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

Кафедра экономики, финансового права и информационных технологий в деятельности ОВД

О.Г.Шмелева, Г.Н.Хадиуллина

МЕРЫ ПО ОБЕСПЕЧЕНИЮ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ, НАПРАВЛЕННЫЕ НА ПРОТИВОДЕЙСТВИЕ НЕЗАКОННОЙ БАНКОВСКОЙ ДЕЯТЕЛЬНОСТИ, СВЯЗАННОЙ С ОБОРОТОМ НАЛИЧНЫХ ДЕНЕЖНЫХ СРЕДСТВ

Казань 2017

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

Кафедра экономики, финансового права и информационных технологий в деятельности ОВД

О.Г.Шмелева, Г.Н.Хадиуллина

МЕРЫ ПО ОБЕСПЕЧЕНИЮ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ, НАПРАВЛЕННЫЕ НА ПРОТИВОДЕЙСТВИЕ НЕЗАКОННОЙ БАНКОВСКОЙ ДЕЯТЕЛЬНОСТИ, СВЯЗАННОЙ С ОБОРОТОМ НАЛИЧНЫХ ДЕНЕЖНЫХ СРЕДСТВ

Научно-практическое пособие

Казань 2017

ОГЛАВЛЕНИЕ

		Стр.
	Введение	4
Глава 1	Преступления в банковской сфере и их характеристика	
1.1.	Становление банковских технологий и характеристика правонарушений (преступлений), совершаемых с их использованием в 90-гг. XX в. - начале XXI в.	6
1.2.	Характеристика правонарушений (преступлений), совершаемых с использованием банковских технологий в современной экономике	10
1.3.	Факторы усиления банковских рисков и необходимость управления ими в системе экономической безопасности кредитных организаций	13
Глава 2	Организация и управление безопасностью в финансово-кредитных организациях	
2.1.	Концептуальные основы функционирования системы экономической безопасности банков	17
2.2.	Правовые, организационные и технико-технологические основы обеспечения экономической безопасности банка	21
2.3.	Защита от преступлений, посягающих на порядок функционирования банка	24
Глава 3	Структура и содержание методики расследования преступлений, совершаемых с использованием банковских технологий в современной экономике	
3.1.	Композиционная функциональная модель противоправных действий в отношении субъектов, управляющих своими активами через системы дистанционного банковского обслуживания	29
3.2.	Методы диагностирования мошеннических сделок в практике управления банковскими рисками	32
3.3.	Методика расследования преступлений, связанных с криминальным использованием пластиковых платежных средств, и направления ее совершенствования	35
3.4.	Методика расследования изготовления или сбыта поддельных денег или ценных бумаг	49
3.5.	Уголовно-правовые и криминологические меры противодействия преступлениям, совершаемым в сфере банковской деятельности, связанной с оборотом наличных денежных средств	51
	Заключение	67
	Список литературы	69

ВВЕДЕНИЕ

В настоящее время банковская система Российской Федерации характеризуется существенными изменениями, которые обусловлены глобализацией мирового экономического пространства, развитием информационно-коммуникационных технологий, появлением новых видов банковских услуг, внедрением продуктовых и процессных инноваций в банковскую деятельность и др. В связи с этим усиливается опасность непредсказуемых изменений в содержании факторов внешней и внутренней среды банковских организаций, что может инициировать возникновение рискообразующих факторов для системы банковской безопасности. Существенный вред банку могут нанести противоправные действия персонала и клиентов. В этих условиях возникает необходимость изучения рисков банковской деятельности и инструментов управления ими, исследования структуры и содержания методики расследования преступлений, совершаемых с использованием высоких банковских технологий в современной экономике, определения методических подходов к организации деятельности подразделений банковской безопасности.

Отсутствие актуальной методической литературы по рассматриваемой категории преступлений, учитывающей изменения в действующем законодательстве Российской Федерации, а также складывающаяся оперативная обстановка по линии преступлений, связанных с незаконной банковской деятельностью, знание которых обеспечивает эффективность деятельности подразделений экономической безопасности и противодействия коррупции, определили цель и задачи исследования.

Цель исследования заключается в разработке научной продукции по вопросам теории и практики выявления преступлений, связанных с незаконной банковской деятельностью в сфере оборота наличных денежных средств. Необходимость реализации цели определила состав задач, которые заключаются в следующем:

1. Научная разработка системы обобщенных типичных данных, создающих риски функционирования системы экономической безопасности кредитных организаций.

