Министерство внутренних дел Российской Федерации

Федеральное государственное казенное образовательное учреждение высшего образования «Казанский юридический институт Министерства внутренних дел Российской Федерации»

Кафедра криминологии и уголовно-исполнительного права

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

на тему: Предупреждение мошеннических действий с использованием платежных карт

Выполнил: Макаров Владислав Александрович
(фамилия, имя, отчество)
слушатель 5 курса 122 учебной группы
младший лейтенант полиции
набора 2012
специальность 40.05.01 - Правовое обеспечение национальной безопасности
(специальность, год набора, № группы)

Руководитель: Профессор кафедры,
кандидат экономических наук, доцент
ст.лейтенант полиции
(ученая степень, ученое звание, должность)
Жуковская Ирина Викторовна
(фамилия, имя, отчество)

Рецензент:

Руководитель следственного органа - начальник СО отдела МВД России по Лаишевскому району подполковник юстиции
(ученая степень, ученое звание, должность)
Халитова Елена Сергеевна
(фамилия, имя, отчество)

К защите_____
(допущена, дата)

Начальник кафедры _____

Дата защиты: "___" _____20___г. Оценка _____

Казань 2017

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Процесс розничных безналичных платежей в сущности своей довольно сложен и предполагает многочисленные пункты доступа к платежной системе, которые могут стать объектом манипуляции правонарушителей с целью совершения мошеннических действий. В этой связи важно определить какое именно звено в цепочке участников платежной системы несет ответственность за причинение ущерба клиенту в случае неправомерных (несанкционированных) списаний. Актуальность приобретает проблема распределения ответственности в случае совершения несанкционированных операций, совершенных с использованием платежных карт. От успешности решения данной проблемы в первую очередь зависит уровень доверия граждан к существующей платежной инфраструктуре. Взаимодействие клиентов с платежными агентами, прежде всего банками, зачастую носят конфликтный характер. Несомненно, во многом этому способствуют сформировавшаяся в современной России законодательная база, регулирующая расчетные правоотношения и сложившаяся платежная практика, упорядочению и изменению которой, по мнению законодателя, должен был послужить Федеральный закон от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе» (далее – Закон 161-ФЗ)[1].

Закон 161-ФЗ частично скорректировал правила осуществления безналичных расчетов, в т.ч. была предпринята попытка устранить пробельность нормативного регулирования эмиссии и использования электронных денег.

Статья 9, вступившая в силу с 01.01.2014 г. стала одним из наиболее противоречивых нововведений Закона 161-ФЗ. Главной целью внесенных изменений стала защита держателей платежных карт от мошенничества.

Степень изученности темы. Данной проблематике посвятили труды ученые-процессуалисты в данной области: Андреев Б.В., Атаманов Р.С., Батурин Ю.М.,

[1] Федеральный закон от 27.06.2011 №161-ФЗ «О национальной платежной системе» (ред. от 29.12.2014) // Российская газета. – №139. – 2011.

Вехов В.Б., Волженкин Б.В., Воробьев В.В., Головин А.Ю., Голубев В.А., Дворецкий М.Ю., Маляров А.И., Номоконов В.А. Селиванов Н. А. Федоров В. Черкасов В. Н.

Объектом исследования являются общественные отношения, обуславливающие установление запрета на преступления с использованием пластиковых карт.

Предметом исследования являются состояние, структура, динамика и другие криминологические параметры, определяющие количественные и качественные особенности за преступления с использованием пластиковых карт.

Цель дипломной работы состоит в изучении основных направлений предупреждения мошеннчества с использованием пластиковых карт.

Задачи дипломной раоты:

- проследить историю развития мошеннических действий с использованием платежных карт,

- охарактеризовать мошенничество с использованием платежных карт: понятие, виды, современное состояние,

- выявить детерминанты преступлений, совершаемых в кредитно-финансовой сфере,

- дать характеристику личности преступника,

- представить зарубежный опыт предупреждения мошеннических действий с использованием платежных карт ,

- рассмотреть общие и специально-криминологические меры предупреждения,

- раскрыть меры предупрежения, основанные на совершенствовании банковских технологий.

Методология исследования. Инструментом в получении фактического материала послужили традиционные методы материалистической диалектики: исторический, формально-логический, системный, сравнительно-правовой, статистический и социологический, а также наблюдение, анализ, синтез, аналогия, абстрагирование, моделирование и обобщение.

Структура работы состоит из введения, трех глав, заключения списка литературы.

Глава 1. Криминологическая характеристика мошеннических действий с использованием платежных карт

§1.История развития мошеннических действий с использованием платежных карт

В последнее время стремительное развитие банковских технологий в сфере безналичных расчетов привело к активному расширению такого платежного инструмента, как кредитные и расчетные карты, которые получили название банковских или платежных карт. В сфере денежного обращения банковские карты являются одним из средств организации безналичных расчетов. Интерес россиян к использованию банковских карт с каждым днем растет, банковские карты прочно вошли в различные сферы экономики и жизни, а именно – в торговую, транспортную, а также в гостиничный, туристический бизнес и др. Свою популярность банковские карты получили в связи с тем, что отпадает необходимость иметь при себе наличными большие суммы денег, что могло бы представлять ряд определенных неудобств. Еще одним преимуществом их использования является то, что осуществление платежей с помощью банковских карт позволяет экономить время на посещение банка и избежать определенных формальностей, связанных со снятием наличных денежных средств с банковского счета[2].

Кроме этого, банковские карты очень удобны для совершения платежей за рубежом, так как позволяют избежать проблем, возникающих с обменом валюты, а также процедурой ввоза-вывоза наличных денежных средств. Еще одним немаловажным преимуществом расчетов с использованием банковских карт является обслуживание платежей физических лиц. Для физических лиц банковские карты представляются удобными тем, что с их помощью в любое

[2] Чирков А.В. Проблемы реализации законодательства о национальной платежной системе в части ответственности банков в расчетных правоотношениях // Банковское право. – М.: Юрист, 2013. – № 5. – С. 63-68.

время можно рассчитаться за приобретенный товар или оказанную услугу и при этом отсутствует необходимость иметь при себе крупные суммы денег.

Использование банковских карт заменяет налично-денежное обращение и позволяет разместить денежные средства, находящиеся на руках у населения, в банках на карточных счетах. При этом объем денежной массы, привлекаемой банками, увеличивается, что влечет к расширению возможностей у кредитных организаций вкладывать кредитные ресурсы в реальный сектор экономики, а это безусловно, стимулирует экономику всей страны в целом.

Как известно, спрос рождает предложение, и увеличение количества держателей банковских карт незамедлительно влечет расширение торгово-сервисных организаций, принимающих эти самые банковские карты к оплате. Это, в свою очередь, повышает легальный оборот денежных средств в торговле, поскольку расчеты с помощью пластиковых карт – это расчеты прозрачные и легальные, так как осуществляются через банковские счета с участием банков. Тем самым при использовании расчетов с пластиковыми картами возникает реальная возможность увеличить легальный оборот денежных средств. Налоговый учет налогоплательщиков и предпринимателей как субъектов торговли станет более прозрачным с точки зрения налогового контроля, более контролируемым налоговым органом.

Рождением современной расчетной карты можно считать 1949 г.

В этом году в Америке образовался Diners club, который представил платежную систему нового типа, предложив директорам розничных торговых точек принимать оплату за товары по пластиковым картам. С тех пор рынок платежный карт и объем совершаемых с их применением операций достигли огромных размеров.

В конце 60-х, через 20 лет после появления первых пластиковых карт в Америке, DCI и «American Express» подписали первое агентское соглашение с ВАО «Интурист» на обслуживание своих карточек в СССР. Следом аналогичные соглашения были подписаны с «Visa» и «Eurocard». Еще через десять лет к этому списку добавились «JCB International». С этого периода иностранные компании

прочно завоевали рынок пластиковых карт на территории бывшего Союза, и так продолжалось вплоть до развала СССР и появления в России коммерческих банков[3].

Свое стремительное развитие и становление рынок пластиковых карт начал после кризиса 1998 г. Наиболее масштабное развитие банковских карт в России приходится на период 2000–2001 гг., поскольку именно в это время были заложены основы карточного бизнеса, развитие которого продолжается и в настоящее время. До 2001 г. развитие происходило за счет отдельных розничных клиентов, получавших карты для поездок на отдых за границу, и небольшого объема выпускаемых зарплатных карт. В 2001 г. начался этап массового внедрения карт через динамичные их продажи в рамках зарплатных проектов. С 2001 г. по октябрь 2005 г. было выпущено 47,4 млн пластиковых расчетных карт. Ежегодный рост эмиссии составил примерно 50 %. В последние годы по пластиковым картам проводится более 900 млн транзакций на сумму более 3 трлн руб. Это наглядно указывает на их активное внедрение и популяризацию в России[4].

Количество пластиковых карт увеличилось в России более чем в пять раз за четыре года. Наряду с этим сформировался новый вид преступности, связанный с изготовлением, сбытом и использованием поддельных карт. Банковские пластиковые карточки, как всякий высокодоходный бизнес, стали мишенью для противоправных посягательств. Преступления, совершаемые с подделкой кредитных и расчетных карт, направлены на мошенническое завладение находящимися в оперативном банковском управлении денежными средствами.

Следует отметить, что подделка пластиковых карт – достаточно сложная, да и дорогостоящая операция, требующая специальное оборудование. Поэтому она

---

[3] Глотов В.С., Шалатов Д.В. Интернет–технологии и электронная торговля: экономика, право, программное обеспечение.–Изд–е 2 — е, перераб. и доп.–В 2-х ч. / Под ред. С.А. Глотова / Центр прав человека и защиты прав потребителей РГТЭУ, Кубанский научный Центр социальных исследований «Законодательная инициатива», Краснодарский ин-т (филиал) РГТЭУ.–М.: НИЦ «Инженер», 2014. С. 183.

[4] Чирков А.В. Проблемы реализации законодательства о национальной платежной системе в части ответственности банков в расчетных правоотношениях // Банковское право. – М.: Юрист, 2013. – № 5. – С. 63-68.

может осуществляться только организованными преступными группами с привлечением специальной техники и технологии. При совершении подобного рода преступлений возможно использование как поддельных пластиковых карт, так и пластиковых карт, надлежаще изготовленных, но содержащих ложные сведения. При этом подделка может быть как полной, так и частичной. Все совершаемые в сфере платежей по банковским картам преступления, в зависимости от конечной цели бывают направленными на получение выгоды от сбыта поддельных банковских карт и на хищение денежных средств, находящихся на банковском счете.

Первая категория преступлений квалифицируется в основном по ст. 187 «Изготовление или сбыт поддельных кредитных либо расчетных и иных платежных документов», вторая – по ст. 159 «Мошенничество» УК РФ. Так, согласно статистике и анализу уголовных дел, мошеннические действия с применением банковских карт совершаются на любой стадии выпуска и функционирования карты, однако чаще всего – в расчетных банках при получении денег в банкоматах и в торгово-сервисной сети, обслуживающей держателей банковских карт.

Подлинные пластиковые карты, которые были похищены, а также утеряны или приобретены обманным путем используются для получения наличных денег в банкоматах либо для покупки товаров или приобретения услуг в организациях, обслуживающих держателей банковских пластиковых карт. При этом используются как подлинные, так и поддельные карты или только их реквизиты. Иногда могут использоваться чеки (слипы) от операций оплаты товаров и услуг посредством карт. Тем самым путем обмана преступники вводят в заблуждение сотрудников торгово-сервисных центров, относительно правомерности пользования данных банковских карт[5].

[5] Глотов В.С., Шалатов Д.В. Интернет–технологии и электронная торговля: экономика, право, программное обеспечение.–Изд–е 2 — е, перераб. и доп.–В 2-х ч. / Под ред. С.А. Глотова / Центр прав человека и защиты прав потребителей РГТЭУ, Кубанский научный Центр социальных исследований «Законодательная инициатива», Краснодарский ин-т (филиал) РГТЭУ.–М.: НИЦ «Инженер», 2014. С. 183.

Обман как способ совершения преступления, состоит в сознательном сообщении заведомо ложных, не соответствующих действительности сведений о правомерности пользования поддельными банковскими кредитными или расчетными картами, при их предоставлении в качестве оплаты, в умышленных действиях, направленных на введение в заблуждение законных владельцев имущества, сотрудников банков, сотрудников торгово-сервисных точек при их использовании с целью последующего хищения чужого имущества. На сегодняшний день подделка банковских карт «лидирует» из всех видов мошенничества. Используя специальное оборудование и знания в области программного обеспечении и компьютерной техники, преступники вносят не соответствующие действительности сведения путем изменения в каждой карточке ее индивидуальных реквизитов, закодированных в магнитной полосе и содержащих информацию о номере карты, сроке ее действия, данных владельца.

Одним из видов мошенничества с подлинными банковскими картами является открытие счета в банке по поддельному, утерянному или украденному паспорту на минимально установленную для этого банком сумму с целью получения банковской карты с последующим хищением денег. Кроме этого, подлинные банковские карты могут использоваться для приобретения товаров и услуг. При этом незаконные действия сопровождаются подделкой подписи законного держателя карты либо предъявлением поддельного документа от его имени.

Мошеннические действия, совершаемые с применением фальшивых банковских карт, направлены на подделку банковских карт полностью или частично. Как правило, на их заготовки наносится логотип эмитента, поле для проставления подписи и в точности воспроизводятся все признаки защиты (используются подлинные реквизиты реально существующих карточек). Полностью карта подделывается двумя способами, а именно имея образец подлинной карты какой- либо платежной системы, мошенники на кусок пластика соответствующего размера наносят все присущие данной карте реквизиты, элементы защиты и идентификационные признаки – эмбоссированную

(рельефную) часть и магнитную полоску.

Либо на подлинной карте фальсифицируются только идентификационные признаки – «перекодируется» магнитная полоса, при этом стирается существующая запись и наносится новая или срезается ранее сделанная рельефная часть и на ее месте путем выдавливания наносится новая часть. Большое количество преступлений совершается с частично подделанными картами.

Частичная подделка заключается в нанесении на пластик стандартного размера только эмбоссированной части либо защитной магнитной полосы. С подлинной карты магнитная полоса копируется или перекодируется. На нее с помощью специальной аппаратуры наносится информация со слипа настоящей карты.

На магнитной полосе находится информация, занесенная электронным способом. Эта информация считывается пос-терминалом или другим специальным устройством, которыми снабжены предприятия торговли или услуг, обслуживающие держателей пластиковых карт, а также банкоматы.Еще одним распространенным видом преступлений являются незаконные операции, когда недобросовестные работники банков или предприятий, занятые изготовлением карточек, пользуются задержкой между открытием счета и доставкой карточки владельцу для совершения по ней операций. Иногда владельцы карточек сами делают ложные заявления о произошедшей краже и потере карточек. Пока процессинговый центр включит номер карточки в стоп-лист и известит торговые точки, проходит несколько дней. За это время владелец проводит с карточкой максимальное число операций, а затем предъявляет банку свои претензии.

Особый интерес для преступников представляют банковские пластиковые карточки, пересылаемые по почте. Кража обнаруживается с большим опозданием, в результате отсутствует возможность немедленного блокирования счета. К моменту кражи карточки, как правило, не подписаны, а значит злоумышленник может поставить свою подпись и легально использовать карточку по своему усмотрению. Выявлены случаи, когда преступники специально устраивались

работать на почту или в частные службы доставки, чтобы иметь возможность изымать конверты с пластиковыми банковскими карточками.

В ходе расследования подобных преступлений существует целый ряд проблем. Как правило, затруднения при расследовании указанных преступлений возникают в связи с определением предмета преступления. Предмет данного преступления – кредитные карты, расчетные карты и иные платежные документы.

Карта является лишь средством, инструментом осуществления безналичных расчетов (т.е. идентификационной картой – средством идентификации самой карты, держателя карты, а в случае необходимости, и хоста в рамках той или иной платежной системы). Сама по себе карта имеет незначительную стоимость, ценность представляют денежные средства, к которым с помощью карты можно получить доступ. Этот доступ осуществляется путем направления в банк документов (составленных с использованием платежных карт или их реквизитов) на бумажном носителе и (или) в электронной форме. Документ по операциям с использованием платежной карты является основанием для осуществления расчетов по указанным операциям и (или) служит подтверждением их совершения[6].

В настоящий момент трудно спрогнозировать насколько изменится платежная практика с введением в действие ст. 9 Закона 161-ФЗ.

