласованности санкций, содержащихся в нормах уголовного закона, ус-

¹Приговор Кировского районного суда г. Кемерово, Кемеровской области от 12.11.2015. Дело № 1-395/15 //

URL: <http://sudact.ru/regular/doc/Y1E4KZB0MKoV/>

²Южин А.А. Мошенничество и его виды в российском уголовном праве: дис. ...на соискание ученой степени кандидата юридических наук. Специальность: 12.00.08 – уголовное право и криминология; уголовно-исполнительное право. М.: МГЮУ им. О.Е. Кутафина, 2016. С. 161.

танавливающих ответственность за различные формы хищения чужого имущества.

Учитывая размеры санкций в специальных составах мошенничества, можно сделать вывод о том, что эти составы являются привилегированными по отношению к ст. 159 УК РФ. Привилегированный состав преступления предполагает, что деяние обладает признаками, понижающими его общественную опасность по отношению к простому составу. Одним из таких признаков выступают общественно опасные последствия. Чем они меньше, тем ниже общественная опасность преступления. Между тем, крупный и особо крупный размеры, предусмотренные в примечании к ст. 159¹ для этой нормы и для ст. 159³-159⁶ УК РФ, в четыре и в шесть раз, соответственно, превышают аналогичные размеры для мошенничества по ст. 159 УК РФ (двести пятьдесят тысяч рублей и полтора миллиона рублей – крупный размер; один миллион рублей и шесть миллионов рублей – особо крупный размер). В связи с этим логически трудно объяснить, почему при более высоких показателях последствий законодатель снижает санкции и признает составы преступлений привилегированными.

Именно указанный технико-юридический дефект, допущенный при конструировании санкций рассматриваемых норм, был положен в основу принятия постановления Конституционного Суда РФ от 11.12.2014 № 32-П «По делу о проверке конституционности положений статьи 159⁴ Уголовного кодекса Российской Федерации в связи с запросом Салехардского городского суда Ямало-Ненецкого автономного округа»^[13]. В соответствии указанным постановлением ряд положений ст. 159⁴ УК РФ признаны неконституционными. Резюмируя результаты рассмотрения дела, Конституционный Суд постановил в срок не позднее шести месяцев со дня провозглашения Постановления внести в Уголовный кодекс Российской Федерации изменения, обеспечивающие устранение выявленных неконституционных аспектов правового регулирования ответственности за мошенничество в сфере предпринимательской деятельности. Если по истечении шестимесячного срока со дня провозглашения постановления законодательные органы не внесут в УК РФ надлежащие изменения, статья 159⁴ утратит силу.

Учитывая тот факт, что при применении уголовного законодательства аналогия не допускается, приведенное решение высшей судебной инстанции не ограничивает применение иных норм, устанавливающих ответственность за специальные виды мошенничества, в том числе ст. 159³ УК РФ, однако если не будет принято соответствующих решений по оптимизации правового инструментария, нельзя исключать аналогичных решений Конституционного Суда России и в отношении указанной нормы уголовного закона.

2.3. Криминалистическая характеристика мошенничества с использованием платежных карт¹

Характеризующим любое преступление, а также его системообразующим и основополагающим элементом является способ его совершения. В.Д. Ларичев 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 преступления². Если правоохранительным органам известен способ совершения преступления, то эта информация влияет на качественность выдвижения версий и, следовательно, ведет к быстрому раскрытию противоправного деяния.

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 уполномочен-

¹Данный 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.

²Ларичев В.Д. Криминалистическая характеристика экономических преступлений и методика её построения // Научный портал МВД России. 2009. № 1. С. 111.

ного 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 мошенничества¹.

Способы совершения преступления. Итак, мошенничество состоит в завладении чужим имуществом обманным путем с использованием платежной банковской карты и заключается:

- 1) в использовании или попытке использования банковской карты не ее законным держателем;
- 2) использовании поддельной карты;
- 3) использовании для проведения операции вместо карты чистого пластика с выбитыми на нем данными с подлинной карты (так называемого *белого пластика*).

Способ данного преступления является полноструктурным, т.е. состоит из подготовки к совершению мошенничества, непосредственных действий, направленных на доведение своего умысла до конца и сокрытие своей преступной деятельности.

Согласно результатам исследования, подготовка к совершению хищения может включать следующие элементы, которые определяют форму и способ хищения:

1. Получение во владение самой банковской карты (поддельной или подлинной). Карта может быть получена как правомерно, например, держатель карты сам передал субъекту преступления банковскую карту для совершения по его просьбе каких-либо действий (4, 5 %), так и неправомочно (7, 7 %). Мы считаем, что в последнем случае применение формулировки «кража карты» не является точной, т.к. кража как форма хищения подразумевает совершение с корыстной целью противоправного безвозмездного изъятия и (или) обращение чужого имущества в пользу виновного (примечание к ст. 58 УК РФ), тогда как проведенное нами исследование показывает, что в 38 % случаев виновный незаметно для держателя возвращает карту ее держателю.

¹Волохова О.В. Расследование преступлений, связанных с обманом. М.: Юрлитинформ, 2008. С.33.

2. Получение информации об именах держателей карт и номерах банковских счетов для последующего изготовления поддельной банковской карты. Данное обстоятельство означает, что преступник или группа преступников должны обладать специальным оборудованием для изготовления карты, а иногда и документов (также подлинных или поддельных) на имя держателя карты – 2,53 %. В 9,7 % случаев преступник использует попавшие к нему в силу исполнения служебных обязанностей персональные данные для изготовления банковских карт на имя клиентов банка в целях последующего хищения денежных средств

3. Подбор соучастников в сервисных центрах (мерчантах), банках-эмитентах или банках-эквайерах или лица, которое будет осуществлять транзакцию или получение денежных средств в банкоматах – 5,67 %. Сюда же мы относим подбор лиц, которые не осведомлены о преступных замыслах преступника.

4. Подбор информации о держателях карт и наличии на принадлежащих им банковских счетах денежных средств в целях определения суммы хищения – 41,13 %.

5. Выбор будущей жертвы – держателя карты и сбор сведений об имеющихся на карте денежных средствах. Данный элемент отличается от предыдущего тем, что характерен для неквалифицированных «быстрых» одноэпизодных хищений – кражи или грабежа, тогда как подбор информации о держателях карт и наличии на принадлежащих им банковских счетах денежных средств типичны для длительного подготовительного этапа и продолжаемых хищений путем мошенничества или растраты – 13,47 %.

6. Выбор места хищения карты и места хищения денежных средств – 76,4 %. Мы рассматриваем место хищения карты не как место совершения самого преступления, а как место совершения подготовки к хищению, так как, по нашему мнению, хищение карты еще не является самым хищением с использованием банковской карты

7. Завладение мобильным телефоном или SIM-картой, подключенной к услуге «Мобильный банк». Преступники получают телефон или SIM-карту в свое владение путем хищения (кражи, грабежа, разбоя), находки утерянного телефона или SIM-карты, покупки (соглас-

но установленному порядку, через шесть месяцев после отказа от телефонного номера оператор сотовой связи вправе передать (продать) абонентские номера другим пользователям) – 6,38 %

8. Получение конфиденциальной информации о держателе карты и его счете, используемом ДБО (потерпевший сам позволяет пользоваться интернет-банкингом третьим лицам, получение пароля доступа через Интернет, получение пароля доступа через SMS-уведомление якобы от банка, использование вредоносных компьютерных программ), наличие у преступников орудий преступления связано с использованием их определенным способом. Как известно, подделка банковской пластиковой карты требует наличия специального оборудования (например, типпера оборудования для окрашивания выдавленных символов на карте методом горячего тиснения, эмбоссера оборудования для выдавливания символов на пластиковой карте, принтера для нанесения на пластиковые заготовки рисунков с символикой банков, программатора нанесения на магнитные дорожки закодированной информации истинных владельцев – держателей банковских карт) и является довольно дорогостоящей процедурой. Это позволяет выбрать преступнику более квалифицированный способ хищения, в ходе которого предметом посягательства может стать достаточно крупная сумма денег. Несмотря на разнообразие способов хищений, анализ судебно-следственной практики позволяет выявить устойчивую тенденцию повторяемости способов рассматриваемых преступлений, совершаемых одним и тем же лицом (лицами). Так, анализ хищений путем обмана, а именно многоэпизодных хищений, показал, что мошенники, выбирая какой-либо способ хищения, совершают все эпизоды преступной деятельности (в т ч действия по подготовке и сокрытию) совершенно идентичными способами. В частности, это относится к мошенничеству с использованием поддельных карт и хищениям, совершаемым банковскими работниками .