2. Характеристика совершающихся в кредитно-финансовой сфере преступлений и определениеих наиболее типичных оперативно значимых признаков.

3. Анализ способов совершения преступления, механизмовследообразования преступных действий, а также личностных данных субъекта преступления в сфере дистанционного банковского обслуживания, оборота наличных денежных средств, изготовления или сбыта поддельных денег или ценных бумаг.

4. Разработка методических подходов к организации деятельности подразделений банковской безопасности.

Данной проблеме посвящено значительное число работ, среди которых труды ученых-специалистов в области уголовного права, криминологии, гражданского и банковского права - Антонова И.О., Арефьевой Е.Н.,

Аверьяновой Т.В., Астапкиной С.М., Борзенкова Г.Н., Васюкова С.В., Вехова В.Б., Викулина А.Ю., Волженкина Б.В., Гамзы В.А., Гаухмана Л.Д., Ефимовой Л.Г., Жалинского А.Э., Жукова Е.Ф., Ивасенко А.Г., Ларичева В.Д., Ляпунова Ю.И., Макаровой Г.Л., Максимова С.В., Новоселовой Л.А., Олейнйк О.М., Суханова Е.А, Тосуняна Г.А., Усоскина В.М., Хилюты В.В., Шалимова А.Н., Южина А.А., Яни П.С., Яцеленко Б.В. и других. Данная проблема стала предметом исследования зарубежных авторов, среди которых Л.Джеймс, Д.Синки, Дж. Т.Уэллс и др. Определенный вклад в решение проблемы противодействия этому виду преступлений внесли авторы инструктивных и аналитических материалов, размещенных на официальных сайтах кредитных организаций, которые направлены на формирование финансовой культуры клиентов банков. В ходе исследования использованы нормы действующего уголовного законодательства РФ; постановления Пленума Верховного Суда РФ; статистические и аналитические данные, материалы судебно-следственной практики по делам о мошенничестве; результаты социологических исследований; научные публикации по теме исследования.

Объектом данного исследования являются общественные отношения, возникающие в процессе предупреждения преступлений с использованием интернет-технологий в банковской сфере. Предмет исследования - криминологическая и уголовно - правовая характеристика преступлений с использованием интернет-технологий в банковской сфере.

Работа состоит из трех глав, в которых представлены, соответственно, теоретические подходы к содержанию системы банковской безопасности, инструменты управления рисками банковской деятельности, криминологическая и уголовно - правовая характеристика преступлений с использованием интернет-технологий в банковской сфере.

Глава 1.Преступления в банковской сфере и их характеристика

1.1. Становление банковских технологий и характеристика правонарушений (преступлений), совершаемых с их использованием в 90-гг. XX в. - начале XXI в.

Интернет-банкинг – это электронная банковская деятельность, осуществляемая в информационной среде глобальной компьютерной сети Интернет.Под угрозами информационной безопасности банка понимается потенциальная возможность нарушения главных свойств информации.

Эволюция банковской системы в сторону дистанционной модели банковского обслуживания обусловлена рядом объективных особенностей экономической и социальной среды, в которой существуют банки, и в первую очередь, изменениями в образе жизни людей, внедрением новых информационных технологий и автоматизацией банковских операций. Особое влияние оказывают следующие факторы: растущая конкуренция;фактор времени;развивающиеся средства коммуникации.

Классификация банков по моделям обслуживания включает:

1. Традиционные банки – банки, предоставляющие банковский сервис по offline-каналам (системы персонального обслуживания клиентов у окошка кассы банка).
2. Виртуальные банки – предлагают интерактивное банковское обслуживание клиентов через сеть Интернет. Виртуальные банки принимают вклады и производят платежи, в основном, посредством банкоматов, а также по почте, в тех случаях, когда то или иное учреждение применяет чеки вместо электронной оплаты.
3. Многоканальные банки – банки, сочетающие дистанционное обслуживание с обслуживанием через розничную сеть.
4. Наиболее перспективное направление банковской деятельности – это Интернет-банкинг, основными задачами которого являются снижение расходов клиентов банка и облегчение процедуры осуществления денежных операций.