Представляется, что доработка ст. 9 законодателем продолжится. Однако вне зависимости от корректировки правовых норм, устанавливающих распределение ответственности банка и клиента в случае несанкционированных списаний денежных средств, уже сегодня российские банки предрекают рост случаев мошенничества.

По мнению некоторых специалистов сегодня закон «стимулирует» некоторых клиентов к недобросовестному поведению. Здесь речь идет, прежде

---

[6] Глотов В.С., Шалатов Д.В. Интернет–технологии и электронная торговля: экономика, право, программное обеспечение.–Изд–е 2 — е, перераб. и доп.–В 2-х ч. / Под ред. С.А. Глотова / Центр прав человека и защиты прав потребителей РГТЭУ, Кубанский научный Центр социальных исследований «Законодательная инициатива», Краснодарский ин-т (филиал) РГТЭУ.–М.: НИЦ «Инженер», 2014. С. 183.

всего, о так называемом «дружеском фронде»[7]. Как показывает опыт ЕС, до 60 % объема мошеннических транзакций в денежном выражении приходится на CNP-транзакции (операции, произведенные без физического присутствия карты). Этот сегмент мошенничества стал наиболее быстроразвивающимся[8].

У банков в случае фрод-инцидента существует два сценария поведения:

1) признание банком фронда и возврат клиенту денежных средств;

2) квалификация совершенной операции как мошенничества со стороны клиента. Правом банка в данном случае является обращение в правоохранительные органы. Факт мошенничества должен быть доказан в суде. Последний подход, представляется, наиболее логичным, т.к. перекладывание бремени доказывания невиновности на физическое лицо, являющееся априори слабой стороной в расчетных правоотношениях, в данном случае нецелесообразно.

Кроме того, законом предусмотрен инструмент «контроля» – проведение банком формальных проверок, предусмотренное ч. 15 ст. 9. В таком случае итогом расследования, проводимого по итогам фронд-мониторинга и установившего правильность введения ПИН-кода, является признание клиента ответственным за осуществленную операцию. В любом случае, вне зависимости от роста рисков мошенничества, очевидно, что одним из наиболее важных позитивных последствий «адаптации» законодателем принципа «нулевой ответственности» в том виде, в котором он закреплен в ст. 9, для развития платежной инфраструктуры в России состоит в «вынужденной» идеологической и технологической модернизации платежных систем, расширению внедрения платежными операторами новых технологий.

Так, проблема скимминга может быть частично решена посредством стимулирования эмиссии EMV-продуктов, массового перевода крупными

---

[7] Есаков П., Чернышев А. Банковская отрасль на пороге выхода из «SMS-тупика»? [Электронный ресурс] // Computel. ПЛАС. – 2014. –№ 4 [203]: апрель. – Режим доступа: http://computel.ru/upload/Computel_newpix_ caps2.pdf.

[8] Главной угрозой остается CNP-фрод [Электронный ресурс] // ПЛАС- журнал. – 30.04.2014. – Режим доступа: http://www.plusworld.ru/journal/online/art170778/

банками-эмитентами своего карточного портфеля на чип. В целом если говорить о дальнейшем совершенствовании положений ст. 9 Закона 161-ФЗ, следует указать, что баланс интересов при распределении ответственности за несанкционированное списание денежных средств возможно обеспечить только с учетом индивидуальных рисков участников расчетных правоотношений, а также их собственной способности (возможности) этот риск снизить.

Стратегии снижения рисков мошенничества в рассматриваемом случае должны включать перераспределение рисков между участниками платежной системы и их страхование.

Застраховать себя от мошенничества со стороны клиентов банки могут несколькими путями:

1) установление штрафов для клиентов на случай доказанного мошенничества держателя карты;

2) регулирование сроков возврата денежных средств – незамедлительный возврат клиенту минимальной суммы, при условии компенсации оставшейся части списанных средств после проведения расследования;

3) подробная регламентация в договорах с клиентами процедуры возмещения несанкционированно списанных денежных средств в части неурегулированной ст. 9 Закона 161-ФЗ;

4) совершенствование методик оценки рисков мошенничества и разработка программ по повышению осведомленности клиентов.

Итак, преступления, совершаемые с подделкой кредитных и расчетных карт, направлены на мошенническое завладение находящимися в оперативном банковском управлении денежными средствами.

Следует отметить, что подделка пластиковых карт – достаточно сложная, да и дорогостоящая операция, требующая специальное оборудование. Поэтому она может осуществляться только организованными преступными группами с привлечением специальной техники и технологии. При совершении подобного рода преступлений возможно использование как поддельных пластиковых карт, так и пластиковых карт, надлежаще изготовленных, но содержащих ложные

сведения. При этом подделка может быть как полной, так и частичной. Все совершаемые в сфере платежей по банковским картам преступления, в зависимости от конечной цели бывают направленными на получение выгоды от сбыта поддельных банковских карт и на хищение денежных средств, находящихся на банковском счете.

§2.Мошенничество с использованием платежных карт: понятие, виды, современное состояние

Существует три вида платежных карт: кредитные карты; дебетовые карты, которые привязаны к отдельному депозиту; предоплаченные карты – анонимные, доступные для общего пользования карты, где стоимость хранится на отдельном для каждой карты депозите у эмитента, или привязанные к закрытой системе (например, подарочные карты конкретных ритейлеров).

Дебетовые и предоплаченные карты часто предполагают возможность использования ПИН-кода для проверки подлинности пользователя, а в кредитных картах для этих целей в основном используется магнитная полоса.

Платежные карты в силу объективных причин восприимчивы к различным мошенническим атакам. С позиции широкого подхода мошенничество в сфере платежных карт может быть определено как любая деятельность, в которой используется личная конфиденциальная (финансовая) информация для незаконных целей, включая инициацию незаконных транзакций без авторизации плательщика. Чаще всего данная деятельность включает подделку платежных инструментов, перехват данных и др. Распространено мошенничество посредством банкоматного скимминга и операции без присутствия карты (card not present) – конфиденциальную информацию похищают при оплате покупок в сети Интернет. Последние тенденции на мировом платежном рынке свидетельствуют о том, что происходит миграция мошенничества из «банкоматного сектора» в

сектор интернет-торговли. Согласно исследованию, проведенному аналитической компании Fair Isaac Corporation, по итогам 2016 года Россия стала одним из лидеров среди стран Европы по темпам увеличения случаев мошеннических действий с банковскими картами. Динамика роста случаев мошенничества с банковскими картами и электронными деньгами, отслеживаемая Банком России, подтверждает, что количество инцидентов, связанных с нарушением требований безопасности при переводе денежных средств, в 2014 г. составило 1562, а по итогам первого полугодия 2016 года – 2484 подобных случая (прирост составил 59 %).

Согласно основным направлениям преступной деятельности можно выделить следующие типы:

1. «Виртуальный товарообмен».
2. «Легкие деньги».
3. Лже-благотворительность.
4. Мошенничество в сфере интернет-знакомств.
5. Телеработа, удаленный заработок.
6. Мошенничество в сфере услуг.
7. Инвестиционные мошенничества.
8. Компьютерное мошенничество.

Виртуальный товарообмен является распространенной разновидностью преступных схем в Интернет. Формальным прикрытием такой схемы в этом случае выступает договор купли-продажи между участниками электронной торговли. Внутри данной группы можно выделить две схемы: мошенничество на он-лайн аукционах и создание лже-предпринимательских (фирм-однодневок) в преступных целях. В первом случае преступники чаще выступают в качестве физических лиц-контрагентов по сделкам купли-продажи, совершаемых через Интернет. При этом взятые на себя обязательства по доставке и передаче якобы выставленного на продажу товара они не исполняют.

Так, 29-летний ранее судимый за кражу и мошенничество житель г. Остров Псковской области Ю.Б. Николаев выманил у потерпевшихнумизматов – 19050

рублей, размещая предложения о продаже старинных российских монет, 19-го и начала 20 века на интернет-аукционе. Для легализации полученных средств он сообщал паспортные и личные данные своих сообщников, которые менялись при каждой сделке. Сообщники получали деньги на Островском почтамте, и делили их между собой. Организатора суд приговорил к 3 годам 8 месяцам лишения свободы с отбыванием наказания в колонии-поселении[9].

Характерной особенностью проведения расчетных операций за «совершенную сделку» является использование способа оплаты, по которому установить конкретного получателя не представляется возможным. Например, все современные электронные платежные системы позволяют злоумышленнику открыть электронный счет на условиях анонимности.

Другой способ связан с открытием виртуальных проектов-однодневок. В данном случае он тесно связан со лжепредпринимательством, которое ныне декриминализировано, что не позволяет как прежде вменять совокупность статей, тем самым ужесточая ответственность за подобные сложноорганизованные формы мошенничества. Данная схема отличается тем, что преступник «маскируется» под фирму-организацию (интернет-магазин) и в отличие от мошенников на интернет-аукционах иногда все же доставляет товары, но не надлежащего качества, взамен обещанных (например, подделку или другой товар). Так, 16.03.2010 года Фрунзенским районным судом г. Владивостока был вынесен приговор в отношении гр-на Д.Б. Степочкина, 1988 г.р., который в течение 2008-2009 г.г. совершал мошенничества через глобальную сеть Интернет, организовав лже-магазин[10]. От противоправных деяний Степочкина пострадали более 20 человек. За совершение преступлений, предусмотренных ст. 159 УК РФ, подсудимому назначено наказание в виде четырех лет лишения свободы условно и обязанностью погашения материального ущерба всем потерпевшим, в сумме

---

[9] См.: Уголовное дело № 1-96/2010. Архив Островского городского суда Псковской области. 2 См.: Левит М. Преступления и наказания в сфере высоких технологий: мошенничества в сети Интернет / «Каскад» [Электронный ресурс] – Миасс, 22 октября 2006. – URL: http://cascad456300.ru/index.php?type=2&id=1161528934 (дата обращения: 07.01.2011).

[10] См.: Уголовное дело № 1-99/2010. Архив Фрунзенского районного суда г. Владивостока

более одного миллиона рублей.

Еще одной вариацией на тему быстрого обогащения выступает схема – «легкие деньги». В данном случае преступники апеллируют ко вполне естественным, но не самым лучшим качествам человека: жадности, что в итоге приводит к росту естественной латентности таких деяний. Среди особенностей преступных приемов Рунета[11] следует отметить следующие схемы.

Секретные кошельки WebMoney[12].

Данная схема имеет и другие распространенные названия: «Золотой кошелек», «Волшебный аккаунт», «Золотой аккаунт», «Двойной баланс». Суть схемы состоит в обещании удвоения (утроения) посланных на него денежных средств в течение нескольких дней или часов. Подобные способы преумножения средств мошенники объясняют различными причинами. Данный способ до сих пор не изжил себя, хотя повсеместно признан мошенничеством. Он постоянно совершенствуется, появляются новые варианты.

Первые «волшебные кошельки» появились в 2001 – 2002 гг. Это были сообщения об игроках на биржах, об инвесторах, которые привлекали «заемные средства вкладчиков», предлагая преумножить вложенный «капитал» на 100 – 150 % за несколько дней. Однако подобные проекты не получили широкой популярности. После нескольких операций суть схемы становилась известна интернет-пользователям и сразу же предавалась гласности. Широко

---

[11] Возможна более узкая формулировка, гласящая, что Рунет – это часть Всемирной паутины, принадлежащая к национальному российскому домену «.ru», однако она не отражает реальной ситуации, так как «относящиеся к Рунету» (то есть русскоязычные) ресурсы могут располагаться в любых доменах (или не иметь домена), а соответствующие серверы могут физически находиться в любой стране мира. Термин изобрел весной 1997 года Раффи Асланбеков и внедрил в круг своего русскоязычного интернет-культурного общения, где термин быстро прижился. Какой-то период некоторая часть пользователей критиковала термин, считая его не очень благозвучным. Тем не менее, в 2001 году слово с заглавной буквы с формулировкой «Рунет, -а (российский Интернет)» (некорректной из-за неоправданного отождествления русского и российского) вошло в орфографический словарь РАН под редакцией В. В. Лопатина

[12] Учетная система WebMoney Transfer обеспечивает проведение расчетов в реальном времени посредством учетных единиц – титульных знаков WebMoney (WM-units). Система является небанковской. Управление движением титульных знаков осуществляется пользователями с помощью клиентской программы WM Keeper или с помощью веб-интерфейса (WM Keeper Light). Дата создания: 1998 год, количество зарегистрированных пользователей 6 млн.

растиражированная новость во всемирной паутине практически отрезала путь преступникам к их потенциальным жертвам. После первой волны получили распространение письма от якобы бывших и несправедливо уволенных сотрудников WebMoney, которые сообщали о тайных кошельках системы. Особое свойство этих кошельков заключалось в автоматическом возврате удвоенной суммы средств, посланных на эти кошельки через несколько часов или дней. Необъяснимость надобности создания подобных кошельков для WebMoney постепенно свела на нет подобные предложения.

В 2004 – 2005 годах волшебные кошельки были повсеместно объявлены мошенничеством, не без активного участия самой компании ЗАО «Вычислительные силы» держателя сервиса WebMoney. На это незамедлительно последовал ответ – схема трансформировалась: в виде спама рассылались сообщения, в которых указывалось, что мошенники один-два раза посланные деньги до 5-10 WMZ и 50-100 WMR1 возвращают для привлечения новых, более крупных средств. Авторы спама якобы являются доброжелателями и предлагают обмануть мошенников, послав им мелкие суммы. На самом деле спамеры и являются владельцами указанных кошельков.

С середины 2006 года определенную популярность получил такой вид мошенничества, как «двойной баланс», якобы рассылаемый от системы WebMoney. Распространяются даже вирусы, запускающие сообщение о выигрыше «двойного баланса» при запуске клиентской программы – так называемого WM Keeper-a.

Менее «волшебных кошельков» популярны «волшебные аккаунты» других платежных систем: E-gold, RUPay и других электронных платежных систем. Несмотря на то, что сервис WebMoney активно борется с мошенниками, количество мошеннических сообщений не снижается. Держатели (владельцы) электронных платежных систем рекомендуют пользователям сообщать о всех случаях подобного мошенничество в службу поддержки. Аккаунты мошенников в данном случае блокируются до выяснения обстоятельств. Интернет-пирамиды. Финансовые пирамиды известны нашей стране.

В глобальной сети Интернет данное явление также получило широкое распространение, но десятилетие спустя. В любом случае мы, имеем дело с финансовой системой перераспределения денег, участники которой получают прибыль из средств других участников, что вступили в систему после них и через их посредничество (не обязательно прямое). Однако характерной чертой интернет-проектов являются частные случаи, когда никакой пирамиды (бизнеса, MLM-матрицы и т.д.) вообще нет, и рассылаемые рекламные предложения – это просто сбор денег с единственного нижнего уровня «пирамиды».

Потерпевший может заплатить первоначальный взнос и начать искать других участников, но это будет крайне трудно сделать, поскольку организаторы такой схемы постараются сами охватить как можно большее число пользователей Интернета. Интернет-пирамиды не следует смешивать с инвестиционным мошенничеством в глобальной сети.

Финансовые пирамиды начала 90-х годов действительно являлись инвестиционным мошенничеством. Интернет-пирамиды не имеют необходимых качественных признаков: отсутствуют официально заверенные договоры, соглашения о членстве, о гарантированной прибыли и прочее. Выигрыш в лотерею. Суть схемы заключается в сообщении пользователю Интернет о фиктивном выигрыше, в процессе «получения» которого возникают дополнительные трудности, требующие соответствующих расходов. Размер самих «затрат» гибко варьируется мошенниками, для чего они обычно просят заполнить анкету в электронном виде, которая покажет приблизительное материальное положение потерпевшего.

«Нигерийские письма»[13].

Один из самых известных видов преступлений в сфере высоких технологий получил наибольшее распространение с появлением массовых рассылок по

[13] В странах Западной Европы проблема нигерийских писем носит настолько массовых характер, что вопросам противодействия этой мошеннической схеме была посвящена специальная конференция «an International Conference on Advance Fee (419) Frauds in New York», состоявшаяся 17 сентября 2002 года, на которой выступали официальные представители правительства Нигерии

электронной почте (спама). Письма названы «нигерийскими» потому, что первые письма с предложениями посылались именно из этой страны, причем еще до возникновения Интернета, по обычной почте. Однако нигерийские письма приходят и из других африканских стран, а также из городов с большой нигерийской диаспорой (Лондон, Амстердам, Мадрид, Дубайи). Значительную роль в распространении нигерийских писем играли молодые студенты или выпускники нигерийских университетов, не нашедшие надлежащей работы. Суть мошеннического предложения состоит в том, что у получателя сообщения просят помощи в отмывании многомиллионных сумм бывших африканских диктаторов, сотрудников министерств и пр., обещая солидные проценты вознаграждения.