Анализируя современное законодательство и исходя из примеров судебной и правоприменительной практики, мы видим, что существует довольно-таки большое количество различных оснований классификации способов мошенничества с использованием платежных карт, которые находят свое отражение в различных трудах таких

авторов, как: В.Б.Вехов, М.Н.Филиппов, Н.Н.Федотов и др.¹

В диспозиции рассматриваемой нами статьи фактически представлен ряд оснований для классификации способов мошенничества. 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 либо кредитная, либо расчетная, либо иная платежная карта.

Другим основанием, которое указано также в объективной стороне состава преступления статьи 159.3, является характеристика лица, против которого направлен обман злоумышленника. По данному основанию способы мошенничества с использованием платежных карт могут быть разделены на три категории:

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

Имеет место быть также классификация 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. Как и во всех преступлениях, особую опасность представляют преступления, совершенные организованными преступными группами.

Так называемые группы кардеров совершают не одно, а сразу серию мошеннических преступлений. Так, в городе Ухте были задержаны участники преступной группы, состоящей из трех человек, занимавшейся мошенничеством с использованием поддельных платежных карт, в противоправной деятельности которой было зафиксировано 23 эпизода преступлений. 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

¹Вехов 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.

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 карт¹. Многоэпизодные преступления с использованием платежных банковских карт также совершаются при неоднократном приобретении товаров и услуг в магазинах и других торговых организациях².

Как и другие киберпреступления, преступления с использованием платежных карт совершаются хорошо организованными, имеющими широкую и разветвленную сеть участников организованными преступными группировками, чаще всего, участники которых имеют свою преступную специализацию³, которая может выглядеть следующим образом: одни члены группы осуществляют сбор информации по платежным картам, другие, например, обрабатывают собранную информацию и передают их тем, кто занимается изготовлением поддельных карт, третьи непосредственно осуществляют объективную сторону состава преступления. Подготовленное таким образом хищение осуществляют лица, специализирующиеся на «вещевом» кардинге – именно они используют платежную карту для обмана работников торговой организации.

Хищения, которые совершаются с использованием платежных карт, входят в состав транснациональной организованной киберпреступности. Показательным в этом отношении является задержание и последующая экстрадиция из Франции в США Владислава Хорохина, известного под ником BadB, который имел гражданство Украины, Израиля и России. Он занимался продажей информационных данных о платежных картах через сеть Интернет на форумах CarderPlanet и carder.su. Преступная организация, возглавляемая им, и схема, придуманная и используемая Хорохиным, смогла похитить

¹Попова Н. Российские банкоматы оказались в ливанской петле//АН-online. 2012. 11 фев. URL: <http://argumenti.ru/crime/2012/02/156477>, свободный.

²Приговор Верхнепышминского городского от 21 февр. 2012 г. по уголовному делу № 1-50/12 URL: <http://docs.pravo.ru/document/view/22393765/>.

³Козловский В. Масштабы кибермошенничества растут//Российская газета. 2012. 29 нояб. URL: <http://www.rg.ru/2012/11/29/karti-site.html>, свободный

денежных средств всего в количестве девяти миллионов долларов Соединенных Штатов Америки. Генеральная прокуратура США в лице помощника Генерального прокурора США Лэнни Брюера (Lanny A. Breuer) считает В. Хорохорина одним из наиболее известных и опасных во всем мире мошенников, занимающихся преступной деятельностью с использованием кредитных карт¹.

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 указаны 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 товаров².

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)³.

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 конфиденциаль-

¹Франция избавилась от российского кибервора и отправила его в США // АН-online. 2012. 17 июня. URL: <http://argumenti.ru/crime/2012/06/184343>, свободный.

²Приговор Верхнепышминского городского от 7 июня 2011 г. по уголовному делу № 1-152/11 URL: <http://docs.pravo.ru/document/view/18392970/>.

³Вехов В.Б. Особенности расследования преступлений, совершённых с использованием пластиковых карт и их реквизитов. Волгоград: ВА МВД России, 2005. С. 91–162.

ной 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.

По мнению В. В. Улейчика, хищения денежных средств при проведении операций с платежными картами могут быть классифицированы следующим образом.

1. Хищения, совершаемые с использованием подлинных платежных карт.

Самыми распространенными способами совершения указанных видов преступлений являются следующие:

1) У злоумышленников имеется оригинал платежной карты:

а) при совершении преступлений злоумышленникам известен ПИН-код владельца карты (ПИН либо нанесен владельцем на самой карте, либо написан на бумажке и хранится вместе с картой в бумажнике или сумочке, либо внесен в записную книжку телефона, и эти предметы одновременно оказались у преступников) – денежные сред-

ства снимаются через банкомат, деяние квалифицируется как кража (ст. 158 УК РФ);

б) при отсутствии ПИН-кода – покупка товаров в магазинах розничной торговли, оплата услуг и т.п. (деяние возможно при условии, что продавцы не требуют предъявления паспорта или иного документа, удостоверяющего личность, и ввода ПИН-кода через POS-терминал) – квалифицируется по ст. 159.3. «Мошенничество с использованием платежных карт».

Так, Ш. совершила мошенничество с использованием платежной карты, принадлежащей другому лицу, путем обмана уполномоченного работника сервисной организации.

Находясь в кафе «Чашка чая», Ш. увидела лежащую в книге оплаты заказов на столе расчетную банковскую карту «Сбербанк России Visa Electron», принадлежащую Н., забытую после оплаты услуг. Осознавая, что указанная расчетная банковская карта ей не принадлежит, Ш. положила ее к себе в сумку с целью последующего возврата администрации кафе.

На следующий день, обнаружив вышеуказанную банковскую карту в сумке, Ш. предположила, что на счете указанной банковской карты могут быть размещены денежные средства, на хищение которых путем обмана у нее внезапно возник преступный умысел. С целью реализации задуманного Ш. пришла в магазин «Terranova», где, осознавая, что она не является собственником карты, с целью оплаты товара передала расчетную карту продавцу М., тем самым умышленно введя последнюю в заблуждение относительно своей личности и законности своих действий. Продавец М., действуя под влиянием обмана, используя POS-терминал, установленный в магазине, произвела с предъявленной Ш. банковской карты оплату приобретенного товара на общую сумму 1798 руб. При этом Ш., продолжая своим поведением формировать ложное представление о происходящих событиях, поставила в чеке подпись вместо законного владельца банковской карты Н.;

в) при отсутствии ПИН-кода – оплата товаров и услуг через сеть Интернет – ст. 158 УК РФ. Оплатить покупки или услуги с использованием сети Интернет можно без наличия в распоряжении преступ-

ника материальной карты, достаточно располагать «визуальными» реквизитами карты, такими, как номер карты, срок окончания ее действия (месяц и год), CVV2 код для карт Visa или CVC2 код для карт Master Card (это 3 последние цифры на полосе для подписи на обороте карты).

2) Несанкционированное снятие денежных средств или оплата товаров и услуг при помощи карты, принадлежащей владельцу, доверившему ее третьему лицу для проведения операций – квалифицируется, соответственно, по ст. 158 или 159.3 УК РФ.

2. Хищения, совершаемые при помощи поддельных платежных карт.

Для совершения указанных видов преступлений злоумышленникам не требуется банковская карта владельца. Достаточно знать реквизиты банковской карты либо данные с магнитной полосы (дамп) и ПИН-код карты, либо только данные с магнитной полосы:

1) при наличии данных с магнитной полосы и ПИН-кода – изготовление поддельных банковских карт, частично имитирующих подлинные (так называемый белый пластик). При использовании в банкоматах поддельные банковские карты предоставляют их обладателям все возможности подлинных банковских карт. Снятие наличных денежных средств квалифицируется как кража (ст. 158 УК РФ);

2) при наличии данных с магнитной полосы и ПИН-кода – изготовление поддельных банковских карт, полностью имитирующих подлинные, дает возможность злоумышленникам как получать наличные денежные средства через банкомат (ст. 158 УК РФ), так и оплачивать товары и услуги (ст. 159.3 УК РФ);

3) при наличии данных с магнитной полосы и отсутствии ПИН-кода – изготовление поддельных банковских карт, полностью имитирующих подлинные, что дает возможность злоумышленникам возможность оплачивать товары и услуги (ст. 159.3 УК РФ).