С юридической точки зрения под *интернет-банкингом* следует понимать деятельность по предоставлению клиенту (физическому или юридическому лицу) удаленного доступа к его счету, открытому в российской либо иностранной организации, осуществляемую данной (кредитной) организацией непосредственно либо через представителей (например, через интернет-систему электронных расчетов) в режиме реального времени с использованием сети Интернет.В свою очередь, с экономической точки зрения *интернет-банкинг* представляет собой систему осуществления с применением того или иного программного обеспечения различных услуг банка (кредитной организации либо оператора интернет-банкинга) по предоставлению доступа к счету клиента через Интернет (с использованием сети Интернет) и осуществлению расчетов в режиме реального времени.

Депозитные учреждения используют интернет-банкинг с целью предложения своим клиентам широкого ассортимента услуг, носящих весьма

разнообразный характер в зависимости от предоставляющего их учреждения. Эти услуги включают в себя изучение балансов, перевод средств с одних счетов на другие, подачу заявок на получение кредита, осуществление электронной оплаты векселей и счетов и предъявление векселей и счетов (когда ремитенты посылают свои векселя и счета через Интернет в банк плательщика, который оплачивает их). Некоторые банковские учреждения предлагают также услуги по страхованию и брокерские услуги. Кроме того, ведение банками своей деловой деятельности через Интернет предоставляет предприятиям возможность обращаться за кредитами, осуществлять телеграфные денежные переводы и пользоваться предоставляемыми через Интернет услугами по контролю и регулированию денежных операций, управлению наличностью и составлению платежных ведомостей.

Преимущества интернет-банкинга: повышение доступности банка всем потенциальным клиентам; отсутствие географической привязки клиента к банку; существенная экономия времени за счет исключения необходимости посещать банк клиенту лично; обеспечение возможности 24 часа в сутки контролировать счета клиентов и, в соответствии с изменившейся ситуацией на финансовых рынках, мгновенно отреагировать на эти изменения (например, закрыв вклады в банке, купив или продав валюту, погасив кредит); повышение степени контроля со стороны клиента за своими операциями; отсутствие необходимости устанавливать на стороне клиента специализированное программное обеспечение; доступность новой услуги всем интернет-клиентам банка, поскольку изменения происходят на сервере банка.

Модели интернет-банкинга включают:

1. Телефонный банкинг (phonebanking) – обслуживание осуществляется посредством телефона.
2. Мобильный банкинг (mobilebanking) – обслуживание осуществляется посредством портативных устройств.
3. PC-банкинг (e-banking) – обслуживание осуществляется посредством персонального компьютера.
4. Видео-банкинг (videobanking) – обслуживание осуществляется посредством систем интерактивного общения с персоналом банка.
5. Домашний банкинг (homebanking) и Банк-Клиент – обслуживание осуществляется посредством установления стационарной связи между банком и клиентом.

Угрозы информационной безопасности, возникающие в связи с внедрением информационных технологий в деятельность банков, подразделяются на:

1. случайные – стихийные бедствия, ошибки по невниманию, ошибки аппаратных и программных средств и т.д.;
2. преднамеренные, т.е. фальсификация или уничтожение данных, неправомерное использование данных, компьютерные преступления и т.д.

К числу угроз информационной безопасности относятся:

1. утрата информации, составляющей банковскую тайну, коммерческую тайну банка и иную защищаемую информацию;

2. искажение (несанкционированная модификация, подделка) защищаемой информации;

3. утечка – несанкционированное ознакомление с защищаемой информацией посторонних лиц (несанкционированный доступ, копирование, хищение и т.д.);

4. несанкционированное использование информационных ресурсов (злоупотребления, мошенничества и т.п.);

5. недоступность информации в результате ее блокирования, сбоя оборудования или программ, дезорганизации функционирования операционных систем рабочих станций, серверов, активного сетевого оборудования, систем управления баз данных, распределенных вычислительных сетей, воздействия вирусов, стихийных бедствий и иных форс-мажорных обстоятельств и злонамеренных действий.