Преступления в сфере высоких технологий профессионально организованы: у мошенников есть офисы, работающий факс. Преступники часто связаны с правительственными организациями, и попытка получателя письма провести самостоятельное расследование, как правило, не обнаруживает противоречий в легенде. Сделка подается как «безвредное» беловоротничковое преступление, что мешает жертве обратиться к властям.

В нашей стране нигерийские письма не столь распространены как в США и странах западной Европы. Вместе с тем утверждать об их полном отсутствии нельзя. Хотя уже много лет в средствах массовой информации детально объясняется механизм преступлений, массовость рассылки приводит к тому, что находятся все новые и новые жертвы, отдающие мошенникам крупные суммы денег.

Супер-стратегии в казино.

В условиях, когда игорный бизнес в Российской Федерации выведен за пределы населенных пунктов в специальные игорные зоны, интернет-казино смогут составить им успешную конкуренцию, поскольку проблема юрисдикции решается простым переносом сервера в государство с более либеральным законодательством. Деятельность подобных игорных учреждений не лицензируется и никем не контролируется, что выступает в качестве значимого криминогенного фактора. Более того, зачастую для привлечения клиента самими

владельцами интернет-казино запускается широкая рекламная компания, предлагающая некий программный продукт или описание системы игры в том или ином заведении, благодаря чему выигрыш посетителю обеспечен. Сама стратегия часто сводится к системе Мартингейла[14], суть которой в том, что в конечном итоге человек проигрывает очень крупную сумму денег.

Может быть предложена и более сложная стратегия игры, но в любом случае она будет проигрышной. Сегодня преступники в России активно используют идею благотворительности в целях личного обогащения. Преступные действия с благотворительными фондами обычно активизируются после природных катаклизмов и других катастроф. Преступники выдают себя за настоящие благотворительные организации и с помощью электронной почты и веб-сайтов собирают «пожертвования» граждан. Для этого мошенники зачастую просто копируют содержание сайтов благотворительных организаций, указывая расчетные счета подставных фирм, через которые обналичивают деньги.

Так, Василеостровский районный суд города Санкт-Петербурга признал виновным В.Е. Балберова в совершении ряда мошенничеств. В частности, подсудимый распространил в Интернете, в том числе и в социальной сети «В контакте», ложную информацию о наличии тяжело больной девочки Раисы Лукашевич, проживающей в Новгородской области. Она якобы была больна онкологическим заболеванием и не имела возможности получить дорогостоящее лечение-операцию. Балберов попросил о помощи для лечения больного ребенка. Откликнувшимся людям был причинен существенный ущерб на суммы от одной тысячи 700 рублей до 50 тысяч рублей. Кроме того, обвиняемый получал с граждан денежные средства в качестве оплаты за проведение несуществующих дистанционных курсов «Журналистика», «Японский язык и культура», «Техника

[14] Система Мартингейла – система управления ставками в азартных играх. Суть системы заключается в том, что игра начинается с некоторой заранее выбранной минимальной ставки. После каждого проигрыша игрок должен увеличивать ставку так, чтобы в случае выигрыша окупить все прошлые проигрыши в этой серии, с небольшим доходом. В случае выигрыша игрок должен вернуться обратно к минимальной ставке.

текста. Стилистика», «Стилистика русского языка»[15].

В сети Интернет получил широкое распространение такой тип преступлений, как обман иностранцев, желающих найти спутницу жизни из России через брачные интернет-агентства. В поле их зрения находятся мужчины из Соединенных Штатов, Великобритании, Австралии, Канады и Новой Зеландии, указавшие информацию о себе на сайтах знакомств. Схема мошенничества рассчитана на доверчивость иностранцев, которые отдавали деньги в качестве оплаты билетов и виз русским невестам. Такая схема даже имеет свое название «русские невесты».

Современная Россия во многих смыслах является идеальным местом для совершения таких преступлений. Здесь живут образованные люди, страдающие от низкой зарплаты и существенной безработицы. Так, в ноябре 2006 года в Екатеринбурге был вынесен обвинительный приговор по аналогичному делу. Подсудимые в 2000 году организовали под видом брачного агентства сайт знакомств «Русские девушки». У жертв преступления – потенциальных женихов, таким образом, было изъято около 27 тысяч долларов. Всего же потерпевшими по делу были признаны 15 человек. В основном, интерес к сайту проявляли граждане США, Великобритании и Канады. Преступная группа состояла из программиста Владимира Осипова и студентки финансово-юридического института Алены Федоровской, специально посещавшей усиленные курсы английского языка[16].

Преступления подобного рода получило настолько широкое распространение, что посольство Соединенных Штатов в Москве получает от обманутых американцев от пяти до десяти жалоб ежедневно. По словам сотрудников американского посольства, жертв убеждает убедительность сценария и хорошее качество поделок. Переписка ведется очень терпеливо, иногда в нее специально включают истории, которые свидетельствуют о честности и доброте

---

[15] Уголовное дело № 1-430/2010. Архив Василеостровского районного суда города Санкт-Петербурга.

[16] Уголовное дело № 2-457/2006. Архив Верх-Исетского районного суда г. Екатеринбурга. 2 Internet Dating Scams / Embassy of the United States in Russia. [Электронный ресурс]. – 2007. – URL: http://www.usembassy.ru/consular/acs.php?record_id=datingscam (дата обращения: 12.10.2007).

персонажа.

В последнее время все большее количество людей интересуются удаленной работой. Но, к сожалению, к ней начали проявлять внимание не только программисты, переводчики, дизайнеры, но и огромное количество мошенников – глобальность, удобство и скорость, – позволили просто и с меньшим риском совершать обманы в сфере трудоустройства. Многие пользователи знают, что современные компании стремятся рассредоточить свой бизнес в пространстве.

Благодаря Интернет взаимосвязь между различными подразделениями и рабочими группами поддерживается весьма оперативно. Характер деятельности при удаленной работе бывает очень разным – создание программных продуктов, дизайн Web-сайтов, переводы и т. п.

Наряду с мошенничеством в области купли-продажи товаров мошенничество в сфере услуг является весьма перспективным направлением для предприимчивых мошенников. Некоторое время назад была популярна идея бесплатных звонков с мобильных телефонов. Суть данного мошенничества состоит в том, что мошенник убеждает жертву, будто бы нашел способ сделать звонки с мобильного телефона бесплатными. За определенное вознаграждение мошенники предлагают загрузить с их сайта необходимое программное обеспечение, после чего те смогут совершать неограниченные бесплатные звонки. По этой же схеме построено и мошенничество, предлагающее организовать бесплатный доступ в Интернет. Однако мошенникам необходимо постоянно совершенствовать способы обмана. Теперь подобные предложения все чаще стали рассылаться не по электронной почте или публиковать на электронных досках объявлений, а рассылать в виде SMS-сообщений на мобильные телефоны. Стали известны случаи, когда абоненты, сами того не зная, подписываются на ежемесячное списывание денег со своего счета.

Еще одна группа «традиционных» преступлений в сфере высоких технологий в рамках данной классификации – инвестиционные мошенничества в сети Интернет. По мере расширения технологических возможностей сети Интернет все большее количество бизнес-структур и финансовых институтов

используют глобальную сеть в работе. Это в полной мере относится к таким явлениям современной жизни, как интернет-трейдинг, прямые инвестиции и пр. Сейчас к услугам трейдеров предоставлены многочисленные информационные ресурсы.

Основными способами обмана в данной области являются дезинформирование инвесторов относительно того или иного положения дел на фондовом или валютном рынке с целью вынудить их совершать выгодные мошенникам сделки. Например, мошенники покупали акции, а затем рекомендовали их посредством электронной почты и инвестиционных сайтов, не упоминая о том, что владеют данными бумагами. После роста котировок, созданного привлеченными жертвами, они продавали свои бумаги. Распространенной схемой, присущей именно российской действительности, является мошенничество с созданием брокерских контор для торговли через Интернет на международном валютном рынке FOREX.

Мошенники, привлекая клиентов, утверждают, что торговля на бирже может принести большие деньги в короткий промежуток времени. Однако как удалось выяснить, около 97 % клиентов компании теряют свои депозиты в очень короткие сроки. 2 Подобные конторы не являются кредитными организациями и не имеют лицензий для работы на финансовых рынках, не предоставляют клиентам реального доступа на международный финансовый рынок, функционируя по принципу казино, даже обладая необходимым программным обеспечением и технической базой для ведения валютного трейдинга. Таким образом, инвестиционные мошенничества в Сети представляют собой закономерный результат развития информационно-коммуникативных технологий и построенных на их основе стратегий ведения бизнеса. Нужно отметить, что пока глобальная сеть накладывает определенные ограничения на развертывание мошенничества в информационной среде. Некоторые виды обычного (или как мы будем говорить в дальнейшем «традиционного») мошенничества не могут быть совершены посредством Интернет до тех пор, пока соответствующие общественные отношения не будут перемещены на информационную основу.

Следующим элементом типологии является компьютерное мошенничество, та его разновидность, что получила распространение в Интернет: Identity Fraud или «Кража личности».

Суть подобных деяний заключается в незаконном получении персональной идентификационной информации, которая в последующем может служить для хищений, причинения имущественного ущерба от имени законного владельца, либо последующего вымогательства. Если проводить аналогию с существующими реалиями Identity Fraud можно сравнивать с рейдерским захватом имущества, либо прав на него. К примеру, в мае 2007 года Дмитрий Фомин, используя домашний компьютер, через Интернет незаконно получил информацию об именах и паролях клиентов ОАО «Альфа-Банк». С помощью этих данных он осуществил несанкционированный доступ к их счетам интернет-систему «Альфа-клик». Действуя от имени потерпевших, он приобрел на их же средства пай инвестиционного фонда «Альфа-Капитал Индекс ММВБ». Несколько позднее ему удалось обналичить 266 тысяч рублей путем их продажи. 18 сентября 2007 года Фомин попытался совершить еще одно преступление путем неправомерного доступа к счету клиента интернет-магазина «ozon.ru», с которого он попытался похитить денежные средства. Однако потерпевший, обнаружив действия Фомина, вовремя обратился к владельцам ресурса, чем предотвратил преступление. Фомину было предъявлено обвинение по ч. 1 ст. 272 УК РФ (неправомерный доступ к компьютерной информации), ч. 2 ст. 159 (мошенничество) УК РФ, ч. 3 ст. 30 и ч. 1 ст. 159 УК РФ (покушение на мошенничество), ч. 1 ст. 174.1 (легализация (отмывание) денежных средств, приобретенных лицом в результате совершения им преступления) УК РФ. 1 «Кража личности» тоже не однородна[17].

Проведя анализ способов совершения преступлений, нам удалось установить, что данное явление можно разделить на три категории: «Фишинг» (phishing) (англ.) представляет собой производное от следующих двух слов: password – пароль и fishing – рыбная ловля, выуживание.

Что, в сущности, означает незаконное получение идентификационных

[17] Уголовное дело № 1-60/2009. Архив Борисоглебского городского суда Воронежской области

данных пользователей путем создания «наживки» – фальшивых сайтов, являющихся точной копией оригинальных. Подобного рода мошенничество получило в глобальной сети широкое распространение и основано на принципах социального инжиниринга. При помощи спам-технологий мошенники могут рассылать миллионы фишингсообщений по электронной почте, которые выглядят как обращения, присланные с популярных или вызывающих доверие веб-узлов, например, от банка или компании по выпуску кредитных карт.

Для обеспечения эффекта правдоподобности используются логотипы банка, имена и фамилии реальных руководителей. В таком письме, как правило, сообщается о том, что изза смены программного обеспечения в системе интернет-банкинга пользователю необходимо подтвердить или изменить свои учетные данные. В качестве причины для изменения данных могут быть названы выход из строя программного обеспечения банка или же нападение хакеров. Во всех случаях цель таких писем одна – заставить пользователя перейти по приведенной в тексте письма ссылке, а затем ввести свои конфиденциальные данные на ложном сайте.

К тому моменту довольно четко проявились два основных метода, к которым фишеры прибегали в своих операциях: проблемы платежных систем. Представляет собой наиболее простой метод кражи персональной информации. Посредством спам-рассылки распространяется сообщение, в котором содержится просьба выслать идентификационные данные на указанный адрес электронной почты. Таким образом, например, были совершены первые фишинговые атаки против интернет-пользователей известного американского провайдера AOL в 1996 году. подделка сайтов платежных систем. В данном случае к массовой рассылке ложных сообщений добавляется создание фальшивого сайта, на котором осуществляется хищение персональной информации. Данный вид мошенничества уже более сложен, потому что требует определенных навыков в программировании, регистрации сайта со сходным именем на подставное лицо.

Поэтому зачастую данная схема уже реализуется организованной группой[18].

Мошенники не могут использовать одну и ту же схему до бесконечности. Появление в конце 2003 года эксплойта уязвимости с подменой реального URL3 привело к появлению нового вида «фишинга» – «спуфинг» (spoofing).. В случае использования данной уязвимости атакуемый пользователь визуально может наблюдать настоящий адрес банковского сайта в адресной строке браузера, но находиться сам при этом будет на поддельном сайте. Сегодня во время пребывания на таком сайте, даже, если пользователь не вводит никаких данных на его компьютер начинает загружаться «троянская» программа, способная сама выявить все интересующие мошенника данные и при подключении к Интернет отправить их своему владельцу.

Таким образом, главное отличие «фишинга» от «спуфинга» заключается в том, что в первом случае жертва преступления сама способна (при должной осмотрительности) распознать обман, а во втором случае это уже невозможно в силу уязвимости программного обеспечения самой компьютерной системы. Именно поэтому виктимологическая профилактика против «спуфинга» оказывается практически бесполезной. Несколько особняком стоит «кардинг» (carding), как форма компьютерного мошенничества, известный и в своих «несетевых» аналогах. Суть мошеннической схемы заключается в использовании чужих реквизитов платежных средств: дебетовых и кредитных банковских при расчетах за покупку. Данная мошенническая схема достаточна сложна в исполнении, зачастую реализуется организованными группами. Санкт-Петербургский городской суд в июле 2010 года вынес приговор по одному из таких дел. Организаторы преступного сообщества Ракутько Кирилл Викторович и Шихалев Алексей Витальевич при участии еще четырех сообщников за год преступной деятельности смогли завладеть двумя с половиной миллионами рублей, принадлежащих банковским структурам. Преступное сообщество было создано с целью изготовления поддельных кредитных и расчетных карт.

[18] Чирков А.В. Проблемы реализации законодательства о национальной платежной системе в части ответственности банков в расчетных правоотношениях // Банковское право. – М.: Юрист, 2013. – № 5. – С. 63-68.

Совершению преступлений способствовали знания Ракутько, полученные в Государственном университете информационных технологий, механики и оптики. Изготовляя поддельные банковские карты, они совершали покупки с использованием поддельных паспортов и водительских удостоверений держателей этих карт. Кроме того, на одном из специализированных сайтов Интернета, посвященном мошенничеству в сфере обращения кредитных и расчетных карт, они разместили рекламу об изготовлении на заказ и продаже пластиковых карт, после чего приступили к их распространению. Все обвиняемые были признаны виновными в создании и участии в преступном сообществе (статья 210 УК РФ), изготовлении в целях сбыта и сбыте поддельных кредитных либо расчетных карт (статья 187 УК РФ), мошенничестве (статья 159 УК РФ) и подделке документов (статья 327 УК РФ). Приговором суда организаторам преступного сообщества, Ракутько и Шихалеву, назначено наказание в виде лишения свободы на срок 10 лет и 8 лет 6 месяцев соответственно, с отбыванием наказания в колонии строгого режима. Кроме того, Ракутько был оштрафован на 250 тыс. рублей, а Шихалев – на 200 тысяч рублей[19].