В. в начале апреля 2012 г., достоверно зная о том, что его знакомый имеет возможность и специальное оборудование для изготовления поддельных платежных карт, получил от него поддельную платежную карту с целью дальнейшего ее использования.

В., имея умысел, направленный на хищение чужого имущества путем обмана, пришел в кафе-бар «Оле», где заказал для себя еду и напитки. Общая стоимость сделанного В. заказа составила 3074 рубля. Достоверно зная о том, что в указанном кафе-баре возможна оплата приобретенных товаров и услуг посредством пластиковой расчетной карты, В. попросил бармена-официанта предоставить ему электронный терминал для оплаты заказа при помощи пластиковой расчетной карты. Бармен-официант, введенная В. в заблуждение относительно личности держателя платежной пластиковой расчетной карты и права В. распоряжаться не принадлежащими ему денежными средствами, находящимися на счете не установленного следствием держателя карты, воспринимая В. как держателя карты, не зная, что данная платежная расчетная пластиковая карта является поддельной, предоставила В. электронный терминал для осуществления оплаты заказа посредством использования платежной пластиковой расчетной карты. В. вставил поддельную платежную пластиковую расчетную карту в терминал, установленный и обслуживаемый ОАО «Сбербанк России», после чего данные об указанной платежной пластиковой расчетной карте через платежную систему VISA (ВИЗА) в автоматическом режиме были обработаны и одобрены банком-эмитентом для проведения операции на заявленную сумму 3074 рубля, а соответственно, согласно договору эквайринга о проведении расчетов при реализации товаров с использованием банковских карт, была совершена оплата, в ходе которой в платежную систему была направлена информация о перечислении ОАО «Сбербанк России» на счет кафе-бар «Оле» денежных средств в сумме 3074 рубля в качестве расчета при реализации товара и услуг.

Таким образом, В. совершил преступление, предусмотренное ч. 1 ст. 159.3 УК РФ – мошенничество с использованием платежных карт, то есть хищение чужого имущества, совершенное с использованием поддельной расчетной платежной карты путем обмана уполномоченного работника торговой организации.

3. Хищения, совершаемые с использованием «визуальных» реквизитов платежной карты.

Злоумышленники различными способами (в том числе с использованием звонков от лица службы безопасности банка) получают данные о владельце платежной карты, сроке ее действия и т.п. В частности, отмечаются случаи направления мошенниками на мобильные телефоны клиентов кредитных организаций SMS-сообщений о необходимости позвонить по номерам телефонов, которые в действительности не принадлежат этим организациям. Также имеют место звонки клиентам с сообщением автоинформаторов о предоставлении продуктов и услуг банка с предложением нажать определенные клавиши на телефоне для подтверждения согласия в их приобретении и т.п. Тем самым клиенты банка провоцируются к вступлению в контакты с мошенниками, целью которых в том числе может являться получение конфиденциальной клиентской информации (например, номера банковской карты и ПИН-кода).

1) наличие реквизитов платежной карты, в том числе кода CVC2/CCV2

При оплате покупок с использованием сети Интернет необходимо иметь следующую информацию о законном владельце пластиковой карты:

номер кредитной карты;

срок окончания действия кредитной карты (месяц и год);

CCV2 код для карт Visa или CVC2 код для карт Master Card (это три последние цифры на полосе для подписи на обороте карты).

Как правило, указанных данных достаточно, чтобы оплатить покупку или совершить, как ее называют CNP (Card Not Present) транзакцию (т.е. такую транзакцию, при которых сама карта не присутствует, а используются только ее реквизиты).

В указанных случаях на квалификацию содеянного будет влиять способ совершения оплаты покупки через Интернет:

заполнение формализованного бланка (формы) с введением соответствующих реквизитов – по ст. 158 УК РФ;

сообщение реквизитов законного владельца пластиковой карты по телефону работнику торгового или сервисного предприятия – по ст. 159 УК РФ.

Во всех ранее перечисленных случаях наличие реквизитов карты и кода SVC2/CVV2 также дает возможность совершать хищение денежных средств с банковского счета держателя карты путем оплаты товаров и услуг с использованием сети Интернет.

Следует отметить, что сам факт хищения кредитной карты не может признаваться оконченным хищением – это приготовление к нему при наличии цели завладеть в дальнейшем той суммой, на которую открыта кредитная карта.

Хищение будет оконченным только тогда, когда преступник использует кредитную карту по назначению, например для того, чтобы оплатить товар или услугу.

Вместе с тем на практике не всегда правильно квалифицируют хищения денежных средств с банковских счетов с использованием пластиковых карт.

Так, приговором Асбестовского городского суда Свердловской области В. осужден за совершение двух преступлений, предусмотренных ч. 1 ст. 158 УК РФ, и двух преступлений, предусмотренных п. «в» ч. 2 ст. 158 УК РФ. Судебная коллегия по уголовным делам Свердловского областного суда нашла приговор подлежащим изменению по следующим основаниям.

Из показаний потерпевшей Е. следует, что она работает вахтером в общежитии. 20 мая 2008 г. к ней подходил В. и просил вызвать такси. В тот вечер она много раз покидала вахту, а утром обнаружила, что из сумки пропали деньги в сумме 930 руб., сотовый телефон и банковская карточка мужа с пин-кодом. В банке ей сообщили, что с карточки сняты через банкомат деньги в сумме 28 тыс. руб. По видеозаписи в банке она узнала В. и увидела, как он снимал деньги. Из показаний потерпевшего М. следует, что у его жены похитили его банковскую карточку и сняли с нее через банкомат 28 тыс. руб. Действия В. в отношении потерпевших Е. и М. суд необоснованно квалифицировал в качестве двух самостоятельных преступлений, поскольку, как установлено судом, банковскую карту В. похитил одновременно с имуществом Е., после чего снял деньги с указанной карты. Из приговора следует, что умыслом В. изначально охватывалось получение по данной карте денег через банкомат. Поэтому

действия осужденного следует квалифицировать как одно преступление, предусмотренное п. «в» ч. 2 ст. 158 УК РФ.

Кража окончена в момент завладения наличными деньгами, поскольку само по себе завладение банковской картой ущерба потерпевшему еще не причиняет.

При квалификации хищений денежных средств необходимо учитывать диспозицию ст. 187 УК РФ, которая предусматривает уголовную ответственность за изготовление в целях сбыта или сбыт поддельных кредитных либо расчетных карт. Буквальное толкование положений указанной статьи исключает возможность привлечения к уголовной ответственности за изготовление в целях сбыта или сбыт поддельных предоплаченных карт. Подделка таких карт и их использование в качестве средства платежа могут квалифицироваться по ст. 158 или 159.3 УК РФ при установлении умысла на завладение чужими денежными средствами путем их использования. В остальных случаях хищение денежных средств с банковских счетов с использованием поддельных кредитных либо расчетных карт предполагает совокупность преступлений, предусмотренных ст. 158 или 159.3 и ст. 187 УК РФ.

Проведенное исследование показало, что в специальной литературе и по ряду конкретных уголовных дел как сбыт квалифицируются действия виновных, заключающиеся в использовании поддельных кредитных или расчетных карт для оплаты товаров и услуг.