В результате воздействия указанных угроз могут возникнуть следующие негативные последствия, влияющие на состояние информационной безопасности банка и его нормальное функционирование:

1. финансовые потери, связанные с утечкой или разглашением защищаемой информации;

2. финансовые потери, связанные с уничтожением и последующим восстановлением утраченной информации;

3. ущерб от дезорганизации деятельности Банка и потери, связанные с невозможностью выполнения им своих обязательств;

4. ущерб от принятия управленческих решений на основе необъективной информации;

5. ущерб от отсутствия у руководства банка объективной информации;

6. ущерб, нанесенный репутации банка;

7. иной вид ущерба

Информационная безопасность в интернет-банкинге включает следующие элементы:

1. Защита трафика: использование протоколов для безопасного уделенного доступа и шифрования передаваемых корпоративных данныхSecureSocketsLayer (SSL), TransportLayerSecurity (TLS)и удаленный доступ, или VPN-решениявиртуальной частной сети.

2. Использование электронно-цифровой подписи (ЭЦП).

3. Контроль документов в “Бэк-офисе удаленных рабочих мест”.

4. Механизмы аутентификации:

4.1. cookies,

4.2. проверка сертификата SSL для каждого запроса,

4.3. проверка адресных строк и запросов.

Система обеспечения сетевой безопасности представлена нарис. 1.