В Интернет данная форма преступной деятельности получила дальнейшее развитие, упростив претворение в жизнь преступных замыслов. Для совершения платежа в Интернет нет необходимости изготавливать дорогостоящий дубликат пластиковой карты, достаточно знать ее реквизиты. Знание пин-кода при этом не обязательно. Это помогает мошенникам избегать уголовной ответственности по ст. 187 УК РФ за изготовление или сбыт поддельных кредитных либо расчетных карт и иных платежных документов. Во-вторых, в Интернет существуют иные платежные системы («электронные деньги»), пока не связанные с банковской системой РФ, но предоставляющие определенные имущественные права пользователям своих систем, которые также становятся жертвами мошенников. В область нашего научного интереса попадает также и «фрикинг» (phreaking) – причинение имущественного ущерба путем обмана и злоупотребления доверием. Широкое распространение этот вид компьютерного мошенничества получил на

[19] См.: Уголовное дело № 2-5/2010. Архив Санкт-Петербургского городского суда

заре развития Интернет в России, когда доступ во всемирную сеть не был столь дешев как сегодня.

Суть преступного деяния состоит в том, что, пользуясь чужими учетными записями для доступа в Интернет, злоумышленник своими действиями наносит вред провайдеру и законному пользователю. Сегодня этот вид преступной деятельности сокращается в связи с повсеместным внедрением широкополосного доступа в Интернет, снижением стоимости безлимитных тарифов.

Таким образом, сегодня существуют две относительно самостоятельные группы преступлений, именуемых нами преступлениями в сфере банковских технологий: традиционные преступные схемы, реализуемые посредством пластиковых карт, и преступность с использованием пластиковых карт совершаемая посредством Интернет.

Глава 2. Причинный комплекс мошеннических действий с использованием платежных карт и личность преступника

§1. Детерминанты преступлений, совершаемых в кредитно-финансовой сфере

Цифровые технологии продолжают коренным образом изменять мир бизнеса, в результате чего перед компаниями не только открываются новые возможности, но и возникают новые угрозы. Поэтому совсем неудивительно, что в мире наблюдается рост киберпреступлений (например, в рейтинге за 2016 год они занимают второе место среди преступлений, с которыми чаще всего сталкиваются компании во всем мире). Киберпреступления – это не просто проблема, связанная с информационными технологиями. Сегодня информационные технологии настолько широко распространены (как внутри, так и за пределами компаний), что киберпреступления могут считаться одной из основных бизнес-проблем.

В 2016 году киберпреступники нанесли ущерб мировому бизнесу в размере 400 миллиардов долларов. По оценкам экспертов, количество киберпреступлений в России к 2018 году может вырасти примерно в четыре раза, а общие потери нашей страны от них могут превысить 2 триллиона рублей.

Эти цифры были озвучены во время панельной сессии «Киберпреступность - одна из ключевых угроз роста мировой экономики. Готова ли Россия к новым вызовам?», которая состоялась на форуме «Сочи-2016».

Только в 2016 году в мире зафиксировано 40 миллионов киберпреступников, которые совершили около 600 миллионов преступлений. Причем ни одна другая криминальная деятельность в мире не показывает таких темпов: их число ежемесячно растет на три-четыре процента.

В России сейчас бум диджитализации, как следствие - Россия находится в числе главных целей киберпреступников. Только за первое полугодие благодаря

работе центра фрод-мониторинга банка удалось предотвратить хищение у клиентов 8 миллиардов рублей.

По мнению аналитиков, количество киберпреступлений в России к 2018 году грозит вырасти в четыре раза, а общие потери могут превысить два триллиона рублей. Чтобы защититься от хакеров, в экономически развитых странах резко увеличиваются затраты на кибербезопасность. А настоящее время в России даже нет ответственности за фишинг и спам, при этом даже не выделен состав преступления "Кража с банковского счета". А максимальное наказание, которое предусмотрено действующим законодательством, не превышает семи лет лишения свободы и штраф в 500 тысяч рублей. К примеру, в США за эти правонарушения можно получить до 25 лет.

В законодательной базе должны быть предусмотрена ответственность за преступления в сфере информационных технологий, уточнены полномочия органов власти, для того чтобы каждый гражданин и представитель бизнес-сообщества понимал, куда обращаться и как наиболее эффективно добиться расследования киберпреступлений и преследования злоумышленников. Если мы не решим эти вопросы, последствия нашей цифровизации негативно скажутся на экономике России.

В настоящее время для коммерческих организаций резко возросли риски, связанные с деятельностью киберпреступников. При этом только семь процентов банков привлекли внешних аудиторов по этой проблеме. Остальные же сами оценивают безопасность своих организаций, считая ее достаточной. Но когда происходят какие-то ЧП, то выясняется, что они явно переоценивали свои возможности.

За последний год по стране совершено более пяти тысяч преступлений, связанных с хищениями средств со счетов клиентов банков. Что также наглядно говорит, о необходимости борьбы с киберпрестурностью на уровне государства.

Однако результаты опроса показывают, что в России ситуация с киберпреступлениями несколько иная. Почти четверть (23%) респондентов отметили, что за последние два года их компании пострадали от

киберпреступлений. По сравнению с предыдущим опросом за 2014 год (25%) значительных изменений не произошло.

В России за последние два года восприятие рисков киберпреступлений не изменилось у 60% респондентов. Наоборот, на глобальном уровне 53 % респондентов считают, что этот риск вырос за последние два года, тогда как в России лишь 32% респондентов ощутили его рост. Означает ли это, что российские компании менее подвержены риску киберпреступлений? Скрытый характер данной угрозы проявляется в том, что определенная часть респондентов, заявивших, что их компании не столкнулись с киберпреступлениями, на самом деле пострадали от них, даже не зная об этом. Иногда хакерам удается оставаться в сети компаний не обнаруженными в течение длительного периода времени.

Руководители компаний склонны беспокоится, что киберпреступления могут сдерживать развитие их компаний. Результаты нашего последнего опроса руководителей крупнейших компаний, работающих в России, показали, что 43 % руководителей выразили беспокойство по поводу растущей угрозы киберпрестпулений, при этом 52 % из них считают ускорение технологических изменений еще одной проблемой.

Респонденты в России отметили, что ущерб репутации и хищение персональных данных являются наиболее разрушительными последствиями киберпреступления. Далее идут утрата интеллектуальной собственности и расходы на юридическое обеспечение и принудительное исполнение. На глобальном уровне респонденты отметили сбои в работе/обслуживании, регуляторные риски и непосредственные финансовые потери.

В России 47% респондентов указали в ответах, что их компании потеряли до 1 миллиона долларов в результате киберпрестпуления, совершенного против них за последние два года. 6% респондентов указали еще более существенный убыток, который они понесли в результате киберпреступлений. Стоит отметить, что значительная доля респондентов (23%), компании которых столкнулись с киберпретспулениями, не могли оценить размер ущерба от них.

Похоже, что в случае с киберпреступлениями только в 45% организаций

есть «полностью обученные» сотрудники, готовые действовать в качестве первого эшелона реагирования, при этом сотрудники отдела ИТ-безопасности составляют подавляющее большинство (74%) из них. Корпоративные киберпрестпуления – одна из самых сложных и трудных проблем, с которой может столкнуться организация. Для принятия эффективных мер реагирования необходима совместная работа специалистов из различных функций, которые имеют соответствующие навыки, знания и опыт (например, юридического отдела, отдела кадров, отдела по работе со СМИ и связям с общественностью, отдела коммуникаций, юридического консультанта по вопросам защиты конфиденциальной информации, аудита и управления рисками, финансового отдела, службы корпоративной безопасности и др.). Определение угроз в сфере информационных технологий и их минимизация входят в круг обязанностей всех подразделений компании.

Еще одной тенденцией на рынке информационной безопасности было названо постепенное приобретение кибератаками «физического» характера. Так, уже порядка 5% информационных преступлений приводят либо к уничтожению данных, либо к урону физическим ресурсам или инфраструктуре.

Europol назвал восемь основных тенденций киберпреступлений[20]:

- Преступление-в-качестве-услуги: «подпольные цифровые услуги» подкрепляются моделью «преступление-в-качестве-услуги», которая становится все более популярной и востребованной. Она объединяет между собой специализированных поставщиков хакерских утилит и организованные преступные группировки. Террористы имеют очевидный потенциал для получения доступа к этому сектору в скором будущем.

- Программы-вымогатели: вымогательство и банковские «трояны» остаются главными угрозами среди вредоносного программного обеспечения. И эта тенденция вряд ли изменится в обозримом будущем.

[20] Паненков А.А. Система преступлений в сфере компьютерной информации, входящих в структуру террористической деятельности (кибертерроризм) как реальная угроза внешнему и внутреннему контурам национальной безопасности России // Военно-юридический журнал. № 4. – 2014. – С.87.

- Преступное использование данных: данные остаются ключевым товаром для киберпреступников. Во многих случаях они используются для получения немедленной финансовой выгоды, но все чаще применяются для реализации более сложных схем мошенничества, зашифровываются с целью получения выкупа, либо используется непосредственно для вымогательства.

- Платежное мошенничество: EMV (чип и PIN-код), гео-блокировка и другие промышленные меры безопасности продолжают помогать в эффективной борьбе с карточным мошенничеством, но, тем не менее, растет и число атак, направленных против банкоматов. Организованные преступные группы начинают компрометировать платежи, связанные с использованием бесконтактных карт (NFC).

- Он-лайн сексуальное насилие над детьми: использование платформ со сквозным шифрованием для обмена медиа файлами, а также применение анонимных платежных систем способствует эскалации он-лайн трансляции жестокого обращения с детьми.

Злоупотребление «темной стороной сети»: «темная часть всемирной интернет-паутины» продолжает содействовать преступникам, участвующим в ряде незаконных видов деятельности, таких как, обмен файлами с записью сексуального насилия над детьми. Степень, в которой экстремистские группы используют кибертехнологии для осуществления атак, в настоящее время ограничены, но предложение в «темной сети» хакерских утилит и услуг, а также незаконных товаров, может быстро изменить сложившуюся ситуацию[21].

- Социальная инженерия: правоохранительными органами был зарегистрирован рост числа фишинг-атак, направленных на цели, имеющие высокую значимость. Главной угрозой стали атаки против генеральных директоров предприятий и организаций.

Виртуальные валюты: Bitcoin остается той валютой, которую мошенники

[21] Паненков А.А. Система преступлений в сфере компьютерной информации, входящих в структуру террористической деятельности (кибертерроризм) как реальная угроза внешнему и внутреннему контурам национальной безопасности России // Военно-юридический журнал. № 4. – 2014. – С.87.

предпочитают для оплаты за приобретение незаконных товаров и услуг в «темной сети. Bitcoin также стал стандартным платежным решением притребовании выкупа и других форм вымогательства.

- По-прежнему наблюдается рост объема, масштаба и стоимости киберпреступлений. За последнее время эти показатели достигли небывалого уровня. Некоторые государства, входящие в ЕС, говорят о том, что случаи преступлений в сфере кибербезопасности, возможно, уже превосходят численность традиционных преступлений.

Рост численности мошенников совместно с увеличением количества возможностей для участия в высокодоходной незаконной деятельности частично подпитывает подобную тенденцию, равно как и появление новых инструментов для совершения киберпреступлений в таких сферах, как мобильное вредоносное ПО и мошенничество, направленное против банкоматов. Тем не менее, главная часть проблемы состоит в недостаточном соблюдении стандартов цифровой безопасности юридическими и физическими лицами.

Значительная часть киберпреступной деятельности по-прежнему использует относительно старые технологии, обеспечение безопасности для которых доступны, но не пользуется широким распространением.

22 сентября 2016 года Check Point Software Technologies Ltd. опубликовала результаты исследования, в котором отметила 9-кратный рост неизвестных зловредов, атакующих системы предприятий и сделала вывод о необходимости внедрения в компаниях лучшей в своем классе защитной архитектуры[22].

Эксперты компании провели анализ сведений, полученных от 31 тыс. шлюзов безопасности Check Point по всему миру, и описали - какие известные и неизвестные виды вредоносного ПО и атак воздействуют на ИТ-системы компаний, каковы последствия интеграции мобильных устройств в ИТ-инфраструктуры предприятий. Также дана оценка потерь компаний от взломов и расходы на устранение их последствий.

---

[22] Электронный ресурс. Режим доступа: http://safe.cnews.ru/news/top/fsb_budet_rukovodit_bezopasnostyu_v_runete

Таким образом, можно заключить, что в настоящее время для коммерческих организаций резко возросли риски, связанные с деятельностью киберпреступников.

В законодательной базе должны быть предусмотрена ответственность за преступления в сфере информационных технологий, уточнены полномочия органов власти, для того чтобы каждый гражданин и представитель бизнес-сообщества понимал, куда обращаться и как наиболее эффективно добиться расследования киберпреступлений и преследования злоумышленников.

§2. Характеристика личности преступника

Типология преступлений основывается на том, что к вопросу классификации преступлений в основном подходят с двух позиций. В первом случае при выделении категории преступлений преступность рассматривается в качестве статистической совокупности преступлений, и для выделения какой-либо группы достаточно выделить одно-два основания, как, например, в случае выделения «преступности несовершеннолетних», «корыстной преступности», «насильственной преступности». Другая позиция сформирована на том основании, что преступность рассматривается как сложное социальное явление в различных сферах общественной жизни (вся совокупность преступлений в сфере экономики, частично включающая в себя все предыдущие виды).

Очевидно, что для создания стройной классификационной модели преступности в сфере банковских преступлений могут использоваться далеко не все из традиционных криминологических оснований. Так, в частности, не может быть использован критерий вины, подразделяющий преступность на умышленную и неосторожную.

Совершение преступлений в сфере банковских преступлений возможно только с прямым умыслом. В силу трансграничности «Всемирной паутины» не

имеет значения и такой критерий, как типы поселений. Одним из самых общих критериев дифференциации преступлений в сфере высоких технологий в глобальной сети Интернет является «техногенно-исторический». Поскольку преступность обладает исторически изменчивым и преходящим характером то существуют:

a) «традиционные компьютеро-независимые» формы преступлений, использующие возможности Интернет для реализации преступного умысла в целях обогащения. Характерной чертой таких видов преступной активности является то обстоятельство, что они не являются «компьютерозависимыми», т.е. изначально совершались в реальном пространстве и только в процессе развития информационных отношений были перенесены в «виртуальную реальность». Примеров подобной трансформации преступной деятельности много: например, изготовление поддельных документов, бланков, марок акцизного сбора, специальных марок или знаков соответствия, поддельных денег или ценных бумаг, сначала с помощью простого перерисовывания, несколько позднее с помощью изготовления клише, еще позднее с помощью копировального оборудования, и в последнее время при помощи компьютера и распечатывания на принтере. Поэтому даже весьма радикальные методы, такие как прекращение функционирования Интернет или даже отказ человечества от компьютерной техники, не способен полностью искоренить преступность;

b) «нетрадиционные компьютерозависимые» формы, зачастую использующие коммуникационные возможности Интернет, являются «компьютерозависимыми» поскольку само преступление (хищение) не мыслимо без модификации, копирования компьютерной информации. «Компьютерозависимое» преступление в сфере высоких технологий является следствием несовершенства информационной безопасности.

В периодической печати и на страницах интернет-изданий регулярно появляется информация о совершенных злоумышленниками конкретных преступлениях в кредитно-финансовой сфере, в том числе связанных с банкоматами и банковскими картами.

Приведем несколько примеров. Так, 05.03.2013 года в Санкт-Петербурге задержаны двое "умельцев", которые пытались украсть из банкомата более 2,5 миллиона рублей. По сообщению пресс-службы ГУ МВД по Санкт-Петербургу и Ленинградской области, злоумышленников поймали в дополнительном офисе одного из городских банков, расположенном на проспекте Славы, дом 4. Денежные средства в сумме 2 миллиона 600 тысяч рублей они пытались похитить с помощью специального оборудования – скимингового устройства.

Обоим задержанным по 28 лет, и регистрации в Санкт-Петербурге мужчины не имели. Возбуждено уголовное дело по статье 30, часть 3, и статье 183, часть 3 УК РФ (незаконные получение и разглашение сведений, составляющих коммерческую и налоговую тайну)[23].

В одном из магазинов Иркутска 09 июля 2013 года с поличным задержали молодого человека, который с помощью написанной им самим программы сумел перепрограммировать банкомат и похитить 75 тысяч рублей. На злоумышленника обратили внимание охранники магазина: тот подозрительно долго не отходит от терминала. Как позже выяснилось, хакер до задержания все же успел взломать системное обеспечение банкомата и перевести солидную сумму на подставные счета. В ГУ МВД по Иркутской области полагают, что план хищения был тщательно продуман и что действовал молодой человек не в одиночку.