Вот как квалифицировались отдельные преступные эпизоды по одному из уголовных дел:

П. совершил изготовление в целях сбыта поддельной кредитной карты, а именно: имея умысел на изготовление в целях сбыта поддельной кредитной карты, вступив в преступный сговор с неустановленными следствием лицами, направленный на изготовление поддельной кредитной карты, в неустановленное следствием время, при неустановленных следствием обстоятельствах, совместно с неустановленными соучастниками, изготовил поддельную банковскую пластиковую карту международной платежной системы VISA № 4263 8700 5915 6505 на свое имя, с целью ее дальнейшего использования в качестве средства платежа при оплате товаров при нижеопи-

санных обстоятельствах. Согласно заключению эксперта ООО «Газкардсервис», по исследованию данной пластиковой карты международной платежной системы VISA № 4263 8700 5915 6505 установлено, что указанная пластиковая карта изготовлена самодельным способом и по способу, качеству воспроизведения полиграфических реквизитов не соответствует образцам международной платежной системы VISA, т.е. является поддельной. Имея умысел на сбыт поддельной кредитной карты, вступил в преступный сговор с П., не установленными следствием лицами, направленный на сбыт поддельной пластиковой карты: 02.04.2004 г., находясь в магазине «М-Видео», расположенном по адресу: г. Москва, Ленинский пр-т, д. 64/2, совершил сбыт подделанной им при вышеописанных обстоятельствах совместно с не установленными следствием лицами пластиковой карты международной системы VISA № 4263 8700 5915 6505, а именно: использовал ее в качестве средства платежа при оплате мобильного телефона NOKIA 8910i стоимостью 20 990 рублей, заведомо зная о поддельности вышеуказанной пластиковой карты, т.е. обвиняется в совершении преступления, предусмотренного ст. 187 ч. 1 УК РФ.

Разъяснения, содержащиеся в п. 14 постановления Пленума Верховного Суда РФ от 27 декабря 2007 г. № 51 «О судебной практике по делам о мошенничестве, присвоении и растрате», не оставляют сомнений, что использование поддельных пластиковых карт для расчета за товар или получения наличных денег, так же как и использование иных поддельных платежных документов для завладения денежными средствами, являются покушением на хищение чужого имущества или оконченным хищением, если завладение денежными средствами фактически состоялось.

Действительно, при включении статьи в УК РФ законодатель предполагал возможность рассматривать использование поддельной банковской карты как ее сбыт. Однако особенности выпуска и обращения пластиковых карт внесли свои корректировки в практику применения этой статьи. Изготовление лицом поддельных банковских расчетных либо кредитных карт для совершения этим же лицом преступлений, предусмотренных ч. 3 или 4 ст. 159 УК РФ, Пленум реко-

мендует квалифицировать только как приготовление к мошенничеству (кстати, хотя в Постановлении этого – очевидно, из-за редакционной оплошности - не сказано, но имеется, конечно, в виду, что для такой оценки приготовительная деятельность должна быть прервана по не зависящим от виновного обстоятельствам). Если бы Пленум считал использование карты видом ее сбыта, он бы потребовал квалифицировать указанные действия дополнительно и по ст. 187 УК РФ как изготовление карты с целью сбыта.

Грамматическое толкование слова «сбыт» не позволяет отнести к нему использование поддельной карты для расчетов, поскольку она как была, так и остается у посягателя. И, насколько можно понять, под сбытом в абзаце третьем п. 14 Постановления понимается именно возмездная передача поддельной карты ее изготовителем другому лицу.

Изготовление поддельных кредитных или расчетных карт является окончанным преступлением, если с целью последующего сбыта изготовлен хотя бы один такой документ независимо от того, удалось ли осуществить его сбыт. Сбыт является окончанным, если лицо произвело отчуждение хотя бы одного поддельного документа.

К сокрытию мошенничества относятся действия по получению оборудования для изготовления поддельных банковских карт и самих пластиковых карт по фиктивным документам, якобы для какого-либо учреждения или предприятия; осуществление процесса изготовления таких карт в отсутствие членов семьи или иных родственников, если этот процесс осуществляется дома; наем квартиры для этих целей и оборудование ее под офис, причем на входе, как правило, ставится дверь с кодовым замком, чтобы никто из посторонних без их ведома не мог туда войти; хранение поддельных банковских карт отдельно от подлинных; быстрое оставление места осуществления операций, совершенных по поддельным банковским картам или по подлинным, но не принадлежащим данным лицам, а также иных действий, направленных на воспрепятствование обнаружению их преступной деятельности и их самих.

Механизм следообразования. К следам данного вида преступления относится, прежде всего, сама банковская карта как со следами подделки, так и подлинная, но не принадлежащая мошеннику.

К материальным следам преступления относятся: обнаруженные при обыске у преступника пластиковые карты белого цвета с нанесенной на них магнитной полосой; скиммеры — специальные накладные устройства для банкомата, которые считывают номер банковской карты; микрокамеры для фиксации набираемого PIN-кода; накладные панели для этой же цели; гибкая плата, которую преступники внедряют в кардридер банкомата для считки данных банковской карты; клейкая лента, с помощью которой блокируется банковская карта, а пока ее держатель выясняет причину у банковских работников, преступники ее извлекают из банкомата; энкодеры для нанесения соответствующей информации на магнитную полосу карты; поддельные накладные, по которым приобреталось это имущество якобы для каких-либо производственных целей; нарезанные тонкие полоски белой бумаги, предназначенные для наклеивания на карту и обозначающие полосу для подписи; краски для окрашивания карты в необходимый цвет и нанесения на нее соответствующих рисунков и голограмм; специальная литература по вопросам изготовления поддельных банковских карт; подлинные банковские карты на разных держателей и иные предметы, свидетельствующие о намеренности мошенника с помощью поддельных банковских карт получать чужое имущество.

Помимо материальных следов при совершении мошенничества с помощью банковских платежных карт остаются еще и идеальные следы. К таким следам можно отнести показания кассиров, продавцов и т.д.

Обстоятельства совершения преступления. Анализ способов совершения хищений с использованием кредитных и расчетных карт позволяет нам установить наиболее распространенные типичные места совершения преступления, а также время, условия, способствующие выбору именно этого способа хищения, к которым относится обстановка совершения преступления. Так, если рассматривать данный вид преступлений, то типичными местами совершения хищений являются «уличные» банкоматы, расположенные вдали от банков на неоживленных улицах (46,6 %); банкоматы, расположенные в торговом - сервисных предприятиях (4,8 %); банкоматы, расположенные в здании банков (4,25 %); торгово-сервисное предприятие (3,6 %), рабочее место сотрудника банка (48 %).

Место хищения карты нами рассматривается не как место совершения самого преступления, а как место совершения подготовки к хищению, знание которого в подавляющем большинстве случаев позволяет более детально выдвинуть версии о личности преступника.

К местам подготовки к мошенничеству следует отнести: квартиры, как жилые, так и съемные, оборудованные под офис, склад и иное недоступное для посторонних лиц помещение, в которых осуществляются изготовление поддельных карт, нанесение на магнитную полосу информации, скопированной с подлинной банковской карты; различные магазины, где приобреталось оборудование для подделки банковских карт («белый пластик», импринтеры, скиммеры, энкодеры, микрокамеры).

Проведенный анализ показывает, что во всех случаях совершения хищения с использованием кредитных и расчетных карт ему предшествуют определенные действия по подготовке к преступлению, которые влияют на выбор не только способа, но и времени и, соответственно, имеют криминалистическое значение как элемент криминалистической характеристики. Время совершения преступления зависит от его места. Так, покупки в крупных торговых точках совершаются в выходные дни или в будние дни, но после окончания рабочего дня, когда в этих местах большое скопление народа, создаются очереди к кассам, и кассиры в связи с большой напряженностью работы теряют бдительность, не обращают внимания на дефекты предъявляемой к оплате карты, небольшие расхождения подписи покупателя на слипе и держателя карты на самой карте и некоторые другие подозрительные моменты.

Время совершения хищения напрямую связано не только с местом совершения хищения, но и с местом и временем завладения банковской картой. Так, в 4,3 % случаев хищения денежных средств совершались в течение трех часов после завладения картой и в 36,54 % - в течение первого часа. Это обусловлено тем, что преступник предполагает скорое обнаружение потерпевшим пропажи карты и последующую блокировку.

Анализ судебно-следственной практики показал, что чаще всего хищения совершаются в период до 8 часов - 34,5 %, с 8 до 4 часов –

3,39 %, с 4 до 6 часов – ,97 % и с 6 до ? часов 21,12 %³.

В случае совершения открытого хищения денежных средств и ряда краж завладение картой и денежными средствами происходит почти одновременно в присутствии потерпевшего - 8,86 % . Выбор времени хищения путем мошенничества с использованием чужих карт или поддельных карт зависит также от места хищения, которое, как правило, бывает крупным торговым центром, магазином по продаже бытовой техники. В данном случае хищение совершается в период с 6 до ? часов, т е в часы работы магазина, когда у продавцов наблюдается усталость и ослабление внимания. Совершение хищений сотрудниками кредитных организаций происходит в часы выполнения служебных обязанностей с 9 до 9 часов. По календарным временам года распределение зарегистрированных хищений довольно равномерно, небольшой рост краж регистрируется в летнее время, что обусловлено увеличением роста карманных краж.