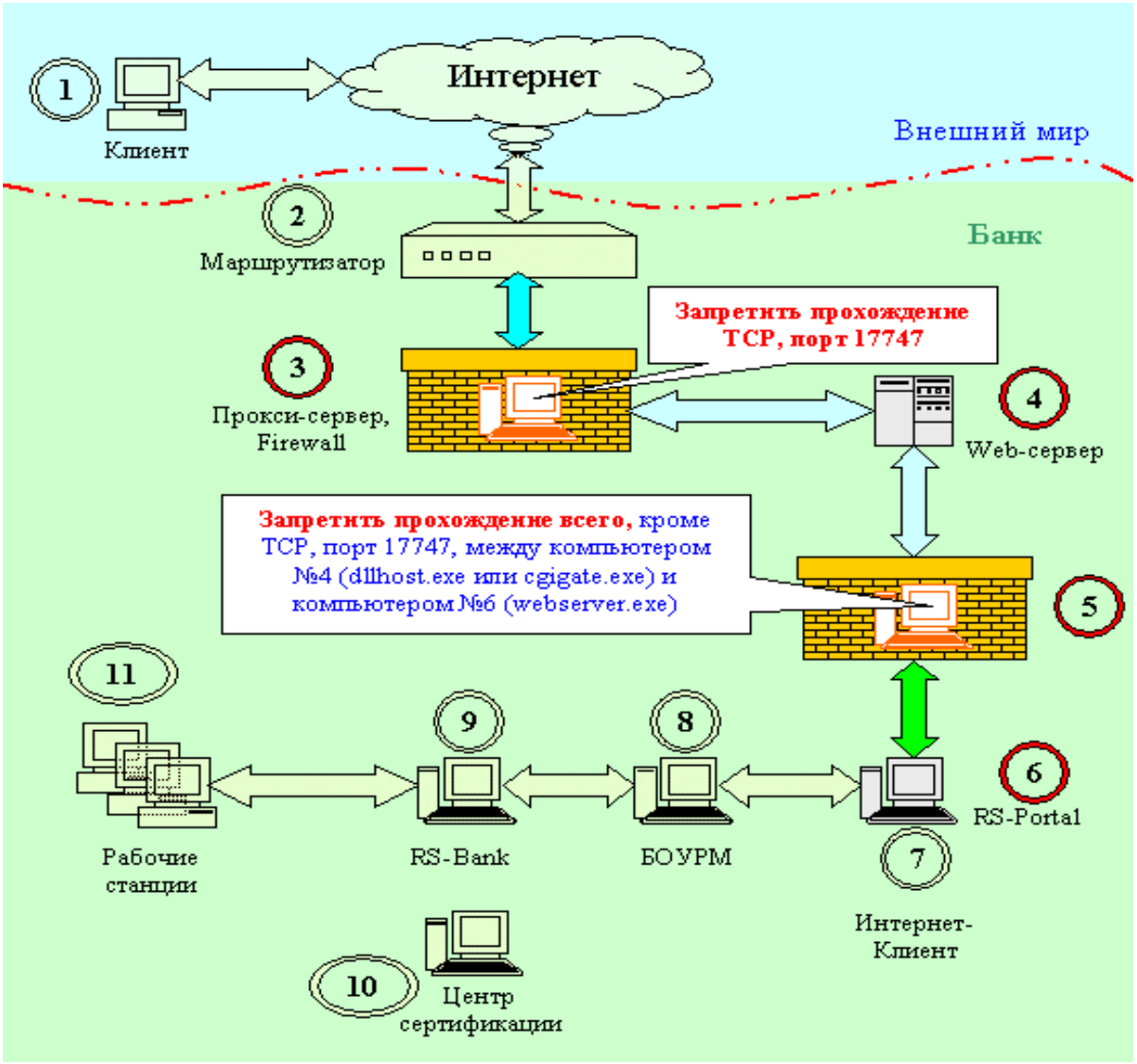

Рис. 1. Система обеспечения сетевой безопасности банка

1 июня 2015 года в Главном управлении безопасности и защиты информации Банка России по поручению Совета Безопасности Российской Федерации создан Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере. К числу его задач относится:

1. Формирование оперативных рекомендаций по снижению рисков, связанных с обеспечением безопасности при предоставлении финансовых услуг и услуг по переводу денежных средств с использованием информационных и телекоммуникационных технологий.

2. Проведение анализа данных о фактах проявления противоправных действий и компьютерных атак в организациях кредитно-финансовой сферы, рисках, связанных с обеспечением безопасности при предоставлении финансовых услуг и услуг по переводу денежных средств с использованием информационных и телекоммуникационных технологий.

3. Установление требований и рекомендаций к реализации контроля в рамках надзора за соблюдением требований Банка России в области обеспечения защиты информации в организациях кредитно-финансовой сферы.

4. Организация и координация оперативного взаимодействия и обмена информацией Центра, правоохранительных органов и организаций кредитно-финансовой сферы, иных организаций.

5. Установление требований и рекомендаций к составу и содержанию информации, передаваемой между Банком России, правоохранительными органами и организациями кредитно-финансовой сферы.

6. Установление требований и рекомендаций в области защиты информации в организациях кредитно-финансовой сферы.

Одной из причин преступных покушений на компьютерные ителекоммуникационные системы является их уязвимость за счет широкого распространения глобальных открытыхкомпьютерных сетей типа Интернет, построенных на основе телекоммуникационных магистралей общего пользования, атакже из-за возможности применения средств вычислительной техники с программным обеспечением, позволяющим легко модифицировать, уничтожать или копировать обрабатываемую информацию. В связи с этим представляется необходимым:

- обеспечить безопасность функционирования банка, его кредитно-финансовой деятельности и защиту конфиденциальной информации;
- организовать работу по правовой, организационной и инженерно-технической защите материальных, финансовых и информационных ресурсов;
- организовать специальное делопроизводство, исключающее несанкционированное получение конфиденциальных сведений;
- выявить и локализовать возможные каналы разглашения, утечки и несанкционированного доступа к конфиденциальной информации в процессе повседневной деятельности и в экстремальных ситуациях;
- обеспечить режим безопасности при проведении всех видов деятельности, включая встречи, переговоры, совещания, связанные с деловым сотрудничеством на национальном и международном уровнях;
- обеспечить охрану зданий, помещений, оборудования и технических средств деятельности банка;
- обеспечить безопасность персонала;
- вести информационно-аналитическую деятельность в интересах оценки ситуации и выявления неправомерных действий злоумышленников и конкурентов.

1.2. Характеристика правонарушений (преступлений), совершаемых с использованием банковских технологий в современной экономике

Компьютерные преступления(ст. 272, 273,274 УК РФ), или киберпреступления, - это преступления, совершенные с использованием компьютерной информации. При этом компьютерная информация является предметом и (или) средством совершения преступления.

Киберпреступления подразделяют на виды в зависимости от объекта и предмета посягательства и т.д. Существует несколько подходов к их

классификации. В соответствии с первым подходом, используемым Организацией Объединенных Наций, выделяют компьютерные преступления и преступления, совершаемые с помощью или посредством компьютеров, компьютерных сетей и иных устройств доступа к киберпространству. В данном контексте компьютерные преступления – это преступления, основным объектом посягательства которых является конфиденциальность, целостность, доступность и безопасное функционирование компьютерных данных и систем. Остальные киберпреступления, помимо компьютерных систем, посягают на другие объекты (в качестве основных): безопасность общества и человека (кибертерроризм), имущество и имущественные права (кражи, мошенничества, совершенные посредством компьютерных систем или в киберпространстве), авторские права (плагиат и пиратство).