Личности сообщников сейчас устанавливаются. Самому хакеру 19 лет, он студент факультета информационных систем и технологий управления Читинского госуниверситета. Весной прошлого года парень занял второе место на всероссийской олимпиаде по информатике. В Иркутск он приехал к другу, погостить[24]. В Новосибирске 06 августа 2013 года злоумышленник похитил два миллиона рублей из банкомата. Как сообщили в пресс-службе ГУ МВД по Новосибирской области, в 3 часа 45 минут в дежурную часть поступило сообщение о взрыве в помещении филиала банка, расположенного по проспекту

---

[23] В Петербурге задержали хакеров // Российская газета [электронный ресурс]. Режим доступа: http://www.rg.ru/2013/03/05/reg-szfo/bankomat-anons.html (17.01.2017).

[24] В Иркутске задержали программиста-олимпиадника // Рос. газ. [электронный ресурс]. Режим доступа: http://www.rg.ru/2013/07/09/reg-sibfo/haker-anons.html (17.01.2017).

Карла Маркса. На место происшествия прибыла следственнооперативная группа. Было установлено, что злоумышленник организовал взрыв корпуса одного из устройств, после чего похитил из банкомата два миллиона рублей[25].

УМВД по городу Владимиру 18 октября 2013 года возбудило уголовное дело по части 4 статьи 158 УК РФ по факту хищения двух банкоматов из здания развлекательного комплекса "Руськино". Как рассказали "РГ" в УМВД по Владимирской области, около 5 часов утра злоумышленники, воспользовавшись отсутствием охранников, отжали пластиковые входные двери и быстро вынесли два из пяти банкоматов. Характерно, что воры действовали избирательно: они захватили именно те устройства, которые не были оснащены GPS-маячками и принадлежали различным банкам. В сейфе одного из них было два миллиона 82 тысячи рублей; сколько денег хранилось в другом банкомате, остается коммерческой тайной. В похищении участвовало сразу шесть человек. Несмотря на то, что их действия зафиксировали камеры слежения, поймать злоумышленников по горячим следам не удалось[26].

Приведенные примеры хищения денежных средств из банкоматов, с одной стороны, свидетельствуют о широкой географии этих преступлений в нашей стране. Если же принять во внимание обстоятельство, что не все подобные случаи становятся достоянием средств массовой информации, то можно говорить о массовости такого рода преступлений в современной банковской практике.

В совершение преступлений с банковскими пластиковыми картами вовлекаются сотрудники банков и процессинговых компаний, а также работники обслуживающих сервисных точек, что является серьезным фактором, «т.к. именно эта категория работников наиболее полно осведомлена о механизме функционирования платежной системы, возможностью доступа к данным об эмитированных картах и их владельцах, а иногда и PIN-кодах, а также

---

[25] В Новосибирске неизвестный украл два миллиона, взо- рвав банкомат // Рос. газ. [электронный ресурс]. Режим до- ступа: http://www.rg.ru/2013/08/06/reg-sibfo/bankomatanons.html (17.01.2017).

[26] Во Владимире возбуждено дело по хищению банкома- тов // Рос. газ. [электронный ресурс]. Режим доступа: http://www.rg.ru/2013/10/18/reg-cfo/bankomat-anons.html (17.01.2017).

возможностью осуществлять преступную деятельность, исполняя свои служебные обязанности». Рассматривая криминалистическое значение информации о личности преступника при расследовании хищений, совершенных с использованием кредитных и расчетных карт, следователю необходимо акцентировать внимание на значимости сведений о характерных свойствах личности субъекта преступления для эффективного выбора дальнейших тактических приемов и выдвижения следственных версий

Распределение лиц по полу имеет определенные особенности:

– грабежи и разбои на открытой местности совершаются лицами мужского пола, которые применяют насилие для завладения картой и получения PIN-кода к ней от потерпевших;

– значительное число мошенничества совершается лицами мужского пола, обладающими определенными знаниями и умениями в области изготовления поддельных карт;

– доля лиц женского пола заметно выше в категории мошенников и расхитителей, которые являются банковскими работниками 65,4 %;

– лица, обладающие обывательскими знаниями в области использования банковских карт, совершают в основном кражи 55,06 %;

– основная масса правонарушителей имеет средне-специальное образование 50,47 %, неполное среднее образование имеют 4, 4 %, среднее – 34, %, студенты 6, 3 %, высшее 6,13 %

Таким образом, при совершении преступлений с использованием кредитных и расчетных карт способ совершения позволяет существенно охарактеризовать отдельные личностные данные преступника. Так, хищения путем мошенничества совершают так называемые профессиональные «компьютерные» преступники с выраженными корыстными целями, в качестве соучастников или непосредственно исполнителей выступают сотрудники эмитента, мерчанта, эквайера, т е лица, также имеющие определенную профессиональную подготовку и имеющие доступ к оформлению расчетных операций с использованием

платежно-расчетных карт. Сотрудники банков, совершающие хищения с использованием кредитных и расчетных карт, имеют доступ к персональным данным лица, обращавшегося в банк по какому-либо вопросу. И, напротив, при совершении тайного хищения денежных средств с использованием кредитных и расчетных карт, например, при хищении карты и PIN-кода преступник может не обладать никакими специальными знаниями, кроме как умением пользоваться банкоматом[27].

Лица, которые занимаются мошенничеством с использованием платежных карт, достаточно четко отличаются от других преступников, так как им не свойственны такие черты характера, как импульсивность и агрессивность, как правило, они характеризуются стремлением к повышению социального статуса. Они имеют широкий кругозор, высокий интеллектуальный уровень, хорошую ориентацию в экономических и юридических вопросах.

Анализ изучения уголовных дел показывает, что в основном это мужчины. Среди лиц, совершивших преступление данной категории, ½ часть - это люди в возрасте от 16 до 35 лет, ¼ часть составляют лица в возрасте от 35 лет до 50, и всего лишь 1/8 часть – это возраст от 50 до 70 лет. Всего 10% составляют лица, имеющие высшее образование, остальная часть, т.е. 90% имеют среднее или средне специальное образование.

Большинство из них – 90% нигде не работает. Следовательно, можно сделать вывод, что все они занимаются преступной деятельностью данного направления в качестве промысла.

[27] Завидов, Б. Д., Ибрагимова, З. А. Мошенничество в сфере высоких технологий.//Современное право. - 2011. № 4. С. 41.

Глава 3. Меры предупреждения мошеннических действий с использованием платежных карт

§1. Зарубежный опыт предупреждения мошеннических действий с использованием платежных карт

Все большую популярность набирает трансграничная преступность[28], которую уже включили в список глобальных проблем человечества. В настоящее время на разработку мер борьбы с международными преступниками выделяется огромное количество сил и времени, необходим обмен опытом между странами в условиях совместной деятельности по укреплению экономической безопасности.

В мире базовые научные постулаты об экономической безопасности, точнее о безопасности бизнеса, были заложены французом М. Патэном в работе "Общая часть уголовного права и уголовное законодательство в сфере бизнеса" (1861 г.)[29].

На сегодняшний день очевидно, что экономическая безопасность Российской Федерации находится под угрозой, преступники обнаруживают все новые сферы деятельности, методы и способы реализации задуманного. В постсоветский период власти начали активно заниматься обеспечением экономической безопасности. Однако, как показывает статистика, число экономических преступлений в России еще достаточно высоко, что, конечно же, влияет на экономическую безопасность нашей страны и национальную безопасность в целом во всем мире.

Обратимся к опыту Соединенных Штатов Америки в борьбе с экономической преступностью. Соединенные Штаты являются одной из наиболее активно развивающихся стран, где основы предпринимательства начали зарождаться несколько раньше, нежели в остальных странах мира, как и понятия

---

[28] Трунцевский Ю.В. Понятие транснационального преступления // Международное уголовное право. 2014. N 3. С. 9 - 12.

[29] Лепешкина М.Н. Эволюция понятия "экономическая безопасность" в США, Западной Европе и России // Экономическая наука и практика: Материалы межд. науч. конф. (г. Чита, февраль 2012 г.). Чита: Молодой ученый, 2012. С. 7 - 9.

частной собственности и банковской деятельности. Именно в этих сферах происходит сейчас наибольшее количество преступлений, опыт борьбы с которыми может быть полезен и для России[30].

Преобладающими в Соединенных Штатах Америки являются экономические преступления[31], совершенные людьми, в чьих руках находится власть: топ-менеджеры, руководство компаний и чиновники. Одним из проявлений таких видов преступлений стало фиктивное банкротство. В настоящее время в российской судебной практике нет различия между фиктивным и преднамеренным банкротством[32]. Данные преступления регламентируются статьями 196 и 197 УК РФ. Однако фиктивное банкротство являет собой некое отличие от преднамеренного и представляет большую угрозу. В США, как и в России, банкротом становится должник, который по решению суда (по собственному заявлению или по заявлению кредиторов) неспособен погасить всю кредиторскую задолженность. По итогам рассмотрения дела чаще всего вводится конкурсное производство, в процессе которого распродаются все активы должника, а сумма, вырученная от продаж, распределяется между кредиторами, заявленными в реестре, согласно очереди и доле вложений. Впрочем, все чаще встречаются так называемые "фиктивные банкроты", которые укрывают свое имущество в целях недопущения конфискации. Основной чертой именно фиктивности являются "фабрики ходатайств"[33], что подразумевает под собой всевозможные схемы, с помощью которых утверждается, что арендатору была оказана материальная помощь, связанная с удержанием от выселения. Процесс запускается через заявление о превышении срока задолженности арендатора в местных СМИ. Но на самом деле это заявление является первым шагом

[30] Карпович О.Г., Трунцевский Ю.В. Серьезные экономические преступления XXI века: опыт противодействия им в Великобритании, России и США: Монография. М.: ЮНИТИ ДАНА; Закон и право, 2013.
[31] Трунцевский Ю.В., Саркисян К.А., Янюк Д.А. Мошенничество в медицинской системе США: организационно-правовые аспекты противодействия // Медицинское право. 2014. N 2. С. 19 - 24.
[32] Лунев В.В. О криминализации экономических преступлений предпринимателей // Дальневосточный федеральный университет. URL: http://www.crime.vl.ru/index.php?p=3866&more=1&c=1&tb=1&pb=1.
[33] УЭБ и ПК МВД РФ. URL: https://23.mvd.ru/gumvd/units/item/302772.

процедуры банкротства против арендатора. После этого все проведенные платежи становятся безосновательными, и арендодатель незаконно получает деньги. Такие дела могут тянуться несколько месяцев, а, в то время как для арендатора создается иллюзия, что он получает необходимую ему помощь от собственника, последний посредством службы оповещения просто уничтожает его сбережения, сводя на нет кредитоспособность арендатора, и откладывает его неизбежное выселение на неопределенный срок. После выселения площади остаются свободными, и схема повторяется снова и снова.

Все дела, связанные с признанием банкротства, в том числе и фиктивного, ведутся исключительно на федеральном уровне. Во-вторых, конкурсное производство осуществляется под надзором так называемого опекуна, который является незаинтересованным лицом. Он проводит необходимые процессы, сделки, контролирует наличие активов и препятствует их выводу. При этом в обязательном порядке он обязан уведомлять о своих действиях ФБР. В-третьих, в США не требуется, чтобы ущерб был причинен в крупном размере, достаточно того, чтобы был зафиксирован ущерб, а размер его учитывается только при вынесении приговора. Если потери небольшого характера, то будет вменен лишь штраф. (К тому же необходимо пересмотреть уголовную ответственность лиц, которые мешают деятельности арбитражного управляющего или вступают с ним в сговор.)

Одним из ярких примеров фиктивного банкротства стало заявление американского филиала компании British Petroleum (далее по тексту - BP) о прекращении их деятельности в связи с неплатежеспособностью. В ходе дела стало известно, что некоторые бухгалтеры и управляющие занимались подделкой бухгалтерской отчетности, завышением цены на пропан, а также пытались вывести средства, которые полагались на предупреждение экологических происшествий. Результатом преступной деятельности стали взрыв в Техасе в 2005 году (погибло 15 человек) и утечка сырой нефти из нефтепровода на Аляске в

2006 году[34].

Второй по значимости проблемой в Америке являются преступления в хедж-фондах. Почему это происходит? Менеджеры хедж-фондов ведут торговлю без всевозможных посредников (дилеров, брокеров), которые могли бы контролировать процесс. Это создает возможность для сговора. Во-вторых, за вложения в такие фонды несет ответственность исключительно инвестор. И в-третьих, можно сказать, отсутствие аудиторских проверок. Нельзя забывать и об отсутствии централизации управления в данных фондах. Торги ведутся исключительно через собственные счета, поэтому существует возможность предоставления фальшивой информации. Существует огромное количество таких примеров. Наиболее новым и показательным является дело главы крупнейшего в США хедж-фонда SAC Capital Advisors Стивена Коэна, который в 2013 году обвинялся в махинациях с ценными бумагами на 275 млн. долларов. По итогам суда Стивен Коэн отстранен от деятельности компании, лишен лицензии и обязан выплатить все долги. Также предъявлено новое обвинение сотруднику данного фонда в торговле инсайдерской информацией.

Нельзя не вспомнить о таком экономическом преступлении, как использование инсайдерской или конфиденциальной информации в пользу чьих-либо интересов. Начнем с того, какая именно информация является инсайдерской. Основными признаками принадлежности являются значимость и существенность при заключении сделок и недоступность для широкого круга инвесторов.

Существенность информация приобретает в том случае, если она обладает способностью изменить цену акции[35].

Самым распространенным случаем среди таких действий является асимметрия сделок. Это нарушение закона подразумевает под собой ситуацию сделки, в которой владение информацией разных сторон не равноценно. И в случае доступа к информации той стороны, которая ей не владеет, сделка становится невозможной по причине невыгодности. Асимметрия информации

[34] Федеральное бюро расследований. URL: www.fbi.gov.
[35] Комиссия по ценным бумагам и биржам. URL: www.sec.gov

очень ярко проявляется в такой теоретической модели рынка, как "рынок лимонов". На рынке подержанных машин возможности покупателя ограничены той информацией, которую ему выдает продавец, со своей стороны заинтересованный в немедленной покупке. Существует рынок подержанных автомобилей хорошего качества, чаще всего средняя цена на которые варьируется от 3500 до 4000 долларов, но на тот же рынок стремятся попасть и недобросовестные продавцы, которые стараются пустить в оборот так называемые "лимоны" - машины с дефектами по цене от 2000 до 2500 долларов. Но среднерыночная цена устанавливается (с учетом равного количества "лимонов" и качественных авто) в размере 3250 долларов, таким образом, добросовестные продавцы рано или поздно будут вытеснены с рынка, а "лимоны" будут продаваться по завышенной цен[36].

Лицо, распространившее инсайдерскую информацию, в США подвергается наказанию при наличии некоторых условий:

- совершении сделки с использованием данной информации;

- доказанности материальной заинтересованности лица, передавшего информацию.

При доказанности совершения преступления лицу, совершившему его, будет вменен штраф, размер которого ограничен трехмерной выручкой от сделки (иначе может определяться как убыток, которого удалось избежать). Срок исковой давности для данного преступления - 5 лет с момента совершения незаконной сделки[37].

Из приведенных выше примеров очевидно, что экономическая преступность может проявлять себя во всевозможных формах, начиная от самого обычного воровства "синих воротничков" и заканчивая искусственным укрыванием активов и махинациями с ценными бумагами на государственном уровне. Обмен опытом между разными странами может упростить процесс изучения новых видов

---

[36] Акерлоф Дж. Рынок "лимонов": неопределенность качества и рыночный механизм // THESIS. 1994. Вып. 6. С. 91 - 104.

[37] Ширинян И.Г. Мировой опыт использования инсайдерской информации на рынке // Рынок ценных бумаг. 2014. N 10.

преступлений и решить вопрос с международным розыском и созданием общей базы компаний, которые однажды уже попадали под подозрение. Российская организованная преступность уверенно вышла на мировую арену и закрепила позиции наравне с лидерами. Ясно, что с развитием бизнеса и экономики будут совершенствоваться методы и появляться новые ухищрения, поэтому именно международное сотрудничество сможет предотвратить или хотя бы уменьшить ущерб от деятельности организованных преступных сообществ. На сегодняшний день все большее распространение получает трансграничная преступность (контрабанда, незаконное хранение оружия, распространение наркотиков, финансовые махинации, рэкет и шантаж), затрагивающая приграничные интересы всех стран мира и вследствие этого попавшая в список глобальных проблем человечества. Аналогичным образом это может стать стимулом для объединения усилий и обмена опытом.