При выборе места и времени совершения хищения преступники учитывают следующие условия:

- знание PIN-кода к банковской карте (в случае, если PIN-код известен, преступник использует ближайший к месту жительства потерпевшего или к месту хищения карты банкомат, в противном случае местом проведения незаконной транзакции будет какой-либо магазин, где не требуется введения PIN-кода);
- наличие на карте определенной суммы денег, заранее известной преступнику;
- наличие благоприятных условий для сокрытия внешности; качество «подделки» карты;
- отсутствие возможных очевидцев использования карты;
- освещенность в месте нахождения банкомата.

В качестве предмета хищения, совершенного с использованием кредитных и расчетных карт, следует признавать имущество в виде безналичных денег, то есть сумму, записанную на карточном счете держателя карточки, либо денежные средства участников осуществления системы безналичных расчетов с использованием кредитных и расчетных карт. Необходимо отметить, что в отличие от наличных денег, безналичные деньги находятся не у держателя карты, а у

третьего лица – банка, который не может ими распоряжаться.

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 набора¹.

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,

¹ 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.

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* – *voicephishing*) – 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 программа («троян»). Фарминг может быть осуществлен и непосредственно на DNS сервере интернет-провайдера владельца карты. Для 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 распространённым мошенничеством по данным международной платёжной системы, является мошенничество с утерянными картами. Ущерб от него составляет почти половину от всех случаев мошенничества с кредитными картами. Вовремя не заблокированная потерянная или украденная карта может послужить преступнику отличным средством для оплаты по счету там, где не требуется ввода никаких паролей¹. 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)².

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,

¹Кривошапова 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.

²Там же.

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.¹

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 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.

Обстоятельства, подлежащие установлению. По делам данной категории устанавливается:

- в каком месте расположен банкомат, касса, каков режим работы, имеются ли средства видеонаблюдения, где находится пункт охраны;
- кто принимал к оплате банковскую карту; каков уровень подготовки данного сотрудника;
- кто является потерпевшим; размер причиненного ущерба;
- каков вид банковской карты, на имя кого и где она была оформлена, количество денежных средств, находящихся на ней;
- где, когда проводилась последняя операция с использованием банковской карты;
- кто помимо владельца банковской карты имел доступ к денежным средствам, находящимся на ней, кто знал PIN-код;
- каков способ совершения мошенничества, какие технические устройства, приспособления использовались для изготовления бан-

¹Криминалистика / под ред. Н.П. Яблокова. М.: Норма: ИНФРА-М, 2010. С.546.

ковских карт, снятия денежных средств со счета держателя банковской карты;

- где, у кого и для каких целей приобретались данные технические устройства;
- личность лица, совершившего мошенничество, обладает ли подозреваемый специальными знаниями в области изготовления поддельных банковских карт, использования специальных приспособлений для снятия денежных средств;
- совершалось ли данное преступление в группе; если да, то какова роль каждого лица.

Возбуждение уголовных дел по делам данной категории происходит по результатам проверки фактов, изложенных в сообщении о преступлении. О фактах мошенничества с использованием банковских карт правоохрнительным органам становится известно от держателя банковской карты; банков-эмитентов, банков-эквайеров; при задержании лица, неправоммерно использовавшего банковскую карту; от представителей торгово-сервисных организаций; из результатов оперативных проверок или при расследовании других уголовных дел.

К числу проверочных мероприятий относятся:

- запросы в банки-эмитенты, банки-эквайеры, торгово-сервисные предприятия с целью получения документов, подтверждающих факты движения денежных средств;

- объяснения, полученные от держателя банковской карты, совместно проживающих с ним лиц, задержанного лица, сотрудников банка, торгово-сервисного предприятия, очевидцев;

- осмотр места, где произошло незаконное использование банковской карты (банкомат, торгово-сервисная точка), с обязательным привлечением специалиста;

- осмотр предметов и документов (скиммеров, банковских карт, заявления держателя банковской карты об опротестовании конкретных транзакций, анкет, копий договоров о предоставлении банковской карты, выписок по карт-счетам за интересующий период, копий электронных журналов банкоматов, POS-терминалов), производится с участием специалиста;

- исследование предметов и документов (банковских карт, скиммеров);
- истребование материалов с камер видеонаблюдения, свидетельствующих о фактах незаконного использования банковской карты .

На первоначальном этапе расследования мошенничества с использованием платежных карт возникают следующие типичные следственные ситуации:

1) мошенник задержан при попытке совершить оплату товара или снять денежные средства путем использования не принадлежащей ему (поддельной) банковской карты.

В данной ситуации необходимо произвести: осмотр места происшествия; допросы держателя банковской карты, свидетелей, подозреваемого; выемку банковской карты у законного держателя с последующим осмотром; выемку документов, подтверждающих факт предоставления банковской карты, выписок по карт-счетам за интересующий период, копий электронных журналов банкоматов, POS-терминалов, их осмотр; предъявление для опознания; получение образцов для сравнительного исследования; назначение экспертиз;

2) информация о незаконном использовании банковской карты поступила от владельца карты.

В этой ситуации необходимо провести комплекс следственных действий и оперативно-разыскных мероприятий: допрос потерпевшего и свидетелей; выемку банковской карты у законного держателя с последующим осмотром; запрос в банк-эмитент и банк-эквайер о предоставлении выписки по счету с указанием всех операций с денежными средствами, произведенными за отчетный период по интересующей следствие банковской карте; выемку документов, подтверждающих факт предоставления банковской карты, выписок по карт-счетам за интересующий период, копий электронных журналов банкоматов, POS-терминалов, их осмотр; выемку видеозаписи с камер наблюдения, расположенных в местах нахождения банкоматов, POS-терминалов, с использованием которых были обналичены денежные средства или приобретен товар, их осмотр; предъявление для опознания.

Задержание подозреваемого. Данное следственное действие проводится по общим правилам криминалистической тактики. Однако следует учитывать, что преступники могут быть вооружены и оказывать сопротивление сотрудникам правоохранительных органов. Поэтому во всех случаях производства задержания его необходимо тщательно планировать.

Личный обыск. После задержания подозреваемого сразу следует провести его личный обыск с целью отыскания каких-либо предметов, имеющих отношение к расследуемому преступлению. При подозреваемом могут находиться следующие предметы: «белый пластик» как с нанесенной на его магнитную полосу информацией о подлинной банковской карте, так и еще не подготовленный для совершения мошеннических действий; подлинные банковские карты, принадлежащие различным лицам; денежные средства; приспособления для считывания информации с банковских карт; различные записи, касающиеся совершения мошеннических действий, в том числе телефоны, имена, клички соучастников, а также иная информация, могущая иметь значение для расследования данного преступления.

Осмотр места происшествия. Типичными местами совершения мошенничества с использованием банковских карт являются места расположения банкоматов, торговые павильоны, оборудованные POS-терминалами. К осмотру места происшествия необходимо привлекать как специалиста-криминалиста, так и специалиста в области компьютерных технологий или радиотехники. Это связано с тем, что зачастую мошенники для считывания информации с банковских карт используют специальные устройства (приспособления), крепящиеся к банкомату; не обладая специальными знаниями, достаточно сложно определить наличие этих устройств.

Осмотр документов и предметов. Это одно из важнейших следственных действий. Осмотр банковской карты необходимо проводить в присутствии специалиста. Описывая банковскую карту в протоколе, следует отразить материал изготовления, цвет, рисунок, расположенный на поверхности карты. По отдельности описываются лицевая и оборотная стороны карты. При описании лицевой стороны указывают: место расположения логотипа, номера карты, срок ее дей-

ствия, персональные данные держателя карты; при описании оборотной стороны - место расположения голографической магнитной полосы, полосы для подписи клиента, подпись держателя карты.