Конвенция Совета Европы о киберпреступности изначально подразделяла киберпреступления на четыре группы (затем, в соответствиис дополнительным протоколом, на пять групп). В первую группу входятсобственно «компьютерные преступления», или преступления против конфиденциальности, целостности и доступности компьютерных данных и систем. К ним относятся, в частности, незаконный доступ, незаконный перехват, вмешательство в данные, вмешательство в систему и т.д. Во вторую группу входят преступления, связанные с использованием компьютерных средств. К ним относятся подлог с использованием компьютерных технологий, мошенничество в целях неправомерного извлечения экономической выгоды для себя или третьих лиц. Третью группу составляют преступления, связанные с контентом (содержанием данных). В четвертую группу вошли преступления, связанные с нарушением авторского права и смежных прав. Виды таких преступлений в Конвенции не выделяются: установление таких правонарушений отнесено документом к компетенции национальных законодательств государств. Однако установление преступлений в сфере авторского права должно основываться на исполнении взятых на себя обязательств, закрепленных в Парижском акте от 24.07.71 г. (с изм. от 02.10.79 г.), Бернской конвенции об охране литературных и художественных произведений, Договоре ВОИС по авторскому праву и Соглашении ВОИС о торговых аспектах интеллектуальной собственности.

В начале 2002 г. к Конвенции был принят протокол, добавляющий в перечень преступлений распространение информации расистского и другого характера, подстрекающего к насильственным действиям, ненависти или дискриминации отдельного лица или группы лиц, основывающимся на расовой, национальной, религиозной или этнической принадлежности.

Помимо классификации, предложенной Конвенцией Совета Европы о киберпреступности, существуют и иные официальные и неофициальные классификации киберпреступлений, разработанные специалистами и исследователями (классификация, разработанная рабочей группой Интерпола в 1991 году; классификация, предложенная американским исследователем Д. Л. Шиндлером и т.д.).

В сфере банковской деятельности в составе киберпреступлений целесообразно выделить:

1. Неправомерный доступ к охраняемой законом компьютерной информации.
2. Создание, использование и распространение вредоносных программ для ЭВМ или машинных носителей с такими программами.
3. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.
4. Использование электронного средства платежа без согласия клиента вследствие противоправных действий, потери, нарушения конфиденциальности информации, необходимой для удостоверения клиентом оператора по переводу денежных средств права распоряжаться денежными средствами.
5. Размещение на банкоматах, платежных терминалах скимминговогo оборудования
6. Распространение информации (социальная инженерия), побуждающей клиента сообщить информацию, необходимую для осуществления перевода денежных средств от его имени и др.

Для российского банковского сектора в настоящее врем характеры:

1. Широкое применение бот-сетей для выполнения различных задач.
2. Рост количества платежей, осуществляемых дистанционно, в том числе с применением карточных счетов и пластиковых карт как средств платежа.
3. Использование уязвимого программного обеспечения для осуществления дистанционных платежей в совокупности с недостаточной информированностью клиентов кредитных организаций о методах социальной инженерии.
4. Укрупнение и повышение организованности преступных сообществ и др.

Все это ведет к росту числа киберпреступлений и правонарушений в банковской сфере.

Субъектами компьютерных правонарушений (преступлений), направленных против безопасности банка выступают:

1. внутренние нарушители – работники банка, неосознанно либо злонамеренно нарушающие режим информационной безопасности;
2. внешние нарушители – лица, не связанные с банком трудовыми отношениями (в том числе стажеры и практиканты), из хулиганских или корыстных побуждений предпринимающие действия, способные нанести ущерб информационным ресурсам банка. Опасность нарушителя во многом определяется количеством и степенью важности доступных ему информационных ресурсов. Исходя из этого, наиболее рисковыми категориями следует считать менеджеров высшего и среднего звена, администраторов информационных ресурсов и лиц, работающих с большими объемами клиентской и финансовой информации.