В начале 2017 года США прошла операция против преступной группы, совершившей крупнейшее в истории страны мошенничество с кредитными картами. Преступникам удалось потратить примерно 13 миллионов долларов. Штаб-квартира группировки находилась в Нью-Йорке, а их сообщники действовали по всему миру - от Ливии до России.

Обвинения в краже личных данных, подделке документов, ограблении и других преступлениях предъявлены 111 подозреваемым. В прессе со ссылкой на заявление полиции сообщалось, что 86 человек уже взяты под стражу, остальных 25 пока не нашли. Сам глава нью-йоркской полиции Раймонд Келли (Raymond Kelly) на пресс-конференции называл другие цифры: арестовали 75 человек, 15 уже находятся под стражей по подозрению в других преступлениях, 21 человек еще не задержан. Четверо, предположительно, сбежали в Россию (в обвинительном заключении упоминаются три русских имени - Ирина Первухина, Светлана Туракаева и Алексей Колтыга). Видеозапись пресс-конференции публикует The New York Post. Расследование продолжалось два года.

В этом деле удивляет масштаб происходившего. Личные данные с кредитных карт тысяч жертв, как установила полиция, снимали официанты и

другие работники сферы услуг в США - там действовали пять групп (некоторые данные о кредитках находили и в интернете). Неизвестные сообщники в России, Ливии, Ливане и Китае делали чистые кредитки, на которые потом в США и наносилась украденная информация. Иногда для убедительности подделывали и водительские права, чтобы информация на них совпадала с данными, указанными на картах.

На снятые с чужих кредиток деньги покупалась преимущественно продукция компании Apple, которая потом продавалась за границу (сбыть продукты этой компании было несложно). Подозреваемые жили в пятизвездочных отелях, ездили на Lamborghini, покупали ювелирные украшения.

Не брезговали и обычными преступлениями. Так, по версии обвинения, пятеро подозреваемых украли груз стоимостью 95 тысяч долларов из аэропорта имени Кеннеди, семеро - компьютерное оборудование на 850 тысяч долларов из здания корпорации Citigroup, планировалось и традиционное ограбление банка. Впрочем, с кражей из аэропорта вышла осечка. Как пишет The Wall Street Journal, преступники узнали, что рейсом Lufthansa прибудет партия компьютеров Apple стоимостью миллион долларов. Когда злоумышленников остановила полиция, выяснилось, что они украли не тот груз. Вместо дорогих компьютеров у них оказались рабочие инструменты.

Группировка была интернациональной. Ее боссами, по версии полиции, были Имран Хан (Imran Khan), Али Хвейсс (Ali Khweiss), Энтони Мартин (Anthony Martin), Санжай Деусорран (Sanjay Deowsarran, известный также как Роки Деусорран), а также Амар Сингх (Amar Singh).

Всего в ходе обысков полиция конфисковала продукцию Apple стоимостью в десятки тысяч долларов, украденное компьютерное оборудование, 650 тысяч долларов наличными, оружие и целый грузовик с электроникой, дорогими часами и обувью, оборудованием для кражи личных данных и другими вещами.

"Схемы и воображение этих воров потрясают", - заявил Келли, слова которого приводит Reuters. Келли особенно отметил технологические знания, которыми обладали преступники. Полиции тоже пришлось постараться.

Обвинение основано на записях телефонных разговоров подозреваемых - детективы потратили много времени, переводя их с русского, китайского, арабского, бенгальского, фарси и испанского. Помогло полиции то, что подозреваемые рассказывали о своей красивой жизни в Twitter'e и Facebook'e. Мать одного из подозреваемых обвиняется в том, что залогинилась на его страничке в Facebook'e, чтобы создать сыну алиби.

По словам прокурора нью-йоркского округа Квинс (там базировалась группировка) Ричарда Брауна, мошенничество с кредитными картами и кража личных данных с целью мошенничества входят в число тех видов преступлений, количество которых в США растет быстрее всего. То, что сообщники преступников, предположительно, находятся в России, давно не удивляет. В марте 2010 года сообщалось о том, что мошенники из Мичигана закупали в РФ номера кредиток. А в ноябре 2009 года в США была разоблачена эстонско-российская группировка, которую обвинили в краже более девяти миллионов долларов с помощью поддельных банковских карточек.

В конце мая 2013 г. прокуратура Нью-Йорка объявила о приостановке деятельности платежной системы Liberty Reserve . Основанная в 2006 г. в Коста-Рике платежная система Liberty Reserve через собственную виртуальную валюту позволяла пользователям анонимно переводить денежные средства в любую точку мира за небольшую комиссию. Через систему прошло 55 млн платежей на сумму $6 млрд.

У Liberty Reserve был почти 1 млн клиентов из разных стран мира. По данным прокуроров, преступные группировки, пользовавшиеся услугами Liberty Reserve, базировались во Вьетнаме, Нигерии, Гонконге, Китае и США. Компания была «любимым банком преступного мира», говорится в обвинительном документе. Мошенников прежде всего привлекала анонимность. Для успешной регистрации, а затем проведения денежных операций было достаточно указать адрес электронной почты. Например, один из секретных агентов (как отметил прокурор Южного округа Нью-Йорка Прит Бхарара) зарегистрировался в Liberty Reserve под именем Джо Фальшивый (Joe Bogus) и дал столь же «красноречивое»

имя своему счету «украсть все» (to steal everything), а свой адрес указал следующим образом: «123, Поддельная Главная Улица» в «Полностью Выдуманном Городе, США» — и его зарегистрировали .

Американские правоохранительные органы назвали Liberty Reserve «крупнейшим в истории отмыванием преступных денег посредством Интернета».

Известная российская компания Group-IB провела свое расследование деятельности Liberty Reserve . Так, по информации сотрудников компании Group-IB клиент мог сохранить инкогнито, даже перечисляя деньги из респектабельной системы вроде WebMoney, которая проверяет своих пользователей. Клиент также мог без проблем купить легально оформленный в таких системах кошелек (так называемый аттестат). В аттестате могли быть данные из украденных документов, но необязательно, так как существуют сервисы по продаже паспортных данных, которые честно куплены у владельцев документов. Людей, добровольно предоставляющих свои данные, называют «дропами» или «мулами» (их данные обычно используются для проведения сделок, приема товаров или банковских переводов, обналички и т. п.). У «дроповодов» можно было купить и электронный кошелек, привязанный к реальному банковскому счету с пластиковой картой, и с купленного счета осуществлять безналичные банковские проводки в ту же Liberty Reserve.

Liberty Reserve принимала площадки, которые ни один банк или процессинг не подключит: финансовые пирамиды, HYIP-фонды , продавцов ложных антивирусов и вредоносных кодов, распространителей мошеннических SMS-подписок, магазины краденых кредиток, сканов паспортов и т. п.

Американские власти утверждают, что целевой аудиторией Liberty Reserve были главным образом наркоторговцы, нелегальные порнографы, кардеры, хакеры, создатели финансовых пирамид, замаскированных под инвестфонды, и их клиенты, а также террористы.

Напомним, что ранее аналогичный случай произошел с платежной системой компании E-gold. В отличие от современных электронных платежных систем E-gold была построена не на денежных единицах, привязанных к доллару или

другой валюте. Вместо этого пользователям предлагалось покупать золото или другие драгоценные металлы (серебро, платину и палладий), находящиеся на хранении у компании E-gold Ltd. На пике существования система проводила транзакции на $2 млрд в год .

Деятельность E-gold привлекала внимание американских властей в 2005 г., в 2007-м владельцам сервиса были предъявлены обвинения в обслуживании создателей мошеннических инвестиционных проектов и других преступных групп.

Так, в частности, компании E-gold и ее руководителям были предъявлены следующие нарушения:

— статья 18 Свода законов США, раздел 1956 (Преступный сговор с целью отмывания денег);

— статья 18 Свода законов США, раздел 371 (Преступный сговор);

— статья 18 Свода законов США, раздел 1960 (Незаконные операции по переводу денежных средств);

— статья 26-1002 Свода законов округа Колумбия (Нелицензионная деятельность по осуществлению денежных переводов);

— статья 18 Свода законов США, раздел 2 (Пособничество, подстрекательство и соучастие в преступлении);

— статья 18 Свода законов США, раздел 982 (a) (1) (Конфискация в уголовном порядке) .

Спустя год генеральный директор компании Дуглас Л. Джексон признался в совершении финансовых операций без лицензии и отмывании денег. Приговор был вынесен в 2008 г. Дуглас Л. Джексон мог получить тюремный срок до 20 лет и штраф $500 000 только за участие в операциях по отмыванию, а также пять лет тюрьмы и штраф $25 000 за работу без лицензии. Однако ему присудили всего три года условного срока (включая шесть месяцев домашнего ареста), 300 часов общественных работ и штраф $200.

Многие эксперты в области применения систем электронных денег сходятся во мнении, что при рассмотрении специфики функционирования подобных

систем с точки зрения противодействия отмыванию денег необходимо помнить, что деятельность по противодействию легализации доходов, полученных преступным путем, и финансированию терроризма является, скорее, вспомогательной. Необходимость в ней возникает не из-за «врожденных» рисков, характерных для финансовых потоков, а из-за совершения преступлений, из которых извлекается прибыль. Эта прибыль может быть направлена в том числе на террористические цели.

В условиях, когда в обороте присутствуют наличные, являющиеся абсолютно анонимными, тотальный контроль не может являться самоцелью. Подразделения финансовых разведок государств понимают это, а потому акцент делают скорее на анализе транзакций, нежели на сборе максимального объема данных о субъектах. Системы электронных денег, в свою очередь, обладают возможностями по выявлению подозрительных транзакций, а также, при необходимости, фиксированию достаточной для проведения оперативно-розыскных мероприятий информации.

Отметим еще одну особенность сегодняшнего времени — значительное ослабление режима сохранения банковской тайны в рамках решения задач по противодействию отмыванию денег, финансированию терроризма и финансированию распространения оружия массового уничтожения. Согласиться с таким подходом пришлось многим странам, включая Швейцарию, где традиционно действовал порядок максимального сохранения конфиденциальных сведений, составляющих банковскую тайну. Законодательство Швейцарии не содержит определения банковской тайны и перечня информации, подлежащей охране банком. Банковская тайна охватывается статьей 13 Конституции Швейцарии, защищающей право всех лиц на уважение тайны частной и семейной жизни. Эта категория включает в себя и охрану тайны источников доходов и происхождения активов, за исключением случаев, которым предшествовало совершение преступления .

В банковской и судебной практике банковская тайна понимается как профессиональная обязанность банкира поддерживать строжайший режим

конфиденциальности в отношении любой информации о личных и финансовых обстоятельствах клиента и некоторых третьих лиц, если она была получена в ходе осуществления им профессиональной деятельности. В статье 47 Закона Швейцарии от 8 ноября 1934 г. «О банках и сберегательных кассах» (с изменениями) для лица, раскрывшего банковскую тайну, доверенную ему или полученную им как чиновником, работником, поверенным, арбитражным управляющим, должностным лицом банка, представителем Комитета по банкам, работником аудиторской компании или лица, пытающегося вовлечь третьих лиц в нарушение банковской тайны, предусмотрена уголовная ответственность в виде лишения свободы на срок до шести месяцев или штрафа на сумму не более 50 000 швейцарских франков. Носителям банковской тайны запрещается даже раскрывать информацию о том, что они обладают банковской тайной. Закон также устанавливает обязанность хранить банковскую тайну даже после прекращения трудового или иного договора, при этом срок действия такой обязанности не устанавливается, из чего можно сделать вывод о ее действии в течение всей жизни ее носителя .

На федеральном уровне в Швейцарии действует Закон от 10 декабря 1997 г. «О борьбе с отмыванием денег и финансированием терроризма в финансовом секторе» (далее — Закон о борьбе с отмыванием денег), который в 2009 г. был приведен в соответствии с Рекомендациями ФАТФ. Учитывая Рекомендацию № 4 (банковская тайна не должна влиять на применение Рекомендаций ФАТФ), Рекомендацию № 13 (обязанность банка сообщать уполномоченному органу о совершении соответствующих правонарушений), Рекомендацию № 36 (взаимная правовая помощь, не зависящая от ограничений, связанных с банковской тайной) федеральный закон налагает на финансового посредника ряд обязанностей. Так, в частности, он должен незамедлительно направить уведомление в уполномоченный орган , если знает или имеет разумные основания полагать, что финансовая операция связана с совершением преступлений, предусмотренных статьями 260ter и 305bis Уголовного кодекса Швейцарии . Также в случае, если активы получены в результате совершения фелонии , находятся в распоряжении

организованной преступной группировки или используются для финансирования терроризма (статья 260 quinquies Уголовного кодекса Швейцарии).

В соответствии со статьей 10 Закона о борьбе с отмыванием денег финансовый посредник обязан заморозить активы на счетах клиента, если они связаны с подозрительной деятельностью. При этом снять ограничение финансовый посредник имеет право только после получения на то прямой санкции соответствующих органов следствия, но не позднее чем через пять рабочих дней.

В течение времени, когда счета клиента заблокированы в соответствии со статьей 10 Закона о борьбе с отмыванием денег финансовый посредник не имеет права сообщать ему или третьим лицам о направлении отчета в уполномоченный орган. Этим же законом снимается ответственность с финансового посредника в связи с нарушением договорных обязательств или режима тайны в деловых отношениях и коммерческой тайны при направлении им уведомления в уполномоченный орган.

После скандала со швейцарским банком USB (банк заплатил штраф € 780 млн и выдал информацию о 300 гражданах США, скрывавших свои доходы для целей неуплаты налогов на родине, Службе внутренних доходов США) Швейцария взяла курс на имплементацию статьи 26 Модельной конвенции ОЭСР о налогообложении дохода и капитала . 13 марта 2009 г. Федеральный совет заявил, что эта норма будет воспринята Швейцарией и станет основанием представления информации при условии подачи конкретного и обоснованного заявления. Однако существует точка зрения, что Швейцария всегда умела грамотно защищать свои интересы и балансировать между требованиями, в частности, банкиров и зарубежных политиков, поэтому процесс пересмотра двухсторонних договоров об избежании двойного налогообложения может затянуться. Хотя соответствующие поправки уже были внесены 24 сентября 2011 г. в двусторонний договор между Швейцарией и Россией, а также еще ранее с Германией и Великобританией .

Характерно, что глобальный тренд в мировой политике по борьбе с

банковской тайной, по всей видимости, отразился и на рассматриваемой статье Конвенции. Так, в пункте 3 статьи 26 Конвенции устанавливается перечень охраняемых национальным законодательством сведений, не подлежащих раскрытию в соответствии с Конвенцией. К ним относятся: торговая, предпринимательская, производственная, коммерческая или профессиональная тайны или ноу-хау, раскрытие информации даже ограничено при нарушении в таком случае публичного порядка, но банковская тайна в этом списке не упомянута. При этом сами разработчики Конвенции утверждают, что исходили из того, что никакой режим конфиденциальности информации, в том числе банковская тайна, не может быть основанием для непредставления информации «ответ на запрос».

Стоит также отметить, что иностранные налоговые органы имеют право запрашивать соответствующую информацию у банков, последние не вправе раскрывать национальным налоговым органам Швейцарии информацию о финансовом состоянии, коммерческой деятельности своего клиента, полученную в ходе проверки его кредитоспособности.

В заключение приведем некоторые выводы:

- активное внедрение различных систем расчетов с использованием электронных платежей сопровождается появлением новых источников рисков, связанных с недостаточным уровнем обеспечения информационной безопасности на всех участках информационного контура, который формируется в процессе выполнения расчетов между участниками сделки;

- в условиях глобального характера рисков использования электронных платежей необходимо учитывать, что существующая правоприменительная практика не всегда может эффективно решать вопросы, связанные с предотвращением использования систем электронных платежей для отмывания денег — необходимо широкое сотрудничество и совместные действия правительства и разработчиков систем электронных платежей, а также правительств ведущих государств с тем, чтобы перекрыть каналы легализации незаконных финансовых средств с использованием систем электронных

платежей;

- сотрудничество в области стандартов (которые регулируют прозрачность) и активный контроль за возможной эксплуатацией выявленных уязвимостей в интересах преступных группировок могут стать залогом успешной защиты систем электронной оплаты от использования в схемах, направленных на отмывание денег, финансирование терроризма и финансирование распространения оружия массового уничтожения;

- проблема отмывания денег с использованием систем электронных платежей должна решаться на международном уровне. Эффективная правоприменительная деятельность требуется, чтобы национальные правительства сотрудничали в урегулировании основных правил создания систем электронных платежей и операций с их применением;

- система ПОД/ФТ, включая мероприятия в отношении усиления контроля за использованием электронных платежей, должна быть ориентирована прежде всего на превентивное реагирование — предупреждение и недопущение проникновения преступных доходов как в финансовый сектор, так и в экономику страны в целом.