Основными признаками, указывающими на подделку банковской карты, являются: отсутствие глянца на поверхности карты; боковые стороны пластика - не белого цвета; наличие механических повреждений; отслаивание ламинирующей пленки по краям карты; некачественное выполнение элементов дизайна карты (рисунки, логотипы, текст); отличие логотипа от подлинного по цвету и его легкое стирание; не читаемая микропечать вокруг логотипа; отслоение голограммы, которая задирается и дает утолщение при надавливании; отсутствие или несовпадение первых четырех цифр номера карты с четырьмя цифрами, напечатанными типографским способом под номером карты; наличие вместо полосы для подписи, выполненной из специального состава, нанесенного тонким слоем, наклеенной тонкой полоски бумаги, которая легко чувствуется на ощупь, причем края полоски легко задираются ногтем, и др.

Осмотру могут подвергаться предметы и устройства, обнаруженные при осмотре места происшествия или при производстве обыска у подозреваемого лица. Чаще всего это эмбоссер - устройство, позволяющее наносить надписи на пластиковую основу карты; тайпер - устройство, с помощью которого «впаивают» магнитную ленту; скиммер - устройство, позволяющее считывать информацию с магнитной полосы, с сохранением или передачей для дальнейшей обработки; энкодер - устройство, позволяющее записывать на пластиковую банковскую карту информацию с ЭВМ, полученную со скиммера.

Производить осмотр и описание указанных устройств также необходимо в присутствии специалиста. Устройства описываются по общим правилам, разработанным в криминалистике, с указанием материала изготовления, формы, цвета, размерных характеристик, составных частей, индивидуализирующих признаков.

Обыск. По делам о мошенничестве с банковскими картами обыск может быть произведен как по месту жительства подозреваемого, так и в иных местах. Особое внимание следует уделить обнаружению пластика, из которого изготавливались поддельные банков-

ские карты; различного оборудования для считывания информации с банковских карт: скиммеров, микрокамер, кардридеров, клейкой ленты и др., а также технических средств, с помощью которых полученная таким способом информация о PIN-коде и владельце банковской карты переносится на поддельную карту; энкодеров и др.

Помимо этого следует обращать внимание на различные схемы и иные документы, на которых обозначены разные терминалы для выдачи денежных средств, с целью последующей проверки и установления случаев обнаружения на этих терминалах дополнительного оборудования.

Допрос потерпевшего. В качестве потерпевшего могут быть допрошены лица, с банковских карт которых были списаны деньги без выполнения ими соответствующих операций. В ходе их допроса можно получить ответы на следующие вопросы:

- как давно они пользуются банковской картой; какая сумма находится на счету банковской карты; где он ее хранит; кто еще пользуется данной банковской картой;

- всегда ли он рассчитывается при совершении покупок или после оказания ему необходимых услуг этой картой; посещал ли он в последнее время какие-либо рестораны, кафе или другие похожие заведения; обращался ли он в автосервис для оказания услуг в связи с неисправностью автомашины и т.д.;

- производился ли расчет за оказанные услуги банковской картой; происходило ли это в его присутствии или банковскую карту сотрудники этих заведений уносили в другое место; не заметил ли он что-либо подозрительное при расчете по своей банковской карте;

- когда у него со счета была списана определенная сумма денег; подключена ли к его телефону услуга «Мобильный банк»; приходили ли ему сообщения о снятии денежных средств;

- какие действия он в связи с этим предпринял; куда и когда обращался для блокирования счета и возврата списанных денег и т.д.

Допрос свидетелей. В качестве свидетелей могут быть допрошены кассиры магазинов, которые прояснят следующие обстоятельства:

- принимают ли они к оплате банковские карты, какие конкретно; как происходит такая оплата; на что они обращают внимание при оплате таким способом; в какое время к ним подошел подозреваемый для оплаты приобретенных им покупок; какой банковской картой он намеревался расплатиться; полностью ли пропечатались цифры и буквы карты на слипе; одинаковые ли были подписи на слипе и на самой карте; совпадал ли номер банковской карты на магнитной полосе и на слипе;

- что конкретно насторожило кассира в предъявленной банковской карте; какие действия он предпринял;

- как вел себя покупатель, что пояснил по поводу несовпадения некоторых реквизитов банковской карты и т.д.

Допрос обвиняемого. Проводится на последующем этапе расследования мошенничества с помощью банковских карт. Предмет допроса может быть такой же, как и при допросе подозреваемого. Однако действия дознавателя будут зависеть от того, какую позицию по предъявленному обвинению занял обвиняемый. В тех случаях, когда он полностью признает свою вину в совершенном мошенничестве, действия дознавателя сводятся к закреплению имеющихся доказательств. В тех же случаях, когда обвиняемый виновным себя не признает или признает частично, дознавателю необходимо, используя существующие тактические приемы допроса, убедить его в неправомерности занятой им позиции и дать правдивые показания по существу обвинения.

Допрос других свидетелей. Свидетелями в данном случае могут быть любые лица, которые могут дать интересующую дознавателя информацию: сотрудники интернет-магазинов по поводу того, кто закупал у них «белый пластик», используемый для изготовления банковских карт, и оборудование для нанесения на магнитную ленту соответствующей информации; владельцы квартир, у которых мошенники снимали данное помещение для оборудования его под офис и т.д.

Назначение экспертиз. При расследовании мошенничества с использованием платежных карт назначают следующие судебные экспертизы: почерковедческую, технико-криминалистическую экс-

пертизу документов, компьютерно-техническую, дактилоскопическую. Рассмотрим более подробно некоторые из них.

Объектом судебно-почерковедческой экспертизы являются банковские карты, на оборотной стороне которых расположена подпись держателя карты или слипы (чеки), выдаваемые при оплате товаров и услуг, получении наличных денежных средств в пунктах их выдачи, также заверенные подписью заподозренного лица. Основной задачей почерковедческой экспертизы является установление факта исполнения спорной подписи конкретным лицом.

На технико-криминалистическую экспертизу чаще всего направляют поддельные банковские платежные карты. Основной вопрос, выносимый на разрешение эксперта, заключается в установлении способа изготовления представленного документа.

Судебная компьютерно-техническая экспертиза назначается в том случае, когда дознавателю необходимо узнать:

- информацию, содержащуюся на магнитной полосе банковской карты, и то, совпадает ли эта информация с данными на поверхности банковской карты;
- возможно ли использовать данные пластиковых карт в стандартно применяемых устройствах, считывающих магнитные полосы, в частности, в POS-терминалах, для совершения финансовых операций;
- данные эмитентов, выпускающих оригиналы представленных на исследование пластиковых карт.

При обнаружении и изъятии таких устройств, как скиммер, эмбоссер, тайпер, энкодер, дознаватель также может назначить компьютерно-техническую экспертизу, на разрешение которой вынести следующие вопросы:

- каково функциональное назначение и возможности представленных устройств; являются ли представленные устройства единым комплектом;
- каким способом изготовлены представленные устройства (кустарным или промышленным);
- возможно ли получение с помощью представленных устройств сведений, содержащихся на банковских картах, в частности, сведений о владельце, номере счета, произведенных операциях по не-

му, остатке денежных средств, PIN-кодах, вводимых пользователем; если да, то каким образом;

- содержатся ли на представленных устройствах информация о платежных пластиковых картах, какая-либо видеoinформация, в том числе свидетельствующая об установке или снятии устройств; если да, то какая?

Криминологическая характеристика субъектов преступлений, совершаемых в сфере проведения безналичных расчетов¹, 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

¹ 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.

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 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%¹.

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%².

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 лет (около 26%), от 18 до 26 лет (около 18%), 50 лет 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

¹Так, 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.

² Васюков С.В. Предупреждение преступлений, совершаемых в сфере проведения безналичных расчетов, проводимых с использованием банковских карт: автореф.т дис. ... на соискание ученой степени кандидата юридических наук. 12.00.08 - Уголовное право и криминология; уголовно-исполнительное право. М., 2013. С. 20-23.

вполне профессиональные преступники, связавшие повышение уровня своего материального благосостояния, да и положение в обществе в целом, с криминалом¹.

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 фактических 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 образования².

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%³.

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%⁴.

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 ответст-

¹ Васюков С.В. Указ.соч.

² Там же.

³ Там же.

⁴ Там же.

венности 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%) были привержены к определенному «своему» способу совершения¹.

Что касается потерпевшего, то им является банк — эмитент платежной карты, с помощью которой мошенник оплатил покупки или оказанные ему услуги. Именно этот банк несет убытки в тех случаях, когда держатель банковской карты делает заявление в соответствующий банк о том, что никаких операций с ее помощью он не совершал. И если это подтвердится в процессе проверки, произведенной сотрудниками банка, то снятая сумма возвращается держателю банковской карты.

Но потерпевшими могут быть и держатели банковских карт в тех случаях, когда банк отказывает им в возмещении причиненного ущерба по каким-либо основаниям².

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

¹ Васюков С.В. Указ. соч.

² Чистова Л. Е., Волкова Г. П., Махова И. В. Криминалистическая характеристика мошенничества с использованием платежных карт // Вестник криминалистики. 2013. Вып. 2(46). С. 24.

техническому регулированию и метрологии на добровольной основе создан заинтересованными организациями Технический комитет по стандартизации № 122 «Стандарты финансовых операций» (далее – ТК № 122) в целях организации и проведения работ по национальной, межгосударственной и международной стандартизации финансовых операций. В 2011 году была утверждена организационная структура и основные направления его деятельности. В настоящее время ТК № 122 состоит из пяти подкомитетов: ПК № 1 «Безопасность финансовых (банковских) операций», ПК № 2 «Технологии операций на финансовых рынках», ПК № 3 «Технологии основных финансовых (банковских) операций», ПК № 4 «Процедуры и технологии расчетов с использованием банковских карт и иных инструментов розничных платежей» (далее – ПК № 4) и ПК № 5 «Мобильные платежи» (далее – ПК № 5). Помимо Банка России, в ТК № 122 участвуют более 50 организаций, представляющих органы государственной власти, кредитные организации и их ассоциации, инфраструктурные организации финансовых рынков и иные заинтересованные стороны, в том числе представители рынка розничных платежных услуг. К приоритетному направлению деятельности ПК № 4 и ПК № 5 можно отнести выработку национального стандарта по предотвращению совершения несанкционированных операций с использованием электронных средств платежа (далее – ЭСП), включая разработку подходов к организации единой 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 Европы» (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, граничащая 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 %¹.

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;

2. Для проведения атаки в 82 % случаев достаточно иметь

¹Выборнов А. Устранение уязвимостей // BIS journal. 2014. № 4.

среднюю или низкую квалификацию;

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

4. Причиной 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 сети¹.

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 банкоматов². 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.

¹ Выборнов А. Устранение уязвимостей // BIS journal. 2014. № 4.

² Смольянинова Е.Н., Фурманов Д.В. Проблемы безопасности расчетов при использовании пластиковых карт // Актуальные вопросы экономических наук. 2012. С. 46–50.

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,
- 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)¹.

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

¹Смольянинова Е.Н., Фурманов Д.В. Проблемы безопасности расчетов при использовании пластиковых карт //Актуальные вопросы экономических наук. 2012. С. 46–50.

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 активность¹. Важно отметить эффективность организационных 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

¹ Эволюция карточного мошенничества в Европе 2013. [Электронный ресурс]. URL: <http://www.fi.co.com/landing/fraudeurope2013>

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 платеж¹. 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

¹Корякин В.М., Саенко А.Ю. Некоторые вопросы безопасности использования банковских карт // Право в Вооруженных силах. 2012. № 2. С. 75.

сумме, или требовать дополнительной авторизации для выполнения операции¹.

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.

¹ Мокрушина А.Л., Рустамова Э.О. Интернет-банкинг - новая форма старых услуг: понятие, безопасность, перспективы развития системы // Проблемы и перспективы развития современного законодательства. М.: Изд-во Рос.тамож. акад., 2013. С.63-66.

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 соответствующих 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, граничащая 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)¹.

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,

¹Смольянинова Е.Н., Фурманов Д.В. Проблемы безопасности расчетов при использовании пластиковых карт //Актуальные вопросы экономических наук. 2012. С. 46–50.

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. 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. 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, будучи введенным в заблуждение относительно того факта, что перед ним находится держатель карты, принимает предоставленную платежную карту в качестве средства платежа. С другой точки зрения, между ст. 159.1 и ст. 159.3 УК РФ существует конкуренция. Денежные средства при оформлении заявления на получение кредитной карты предоставляются в определенных объемах и на определенный срок, при условии возвратности, в соответствии со ст. 159.1 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 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.

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 IT технологий.
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, относится:

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 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.

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-І// Ведомости съезда народных депутатов РСФСР – 1990. - N 27 - Ст. 357.

5. О Центральном банке Российской Федерации (Банке России): Федеральный закон от 10 июля 2002 г. N 86-ФЗ // 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 // Собрание законодательства Российской Федерации. - 2003. - N 52 (часть І). - Ст. 5029.

7. О национальной платежной системе: Федеральный закон от 27.06.2011 N 161-ФЗ (действующая редакция, 2016). - 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). - 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). - 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. Порядок обеспечения и защиты банковской информации: Положение ЦБ РФ от 16.12.2003 г. № 242-П: (с изменениями и дополнениями). - URL: <http://base.garant.ru/584330/>(дата обращения: 27.10.2016).

12. 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: Положение Банка России от 9 июня 2012 года № 382-П в редакции указания Банка России от 5 июня 2013 года № 3007-У.

13. Об эмиссии платежных карт и об операциях, совершаемых с их использованием: положение (:утв. Банком России 24.12.2004 № 266-П ред. от 14.01.2015 // Вестник Банка России. - 03.2005.- №17.

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

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

16. О судебной практике по делам о краже, грабеже и разбое: Постановление Пленума Верховного Суда РФ от 27.12.2002 № 29: ред. от 03.03.2015 // Российская газета. - 2003. – 18 янв.

17. О судебной практике по делам о преступлениях против личной собственности: постановление Пленума Верхов. Суда СССР от 5 сентября 1986 г. N 11: в ред. от 30.11.1990 // СПС "Консультант-Плюс" (док. недейств.).

18. Приговор Ленинского районного суда г. Новосибирска от 05.05.2015. Дело № 1-420/2015 // URL: <http://sudact.ru/regular/doc/n1gmRVegiglg/>

19. Приговор Кировского районного суда г. Кемерово, Кемеровской области от 12.11.2015. Дело № 1-395/15. // URL: <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/](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/](http://docs.pravo.ru/document/view/22393765/).

Специальная литература

22. Акимов В.Е. Методика расследования преступлений, связанных с хищением денежных средств, совершенных с использованием банковских пластиковых карт: автореф. дис. ... канд. юрид. наук / В.Е. Акимов. – М., 2008. – 20 с.

23. Александрова И.А. Новое уголовное законодательство о мошенничестве / И.А. Александрова // Юридическая наука и практика. Вестник Нижегородской академии МВД России. - 2013. - № 21. - С.54-62.

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

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

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

27. Безопасность банковских карт: взгляд потребителя и активность игроков рынка: Отчет по результатам исследования. - М.: Национальное агентство финансовых исследований, 2016. - URL:

http://nacfin.ru/wpcontent/uploads/2015/01/moshennichestvo_bankovskie_karty.pdf. (проверено на 30.10.2016).

28. Бизнес-энциклопедия "Платежные карты" / И.М. Голдовский и др.; ред.-сост. А.С. Воронин. - 2-е изд., перераб. и доп. - М.: КНО-РУС, ЦИПСИР, 2014. 560 с.

29. Боровых Л.В. Проблема квалификации хищения с использованием банковских карт / Л.В. Боровых, Е.А. Корепанова // Российский юридический журнал. - 2014. - № 2. - автореф. канд. экон. наук. М., 2013.

30. Бочаров О.А. Формирование основ экономической безопасности банковской деятельности: автореф. дис. ...канд. экон. наук / О.А. Бочаров. - М., 2013.

31. Волженкин Б.В. Преступления, связанные с нарушением установленного порядка осуществления предпринимательской и иной экономической деятельности / Б.В. Волженкин // Новое уголовное право России. Особенная часть: учеб. пособие. - М., 2011.

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

33. Васюков С.В. Предупреждение преступлений, совершаемых в сфере проведения безналичных расчетов, проводимых с использованием банковских карт: автореф. дис. ... канд. юрид. наук: 12.00.08 - Уголовное право и криминология; уголовно-исполнительное право. - М., 2013.