§2. Общие и специально-криминологические меры предупреждения

Предупреждение преступности представляет собой целенаправленную деятельность, исходящую от различных субъектов. Среди субъектов предупредительной деятельности необходимо выделить специализированные и неспециализированные[38]. В качестве критерия их разделения выступают возможности и определенность их правовых полномочий. Субъект – это носитель

[38] Ларичев В.Д. Теоретические основы предупреждения преступлений в сфере экономики: Монография. – М.: Юрлитинформ, 2010. С. 72.

определенных прав, имеющий границы своей компетенции, которая регламентируется определенными нормами. Таковыми являются, прежде всего, государство, правоохранительные органы, различные учреждения, организации и объединения. Так, Г. М. Миньковский относит к субъектам предупреждения, помимо вышеназванных, еще и отдельных граждан, на которых закон возложил определенные полномочия по предупреждению преступности[39]. В литературе криминологами предложены достаточно разнообразные классификации мер по противодействию преступности. Так, выделяют по уровню, правовой характеристике, целям и задачам применения данных мер, по субъекту и объекту воздействия, масштабу реализации, по степени интенсивности воздействия, а также по содержанию.

Достаточно распространенной является точка зрения, согласно которой основными звеньями системы противодействия преступности являются такие меры предупреждения, как общесоциальные и специально-криминологические. Относительно рассматриваемой нами проблемы противодействия кредитнобанковским преступлениям, осуществляемая на общесоциальном уровне, данная профилактика, является такой деятельностью, которая направлена на модернизацию общественных отношений посредством разрешения различных глобальных социальных, экономических, а также иных вопросов жизнедеятельности социума, которые масштабно положительным образом отражаются на состоянии кредитнобанковской преступности.

Рост кредитно – банковской преступности и сумм ущерба от преступлений в данной сфере обусловлен не только сложным характером становления рыночной экономики в нашей стране в целом, но также и проблемами культурного, социального и политического характера. Вышеуказанные факторы обладают статусом значимой проблемы, увеличивающей рост криминальных проявлений в кредитно-банковской сфере. Главную роль, по нашему мнению, в системе противодействия вышеуказанной группе преступлений играют

[39] Криминология: учебник / Под. ред. проф. Н.В. Кузнецовой, проф. Г.М. Миньковского. М.: БЕК, 1998. С.195.

экономические факторы.

Можно утверждать, что первостепенной задачей государства является стратегия по обеспечению надлежащего уровня социально-экономического развития России, ее стабильности в политической и военной сферах, а также обеспечение высокого уровня национальной безопасности. Выполнение перечисленных задач позволит обеспечить надлежащую обстановку и создаст благоприятные условия для культурного и личностного роста каждого члена социума, а также позволит избежать угроз безопасности нашей страны как внутри ее, так и с внешней стороны.

С учетом вышеуказанного, полагаем, что меры противодействия кредитнобанковским преступлениям на общесоциальном уровне должны быть в первую очередь направлены на:

– снижение уровня имущественного неравенства населения и его дифференциации путем эффективного развития системы социального обеспечения и гарантий с целью повышения уровня жизни;

– расширение в экономическом секторе круга хозяйствующих субъектов с многообразием применения различных легальных форм собственности и свободный выбор экономического поведения указанными субъектами;

– интенсификацию дальнейшего эффективного развития рыночной экономики в России;

– увеличение уровня инвестиций в различные секторы экономики;

– стимулирование развития промышленного производства;

– обеспечение правовой и экономической защиты частной собственности.

– государственное стимулирование развития малого предпринимательства с возможностью предоставления налоговых кредитов и регулирования налогового бремени.

Противодействие преступлениям с банковскими картами должно осуществляться не только с помощью технических средств, но и целым комплексом мер. Заинтересовавшись данной проблемой, мы составили примерный перечень таких мер. Во-первых, это, конечно же, организационные

меры, в которые включены правила выдачи карты ее держателю и ее использования, правила приема и проверки валидности карты в точке обслуживания, предупреждение банками мошенничеств в точках обслуживания.

Во-вторых, использование технических средств защиты, при попытке получить доступ к услуге с помощью банковской карты, в том числе системы блокировки карты при неверном наборе PIN – кода.

В-третьих, это установка средств видеонаблюдения в местах расположения банкоматов и осуществления денежных операций с помощью банковских карт: в местах оплаты услуг, магазинах и т.д.

В-четвертых, ускорение ответа банка на заявление о потере или краже банковской карты. В настоящее время, любой банк, выдавая пластиковую карту пользователю, в обязательном порядке выдает инструкцию действий в случае кражи или потери карты. В таких случаях держатель карты может связаться с банком по указанным телефонам, после чего банк заблокирует указанную карту на срок от двух недель до одного месяца. Для осуществления такой операции в максимально короткие сроки крайне необходимо улучшение технических условий. Но, все-таки решающую роль в деле борьбы с преступностью в сфере использования банковских карт, на наш взгляд, играет внимательность и 96 бдительность самого держателя карты.

Владелец карты, который больше не нуждается в ней, обязан помнить о том, что выбрасывать ее в целом состоянии категорически запрещается. Необходимо разломить или разрезать ее на несколько частей или нанести вред магнитной полосе. Носить карту вместе с PIN – кодом, например, в кошельке, так же запрещается. Не стоит вводить PIN – код «с листика», лучше запомнить его и не доставать каждый раз листик с цифрами, которые могут увидеть. Большинство преступлений в сфере оборота банковских карт совершаются именно по указанным причинам.

Предупреждение такого рода преступлений является общей и наиболее важной задачей государства и банковских учреждений, без решения которой невозможно дальнейшее успешное развитие электронных платежей.

§3.Меры предупреждения, основанные на совершенствовании банковских технологий

Для минимизации влияния рисковых факторов при использовании банковских карт большое значение имеет налаживание взаимодействия между банком и клиентом. При этом, учитывая сложность построения адекватной статистической модели поведения клиента, можно порекомендовать передать часть функций управления рисками непосредственно держателям карт. Если держатель карты сможет сам определять для себя стандартную модель поведения, банку необходимо обеспечить возможность оперативно изменять параметры модели использования карты самому клиенту.

К таким параметрам следует отнести:

- регион использования карты (чем меньше регион, тем меньше риски успешного использования поддельной карты);

- установление лимитов на сумму и количество операций на покупки и выдачу наличных (на один день, на неделю, на месяц и т.д.);

- определение категорий торговых точек (интернет, заказы по почте, покупки в обычных магазинах и т.д.).

Управление параметрами риска клиентом может осуществляться через:

- круглосуточную службу помощи;

- автоматизированную службу помощи, позволяющую получать информацию по счету и блокировать/разблокировать карту;

- услугу «Мобильный банк», позволяющую в режиме онлайн получать SMS-сообщения о любом движении по счету; узнавать остаток по счету; блокировать/разблокировать карту; устанавливать регион использования карты.

Введение ограничений на использование карты самим клиентом в значительной степени повышает эффективность работы банка и позволяет на ранней стадии выявлять случаи подделки карт.

Особо следует отметить реакцию регулятора на складывающуюся тревожную ситуацию в области карточного бизнеса коммерческих банков. Центральный Банк Российской Федерации 01 марта 2013 года направил в кредитные организации Письмо № 34-Т «О рекомендациях по повышению уровня безопасности при использовании банкоматов и платежных терминалов».

Банк России, в частности, рекомендует:

- классифицировать места установки банкоматов и платежных терминалов (далее – устройства) по степени риска подвергнуться попыткам физического взлома, установки скиммингового оборудования и (или) воздействия вредоносного кода, а также совершения несанкционированных операций, и периодически пересматривать классификацию мест установки устройств по мере развития технологий, в том числе технологий атак;

- осуществлять на регулярной основе, в зависимости от классификации места установки устройства, контроль внешнего вида устройства, а также действий обслуживающих данное устройство организаций;

- оборудовать устройства системами видеонаблюдения (минимум двумя видеокамерами) со сроком хранения записей видеосъемки не менее 60 календарных дней;

- размещать на экране устройства либо в пределах прямой видимости от него предупреждающие сообщения о необходимости соблюдения мер предосторожности при наборе персонального идентификационного номера;

- устанавливать устройства в безопасных местах (например, в государственных учреждениях, собственных подразделениях, крупных торговых комплексах, гостиницах, аэропортах и тому подобное);

- страховать устройства и (или) наличные денежные средства, находящиеся внутри данных устройств[40].

Банк России также настоятельно рекомендует коммерческим банкам уходить от использования пластиковых карт с магнитной полосой и заменять их на чиповые – как более надежные и менее подверженные криминальному

[40] Вестник Банка России. М.: ЗАО «АЭИ «ПРАЙМ», 2013. №15. 54 с

воздействию.

Издательский дом «Комсомольская правда» 11 сентября 2016 года организовал круглый стол «Состояние российского рынка банковских пластиковых карт: изменения законодательства, тенденции и перспективы. Насколько защищены клиенты?». В рамках мероприятия обсуждались такие вопросы, как финансовая безопасность россиян, меры для борьбы с мошенничеством в банковской сфере, развитие в стране рынка банковских пластиковых карт[41].

К сожалению, статистика происшествий, связанных с банкоматами и банковскими картами, указывает на недостаточный уровень компетенции сотрудников служб экономической безопасности в данном вопросе.

Таким образом, мы приходим к выводу, что для обеспечения безопасности банкоматов и банкоматных карт в банках должны быть намечены и реализованы следующие организационно-технические мероприятия:

1. Осуществление выездной проверки места установки банкомата на соответствие требованиям:

- помещение объекта, где установлен банкомат, должно охраняться службой безопасности арендодателя, либо организации, где устанавливается банкомат, или техническими системами безопасности;

- банкомат должен находиться в зоне видеонаблюдения или в зоне видимости охраны арендодателя.

Если это невозможно, то безопасность банкомата должна быть обеспечена техническими средствами (охранная сигнализация с выводом сигнала на ПЦН охранной организации);

- место установки банкомата должно исключать возможность наблюдения с лестниц и балконов за действиями клиентов на клавиатуре банкомата;

- банкомат, установленный вне помещения банка, должен быть закреплен к полу.

---

[41] Мошенничество с банковскими картами. Насколько защищены клиенты? // Национальное агентство финансовых исследований [электронный ресурс]. Режим доступа: http://nacfin.ru/novosti-ianalitika/publications/article/single/10664.html (17.04.2017).

Если это невозможно, то безопасность банкомата осуществляется техническими средствами (охранная сигнализация с выводом сигнала на ПЦН охранной организации);

- порядок допуска сотрудников банка к банкомату для его технического обслуживания и инкассирования, в том числе допуск вооруженного охранника, должен быть определен на этапе подписания договора.

Проверка документов сотрудников инкассации банка охраной объекта арендодателя должна осуществляться до момента выноса инкассаторами банка сумок с наличностью из специального транспорта;

- со стороны арендодателя не должно быть препятствий подъезду бронированного автомобиля максимально близко к инкассируемому объекту и парковке автомобиля на этом месте до выхода бригады из помещения;

- банкомат, установленный вне помещения банка, не должен размещаться между двумя и более не блокируемыми при инкассации дверями.

Если блокировка дверей невозможна, безопасность процесса инкассации должна быть обеспечена другими возможными способами с соблюдением всех необходимых мер безопасности.

2. Соблюдение требований технической укрепленности мест установки банкоматов: стены должны соответствовать требованиям ГОСТ Р 51113-97 или 4 и 3 класс устойчивости ко взлому по РД МВД России 78.36.003-2002; защитное остекление должно соответствовать требованиям ГОСТ 51136-2008.

3. При установке банкомата в банке (обычно это зона доступа 24х7), необходимо оснащать помещение камерами видеонаблюдения с выводом on-line изображения в мониторинговый центр службы экономической безопасности (система удаленного видеонаблюдения).

4. Использование новейших разработок – технических средств защиты и предупреждения – также является эффективным средством сохранности банкоматов:

- система ограничения доступа в круглосуточную зону самообслуживания банкомата компании «ЭНИГМА» – Привратник – 02А;

- система дымовой защиты «Protect», выпускающая «сухой» дым, препятствуя злоумышленникам ориентироваться в замкнутом пространстве;

- изделие «Алабай», позволяющее сигнализировать о попытках взлома, подбора ключей, включать громкий звуковой сигнал тревоги и с навигационной точностью при помощи компьютера следить за перемещением украденного банкомата.

5. Обследование банкоматов на наличие признаков установки скиммингового оборудования и работоспособности систем локального видеонаблюдения должно проводиться на регулярной плановой основе.

6. Размещение на экране банкомата либо в пределах прямой видимости от него предупреждающих сообщений о необходимости соблюдения мер предосторожности при наборе персонального идентификационного номера.

7. Оснащение банкомата системой локального видеонаблюдения (минимум две камеры) со сроком хранения записей видеосъемки не менее 60 календарных дней.

8. Установка на банкоматы специального антискиммингового оборудования.

Помимо всего перечисленного, службы безопасности и кадровые службы коммерческих банков обязательно должны учитывать следующее обстоятельство. По данным Центрального банка Российской Федерации, более 15 % средств было похищено путем сговора между владельцем карты и третьими лицами. Есть основание предположить, что сообщниками преступников могут выступать и работники банков – эмитентов пластиковых карт[42]. Это накладывает особую ответственность на кадровые и службы безопасности банков при приеме служащих на работу и вызывает необходимость постоянно осуществлять мониторинг персонала на предмет совершения противоправных действий.

Таким образом, нами не только показаны наиболее слабые, незащищенные моменты в безопасном использовании банковских карт и банкоматов, но и даны

[42] Шаламов Г.А. Воровство в банковской сфере: моногра- фия. Иркутск: Изд-во ИрГТУ, 2016. С.110.

конкретные рекомендации по обеспечению безопасности банкоматов и противодействию мошенничеству с банковскими картами. Это вызывает необходимость перестройки работы не только служб безопасности, но и всех подразделений коммерческих банков.

ЗАКЛЮЧЕНИЕ

Преступления, совершаемые с подделкой кредитных и расчетных карт, направлены на мошенническое завладение находящимися в оперативном банковском управлении денежными средствами.

Следует отметить, что подделка пластиковых карт – достаточно сложная, да и дорогостоящая операция, требующая специальное оборудование. Поэтому она может осуществляться только организованными преступными группами с привлечением специальной техники и технологии. При совершении подобного рода преступлений возможно использование как поддельных пластиковых карт, так и пластиковых карт, надлежаще изготовленных, но содержащих ложные сведения. При этом подделка может быть как полной, так и частичной. Все совершаемые в сфере платежей по банковским картам преступления, в зависимости от конечной цели бывают направленными на получение выгоды от сбыта поддельных банковских карт и на хищение денежных средств, находящихся на банковском счете.

Согласно основным направлениям преступной деятельности можно выделить следующие типы:

1. «Виртуальный товарообмен».
2. «Легкие деньги».
3. Лже-благотворительность.
4. Мошенничество в сфере интернет-знакомств.
5. Телеработа, удаленный заработок.
6. Мошенничество в сфере услуг.
7. Инвестиционные мошенничества.
8. Компьютерное мошенничество.

Проведя анализ способов совершения преступлений, нам удалось установить, что данное явление можно разделить на три категории: «Фишинг» (phishing) (англ.) представляет собой производное от следующих двух слов:

password – пароль и fishing – рыбная ловля, выуживание.

Появление в конце 2003 года эксплойта уязвимости с подменой реального URL привело к появлению нового вида «фишинга» – «спуфинг» (spoofing). В случае использования данной уязвимости атакуемый пользователь визуально может наблюдать настоящий адрес банковского сайта в адресной строке браузера, но находиться сам при этом будет на поддельном сайте. Несколько особняком стоит «кардинг» (carding), как форма компьютерного мошенничества, известный и в своих «несетевых» аналогах. Суть мошеннической схемы заключается в использовании чужих реквизитов платежных средств: дебетовых и кредитных банковских при расчетах за покупку.

Сегодня существуют две относительно самостоятельные группы преступлений, именуемых нами преступлениями в сфере банковских технологий: традиционные преступные схемы, реализуемые посредством пластиковых карт, и преступность с использованием пластиковых карт совершаемая посредством Интернет.

В настоящее время для коммерческих организаций резко возросли риски, связанные с деятельностью киберпреступников.