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

35. Волохова О.В. Расследование преступлений, связанных с обманом / О.В. Волохова. - М.: Юрлитинформ, 2008.

36. Выборнов А. Устранение уязвимостей / А. Выборнов // BIS journal. - 2014. - № 4.

37. Горова Н. Туз в кошельке / Н. Горова // Коммерсантъ. Юг

России - Ростов-на-Дону. - 2013. - 30 апр.; URL: <http://kommersant.ru/doc/2179379?isSearch=True>, свободный.

38. Джеймс Л. Фишинг: Техника компьютерных преступлений / Л. Джеймс; пер. с англ. Р.В. Гадицкого. - М.: НТ Пресс, 2008. - 314 с.

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

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

41. Звезда И.И. Расследование хищений в банковской сфере, совершенных путем мошенничества: автореф. дис. ... канд. юрид. наук / И.И. Звезда. - М., 2008. - 22 с.

42. Кирюшин А.В. Правовые аспекты обеспечения экономической безопасности Российской Федерации / А.В. Кирюшин, С.В. Плотников // История государства и права. - 2014. - № 9. - С.69.

43. Киселев А. Кражи с пластиковых карт часто происходят с участием сотрудников банков / А. Киселев // Коммерсантъ FM. - 2013. - 23 мая; URL: <http://kommersant.ru/doc/2195462?isSearch=True>, свободный.

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

45. Компьютерное мошенничество. Битва байтов / под ред. Дж. Т. Уэллса; пер. с англ. С.А. Филина. - М.: Маросейка, 2010. - 354 с.

46. Корякин В.М. Некоторые вопросы безопасности использования банковских карт / В.М. Корякин, А.Ю. Саенко // Право в вооруженных силах. № 2. 2012.

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

48. Криминалистика / под ред. Н.П. Яблокова. - М.: Норма: ИН-

ФРА-М, 2010. – 751 с.

49. Ларичев В.Д. Криминалистическая характеристика экономических преступлений и методика ее построения / В.Д. Ларичев // Научный портал МВД России. - 2009. - № 1.

50. Лясковский Е.Н. Организационно методические основы обеспечения экономической безопасности банковской сферы / Е.Н. Лясковский // Проблемы управления рисками в техносфере. - 2009. - №1(9)2(10). - С.90.

51. Малов А. Исповедь кардера / А. Малов. - М.: ЦИПСИР: Альпина Паблишерз, 2010. - 198с.

52. Мещеряков В.А. Преступления в сфере компьютерной информации: основы теории и практики расследования / В.А. Мещеряков. - Воронеж: Изд-во Ворон.гос. ун-та, 2002.- 408 с.

53. Мишина И.М. Расследование мошенничества, совершенного с использованием банковских карт: криминалистические и уголовно-процессуальные аспекты: автореф. дис. ... канд. юрид. наук / И.М. Мишина. - М., 2009. - 26 с.

54. Мокрушина А.Л. Интернет-банкинг - новая форма старых услуг: понятие, безопасность, перспективы развития системы / А.Л. Мокрушина, Э.О. Рустамова // Проблемы и перспективы развития современного законодательства. - М.: Изд-во Рос. тамож. акад., 2013. - С.63-66.

55. Национальная система платежных карт Российской Федерации. - URL: <http://www.nspk.ru/> (дата обращения: 27.10.2016).

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

57. Официальный сайт Центрального Банка Российской Федерации. - URL: <https://www.cbr.ru/> (проверено на 30.10.2016).

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

59. Россинская Е.Р. Криминалистика / Е.Р. Россинская. - М.: НОРМА:ИНФРА-М, 2012. - 464с.

60. Россия в глобализирующемся мире: Стратегия конкурентоспособности / Российская академия наук, отделение общественных наук, секция экономики; акад. Д.С. Львов [и др.]. - М.: Наука, 2014.
61. Смольянинова Е.Н. Проблемы безопасности расчетов при использовании пластиковых карт / Е.Н. Смольянинова, Д.В. Фурманов // Актуальные вопросы экономических наук. - 2012. - С. 46–50.
62. Состояние преступности в России за 2011 год: сборник ГИАЦ МВД России. - М., 2012.
63. Теоретические основы квалификации преступлений, предусмотренных ст. 159-159.6 УК РФ: методические рекомендации / М.Р. Гарафутдинов и др. – Казань: КЮИ МВД России, 2014. – 75 с.
64. Теряева А.С. Национальная платежная система России: предпосылки возникновения и текущее состояние / А.С. Теряева, Т.А. Журавлева, Е.С. Харитонюк // Дискуссия. - 2016. - Выпуск №2 (65).
65. Федотов Н.Н. Форензика – компьютерная криминалистика / Н.Н. Федотов. - М.: Юрид.мир, 2007. - 359 с.
66. Филиппов М.Н. Расследование краж и мошенничеств, совершенных с использованием банковских карт и их реквизитов: автореф. дис. ... канд. юрид. наук / М.Н. Филиппов. - М., 2012. - 30 с.
67. Фирсов Е. П. Расследование изготовления или сбыта поддельных денег или ценных бумаг, кредитных либо расчетных карт и иных платежных документов / Е.П. Фирсов. - М.: Юрлитинформ, 2004. - 155 с.
68. Франция избавилась от российского кибервора и отправила его в США // АН-online. - 2012. - 17 июня. URL: <http://argumenti.ru/crime/2012/06/184343>, свободный.
69. Хилjuta В.В. Момент окончания хищения: практика применения теоретических концепций / В.В. Хилjuta // Вестник БДУ. – 2010. - Сер. 3. - № 3. - С. 93.
70. Чистова Л. Е. Криминалистическая характеристика мошенничества с использованием платежных карт / Л.Е. Чистова, Г.П. Волкова, И.В. Махова // Вестник криминалистики. - 2013. - Вып. 2(46). - С. 24.
71. Эволюция карточного мошенничества в Европе 2013. - URL: <http://www.fico.com/landing/fraudeurope2013>
72. Эрлихман В. Кошелек и жизнь / В. Эрлихман // Gala Биография. - 2012. - № 11 (95). - С. 96.

73. Южин А.А. Мошенничество и его виды в российском уголовном праве: дис. ... канд. юрид. наук: 12.00.08 – уголовное право и криминология; уголовно-исполнительное право / А.А. Южин. – М.: МГЮУ им. О.Е. Кутафина, 2016.

Электронные источники

74. Аналитический обзор статей об ответственности за мошенничество // Официальный сайт справочной правовой системы «КонсультантПлюс» <http://www.consultant.ru/law/review/1657522.html>

75. Безопасность банковских карт: взгляд потребителя и активность игроков рынка. Отчет по результатам исследования. - М.: Национальное агентство финансовых исследований, 2016. - URL: http://nacfin.ru/wpcontent/uploads/2015/01/moshennichestvo_bankovskie_karty.pdf. (проверено на 30.10.2016).

76. Добрынин Ю. Классификация преступлений, совершаемых в сфере компьютерной информации / Ю. Добрынин. - URL: http://www.russianlaw.net/law/computer_crime/a158/ (проверено 04.11.2016).

77. История платежной системы MasterCard International. Начало истории. URL: http://rbcard.com/history/hist_master.htm/, www.mastercard.com.

78. Лаврентьева Н. Российские банки внедряют технологию, отбирающую "хлеб" у инкассаторов / Н. Лаврентьева // Сnews.ru. – 2012. - 16 марта. URL: <http://www.cnews.ru/news/top/index.shtml?2012/03/16/481803>.

79. Национальная система платежных карт Российской Федерации. - URL: <http://www.nspk.ru/> (дата обращения: 27.10.2016).

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

81. Распространение пластиковых карт по миру. - URL: <http://www.belcard.by/cgi-bin/view.pl?topicid=feeb0ecf>.

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

83. Western Union / Our Rich History. - URL: <http://corporate.westernunion.com/history.html>.

Учебное издание

БАНКОВСКАЯ БЕЗОПАСНОСТЬ

Учебное пособие

Составители

Ольга Геннадьевна Шмелева
Гульнара Насимовна Хадиуллина

Корректор Н.А. Климанова

Подписано в печать 29.06.2018 Усл.печ.л. 8,25
Формат 60х84 1/16 Тираж 30

Типография КЮИ МВД России
420108, г. Казань, ул. Магистральная, 3