В законодательной базе должны быть предусмотрена ответственность за преступления в сфере информационных технологий, уточнены полномочия органов власти, для того чтобы каждый гражданин и представитель бизнес-сообщества понимал, куда обращаться и как наиболее эффективно добиться расследования киберпреступлений и преследования злоумышленников.

При совершении преступлений с использованием кредитных и расчетных карт способ совершения позволяет существенно охарактеризовать отдельные личностные данные преступника. Так, хищения путем мошенничества совершают так называемые профессиональные «компьютерные» преступники с выраженными корыстными целями, в качестве соучастников или непосредственно исполнителей выступают сотрудники эмитента, мерчанта, эквайера, т е лица, также имеющие определенную профессиональную подготовку и имеющие доступ к оформлению расчетных операций с использованием

платежно-расчетных карт. Сотрудники банков, совершающие хищения с использованием кредитных и расчетных карт, имеют доступ к персональным данным лица, обращавшегося в банк по какому-либо вопросу. И, напротив, при совершении тайного хищения денежных средств с использованием кредитных и расчетных карт, например, при хищении карты и PIN-кода преступник может не обладать никакими специальными знаниями, кроме как умением пользоваться банкоматом.

Лица, которые занимаются мошенничеством с использованием платежных карт, достаточно четко отличаются от других преступников, так как им не свойственны такие черты характера, как импульсивность и агрессивность, как правило, они характеризуются стремлением к повышению социального статуса. Они имеют широкий кругозор, высокий интеллектуальный уровень, хорошую ориентацию в экономических и юридических вопросах.

Активное внедрение различных систем расчетов с использованием электронных платежей сопровождается появлением новых источников рисков, связанных с недостаточным уровнем обеспечения информационной безопасности на всех участках информационного контура, который формируется в процессе выполнения расчетов между участниками сделки.

В условиях глобального характера рисков использования электронных платежей необходимо учитывать, что существующая правоприменительная практика не всегда может эффективно решать вопросы, связанные с предотвращением использования систем электронных платежей для отмывания денег — необходимо широкое сотрудничество и совместные действия правительства и разработчиков систем электронных платежей, а также правительств ведущих государств с тем, чтобы перекрыть каналы легализации незаконных финансовых средств с использованием систем электронных платежей.

Сотрудничество в области стандартов (которые регулируют прозрачность) и активный контроль за возможной эксплуатацией выявленных уязвимостей в интересах преступных группировок могут стать залогом успешной защиты систем

электронной оплаты от использования в схемах, направленных на отмывание денег, финансирование терроризма и финансирование распространения оружия массового уничтожения.

Проблема отмывания денег с использованием систем электронных платежей должна решаться на международном уровне. Эффективная правоприменительная деятельность требуется, чтобы национальные правительства сотрудничали в урегулировании основных правил создания систем электронных платежей и операций с их применением.

Система ПОД/ФТ, включая мероприятия в отношении усиления контроля за использованием электронных платежей, должна быть ориентирована прежде всего на превентивное реагирование — предупреждение и недопущение проникновения преступных доходов как в финансовый сектор, так и в экономику страны в целом.

Полагаем, что меры противодействия кредитно-банковским преступлениям на общесоциальном уровне должны быть в первую очередь направлены на:

– снижение уровня имущественного неравенства населения и его дифференциации путем эффективного развития системы социального обеспечения и гарантий с целью повышения уровня жизни;

– расширение в экономическом секторе круга хозяйствующих субъектов с многообразием применения различных легальных форм собственности и свободный выбор экономического поведения указанными субъектами;

– интенсификацию дальнейшего эффективного развития рыночной экономики в России;

– увеличение уровня инвестиций в различные секторы экономики;

– стимулирование развития промышленного производства;

– обеспечение правовой и экономической защиты частной собственности.

– государственное стимулирование развития малого предпринимательства с возможностью предоставления налоговых кредитов и регулирования налогового бремени.

Для обеспечения безопасности банкоматов и банкоматных карт в банках

должны быть намечены и реализованы следующие организационно-технические мероприятия:

1. Осуществление выездной проверки места установки банкомата на соответствие требованиям:

- помещение объекта, где установлен банкомат, должно охраняться службой безопасности арендодателя, либо организации, где устанавливается банкомат, или техническими системами безопасности;

- банкомат должен находиться в зоне видеонаблюдения или в зоне видимости охраны арендодателя.

Если это невозможно, то безопасность банкомата должна быть обеспечена техническими средствами (охранная сигнализация с выводом сигнала на ПЦН охранной организации);

- место установки банкомата должно исключать возможность наблюдения с лестниц и балконов за действиями клиентов на клавиатуре банкомата;

- банкомат, установленный вне помещения банка, должен быть закреплен к полу.

Если это невозможно, то безопасность банкомата осуществляется техническими средствами (охранная сигнализация с выводом сигнала на ПЦН охранной организации);

- порядок допуска сотрудников банка к банкомату для его технического обслуживания и инкассирования, в том числе допуск вооруженного охранника, должен быть определен на этапе подписания договора.

Проверка документов сотрудников инкассации банка охраной объекта арендодателя должна осуществляться до момента выноса инкассаторами банка сумок с наличностью из специального транспорта;

- со стороны арендодателя не должно быть препятствий подъезду бронированного автомобиля максимально близко к инкассируемому объекту и парковке автомобиля на этом месте до выхода бригады из помещения;

- банкомат, установленный вне помещения банка, не должен размещаться между двумя и более не блокируемыми при инкассации дверями.

Если блокировка дверей невозможна, безопасность процесса инкассации должна быть обеспечена другими возможными способами с соблюдением всех необходимых мер безопасности.

2. Соблюдение требований технической укрепленности мест установки банкоматов: стены должны соответствовать требованиям ГОСТ Р 51113-97 или 4 и 3 класс устойчивости ко взлому по РД МВД России 78.36.003-2002; защитное остекление должно соответствовать требованиям ГОСТ 51136-2008.

3. При установке банкомата в банке (обычно это зона доступа 24х7), необходимо оснащать помещение камерами видеонаблюдения с выводом on-line изображения в мониторинговый центр службы экономической безопасности (система удаленного видеонаблюдения).

4. Использование новейших разработок – технических средств защиты и предупреждения – также является эффективным средством сохранности банкоматов:

- система ограничения доступа в круглосуточную зону самообслуживания банкомата компании «ЭНИГМА» – Привратник – 02А;

- система дымовой защиты «Protect», выпускающая «сухой» дым, препятствуя злоумышленникам ориентироваться в замкнутом пространстве;

- изделие «Алабай», позволяющее сигнализировать о попытках взлома, подбора ключей, включать громкий звуковой сигнал тревоги и с навигационной точностью при помощи компьютера следить за перемещением украденного банкомата.

5. Обследование банкоматов на наличие признаков установки скиммингового оборудования и работоспособности систем локального видеонаблюдения должно проводиться на регулярной плановой основе.

6. Размещение на экране банкомата либо в пределах прямой видимости от него предупреждающих сообщений о необходимости соблюдения мер предосторожности при наборе персонального идентификационного номера.

7. Оснащение банкомата системой локального видеонаблюдения (минимум две камеры) со сроком хранения записей видеосъемки не менее 60 календарных

дней.

8. Установка на банкоматы специального антискиммингового оборудования.

Таким образом, нами не только показаны наиболее слабые, незащищенные моменты в безопасном использовании банковских карт и банкоматов, но и даны конкретные рекомендации по обеспечению безопасности банкоматов и противодействию мошенничеству с банковскими картами. Это вызывает необходимость перестройки работы не только служб безопасности, но и всех подразделений коммерческих банков.

СПИСОК ЛИТЕРАТУРЫ

Официальные документы

1. Федеральный закон от 27.06.2011 №161-ФЗ «О национальной платежной системе» (ред. от 29.12.2014) // Российская газета. – №139. – 2011.
2. Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ 9 сент. 2000 г. N Пр-1895) // Рос. газ. 2000. 28 сент.
3. Конвенция о преступности в сфере компьютерной информации (ETS N 185) (Заключена в г. Будапеште 23 нояб. 2001 г.). Доступ из справ.-правовой системы «консультантПлюс»

Монографии, публикации

4. Айдарова А.Ю. Проблема защиты населения от преступлений в сфере мошенничества с банковскими картами / А.Ю. Айдарова, Н.В. Агеев // Инновационные технологии в науке и образовании: Материалы III Междунар. науч.-практ. конф. (Чебоксары, 23 окт. 2015 г.) / Редкол.: О.Н. Широков [и др.]. – Чебоксары: ЦНС «Интерактив плюс», 2015. – №3 (3). – С. 352–353.
5. Акерлоф Дж. Рынок "лимонов": неопределенность качества и рыночный механизм // THESIS. 1994. Вып. 6. С. 91 - 104.
6. Андреев Б.В., Пак П.Н., Хорст В.П. Расследование преступлений в сфере компьютерной информации. М.: Юрлитинформ, 2012. - С.69.
7. Анохин В.Н. Электронные платежи в обеспечении эффективного функционирования платежной системы: дисс… канд.экон.наук. – М., 2015. – С. 56.
8. Главной угрозой остается CNP-фрод [Электронный ресурс] // ПЛАС- журнал. – 30.04.2014. – Режим доступа: http://www.plusworld.ru/journal/online/art170778/.
9. Глотов В.С., Шалатов Д.В. Интернет–технологии и электронная торговля: экономика, право, программное обеспечение.–Изд–е 2 — е, перераб. и доп.–В 2-х ч. / Под ред. С.А. Глотова / Центр прав человека и защиты прав потребителей РГТЭУ, Кубанский научный Центр социальных исследований «Законодательная инициатива», Краснодарский ин-т (филиал) РГТЭУ.–М.: НИЦ «Инженер», 2014.

С. 183.

10. Горовцова М. Возврат денег по несанкционированным транзакциям: что изменится с 1 января 2014 года [Электронный ресурс] // ГАРАНТ.РУ. – 26.11.2013. – Режим доступа: www.garant.ru/article/507445/#ixzz3cr32JJNs.

11. Горянинов К.К., Овчинский В.С., Синилов Г.К. Теория оперативно-розыскной деятельности. М.: Изд-во ИНФРА-М, 2014.

12. Гудзь Е.Г. Актуальность проблемы ведения борьбы с преступлениями в сфере высоких технологий // Сб. докладов науч.-практ. семинара “Применение специальных познаний при раскрытии и расследовании преступлений, сопряженных с использованием компьютерных средств, М., 2012. С.62.

13. Еремченко В. И., Зиновьева Н. С. Современные информационно-телекоммуникационные системы: проблемы и возможности их использования в раскрытии и расследовании террористической и экстремистской деятельности // Преступность в СНГ: проблемы предупреждения и раскрытия преступлений: сборник материалов международной научно-практической конференции. Воронежский институт МВД России. Воронеж. – 2015. – С. 27-28.

14. Есаков П., Чернышев А. Банковская отрасль на пороге выхода из «SMS-тупика»? [Электронный ресурс] // Computel. ПЛАС. – 2014. –№ 4 [203]: апрель. – Режим доступа: http://computel.ru/upload/Computel_newpix_ caps2.pdf.

15. Карпович О.Г., Трунцевский Ю.В. Серьезные экономические преступления XXI века: опыт противодействия им в Великобритании, России и США: Монография. М.: ЮНИТИ ДАНА; Закон и право, 2013.

16. Кесареева Т. П. Криминологическая характеристика и проблемы предупреждения преступности в российском сегменте сети Интернет. Автореф. дис… канд. юрид. наук. – М., 2014. – С.4

17. Киданов Р.В. Организованные формы экономической преступности (статья выполнена в рамках программы малых грантов). URL: http://kiev-security.org.ua/box/4/92.shtml.

18. Кудрявцев В.Н. Борьба мотивов в преступном поведении. – М., Норма. – 2014.

19. Курс уголовного права. Общая часть. Т.1 / Под ред. Н.Ф. Кузнецовой, И.М.

Тяжковой. – М.: ИКД «Зерцало-М», 2013. – С. 214.

20. Лепешкина М.Н. Эволюция понятия "экономическая безопасность" в США, Западной Европе и России // Экономическая наука и практика: материалы междунар. науч. конф. (г. Чита, февраль 2012 г.). Чита: Молодой ученый, 2012. С. 7 - 9.

21. Лукьянов С. О. Мошенничество с использованием банковских карт в России: современное состояние и виды защиты // Вестник ТГЭУ. –2012. – №2. – С. 118.

22. Лунев В.В. О криминализации экономических преступлений предпринимателей // Дальневосточный федеральный университет. URL: http://www.crime.vl.ru/index.php?p=3866&more=1&c=1&tb=1&pb=1.

23. Мазуров В.А. Преступность в сфере высоких технологий: понятие, общая характеристика, тенденции // Вестник Томского государственного университета. 2007. № 300-1.

24. Маркушин А.Г. Оперативно-розыскная деятельность. М.: Изд-во Юрайт, 2013.

25. Мещеряков В.А. Теоретические основы криминалистической классификации преступлений в сфере компьютерной информации // Конфидент. – 1999. – №4-С.5.

26. Нагорный В. А. Скимминг в системе преступлений, сопряженных с использованием платежных карт: современное состояние, тенденции и проблемы уголовно-правовой квалификации// Методология и практика современной юриспруденции. Сборник научных трудов. М.: Издательство «Планета». – 2013. – С.87

27. Никулина О.В., Иванова Н.В. Развитие инновационных технологий в банковской деятельности // Экономика: теория и практика. – 2013. – № 4 (32). – С. 20-26.

28. Осипенко А.Л. Сетевая компьютерная преступность теория и практика борьбы: монография. Омск: Омская академия МВД России, 2015.

29. Паненков А.А. Система преступлений в сфере компьютерной информации, входящих в структуру террористической деятельности (кибертерроризм) как реальная угроза внешнему и внутреннему контурам национальной безопасности России // Военно-юридический журнал. № 4. – 2014. – С.87.

30. Петровский С. В. Интернет-услуги в российском праве. – М.: Агентство «Издательский сервис», 2003. – С.8.

31. Поляков В.В. Обстановка совершения преступлений в сфере компьютерной информации как элемент криминалистической характеристики // Известия Алтайского государственного университета. 2013. № 2.

32. Поляков В.В. Особенности расследования неправомерного удаленного доступа к компьютерной информации: дис. ... канд. юрид. наук. Омск, 2011.

33. Поляков В.В., Слободян С.М. Анализ высокотехнологичных способов неправомерного удаленного доступа к компьютерной информации // Известия Томского политехнического университета. 2015. Т. 310. № 1.

34. Российское уголовное право. В двух томах. Том I. Общая часть. Под ред. проф. А.И. Рарога. – М.: Профобразование. – 2001. – С. 196.

35. Суслина Е.В. Ответственность за мошенничество по Уголовному кодексу Российской Федерации: автореф. дисс. канд. юрид. наук. – Екатеринбург, 2014. – 27 с.

36. Трунцевский Ю.В. Понятие транснационального преступления // Международное уголовное право. 2014. N 3. С. 9 - 12.

37. Трунцевский Ю.В., Саркисян К.А., Янюк Д.А. Мошенничество в медицинской системе США: // Медицинское право. 2014. N 2. С. 19 - 24.

38. Чирков А.В. Проблемы реализации законодательства о национальной платежной системе в части ответственности банков в расчетных правоотношениях // Банковское право. – М.: Юрист, 2013. – № 5. – С. 63-68.

39. Ширинян И.Г. Мировой опыт использования инсайдерской информации на рынке // Рынок ценных бумаг. 2014. N 10.

Юридическая практика

40. В Иркутске задержали программиста-олимпиадника // Рос. газ. [электронный ресурс]. Режим доступа: http://www.rg.ru/2013/07/09/reg-sibfo/haker-anons.html (17.01.2017).

41. В Новосибирске неизвестный украл два миллиона, взо- рвав банкомат // Рос. газ. [электронный ресурс]. Режим до- ступа: http://www.rg.ru/2013/08/06/reg-

sibfo/bankomatanons.html (17.01.2017).

42. В Петербурге задержали хакеров // Российская газета [электронный ресурс]. Режим доступа: http://www.rg.ru/2013/03/05/reg-szfo/bankomat-anons.html (17.01.2017).

43. Во Владимире возбуждено дело по хищению банкома- тов // Рос. газ. [электронный ресурс]. Режим доступа: http://www.rg.ru/2013/10/18/reg-cfo/bankomat-anons.html (17.01.2017).