1.3. Факторы усиления банковских рисков и необходимость управления ими в системе экономической безопасности кредитных организаций

Глобальный характер Интернета существенным образом увеличивает важность и вместе с тем сложность систем контроля за обеспечением безопасности, методов аутентификации клиентов, защиты данных и норм соблюдения клиентской тайны. Поэтому традиционные принципы управления рисками банковской деятельности должны учитывать сложные характерные особенности интернет-услуг. Банкам целесообразно использовать интегрированный подход к управлению риском, контроль которого должен стать неотъемлемой частью общей структуры управления рисками банка. Необходимо разрабатывать процедуры управления, соответствующие специфике интернет-услуг, общему профилю риска, операционной структуре и корпоративной культуре управления. Системы контроля и безопасности банка должны быть адекватными технологическим нововведениям.

Принципы управления рисками интернет-банкинга были впервые сформулированы Базельским комитетом по банковскому надзору в 2003 г. в документе, получившем соответствующее название «Принципы управления рисками для предоставления банковских услуг в электронной форме». Принципы управления рисками носят характер рекомендаций для кредитных организаций, осуществляющих интернет-банкинг, в области построения надлежащей системы безопасности применения интернет-технологий.

Принципы управления рисками интернет-банкинга классифицируются на три группы:

- для совета директоров и правления банка;
- для выбора и адекватного функционирования средств обеспечения безопасности;
- для повышения значимости управления правовым и репутационным рисками.

Группа принципов «Наблюдение со стороны совета и руководства» включает:

1. эффективное наблюдение со стороны руководства за деятельностью в рамках электронного банкинга;
2. организацию полноценного процесса контроля за безопасностью;
3. организацию полноценного и непрерывного процесса наблюдения за выполнением обязательств и управлением отношений банка с провайдерами услуг и прочими организациями, обеспечивающими поддержку выполнения операций интернет-банкинга.

Их суть заключается в том, что совет директоров и правление банка отвечают за разработку корпоративной стратегии банка и за организацию эффективного наблюдения за рисками. Предполагается, что они принимают четкие, обоснованные и формализованные стратегические решения относительно того, будет ли в будущем предоставлять банк услуги в рамках интернет-банкинга и, если да, то каким именно образом.

Совет директоров несет ответственность за политику управления рисками при осуществлении операций интернет-банкинга и за наличие контроля за безопасностью. В свою очередь, правление банка должно обеспечить надлежащее содержание этих процессов. Это означает введение должных правил авторизации и способов аутентификации, средств контроля логического и физического доступа, построение адекватной структуры безопасности для поддержания необходимых допусков и ограничений в части действий как внутренних, так и внешних пользователей, а также целостности трансакций, записей и информации.

Следующие семь принципов управления рисками Базельским комитетом сгруппированы в тематическую категорию «Средства обеспечения безопасности»:

1. аутентификация клиентов в операциях интернет-банкинга;

2. отсутствие отказов от проведения операций и возможность учета для трансакций, осуществляемых в рамках интернет-банкинга. Данный принцип управления рисками интернет-банкинга означает, что банкам следует использовать те методы аутентификации трансакций, которые способствуют невозможности отказа от операций (доказательного подтверждения операции) и обеспечивают возможность учета трансакций в рамках интернет-банкинга;

3. должные меры по обеспечению разделения обязанностей;

4. средства авторизации в системах электронного банкинга, базах данных и прикладных программах;

5. целостность данных в трансакциях электронного банкинга, записях и информаци;

6. организация формированияточных аудиторских записей длятрансакций, осуществляемых врамках электронного банкинга;

7. конфиденциальность банковской информации.

Меры, принимаемые для сохранения конфиденциальности, должны быть соразмерны значимости передаваемой и/или хранимой в базахданных информации.Такая категория представляет особую значимость вследствие повышенной сложности технологий, применяемых при операциях интернет-банкинга. Поэтому для банка актуальны вопросы аутентификации клиентов, целостности данных и трансакций, разделения обязанностей, использования средств управления авторизацией, поддержания аудиторских записей, а также конфиденциальности банковской информации.

Третья группа принципов управления рисками электронного банкинга включает рекомендации по управлению правовым и репутационным рисками. Их возможное обострение обусловлено различиями в законодательных актах стран, через которые производятся такого рода операции, в обеспечении конфиденциальности информации и правилах защиты клиента, действующих на территориях этих стран.Банки несут ответственность за обеспечение требований раскрытия информации, защиты клиентских данных и доступности деловых операций, а также требований, действующих при проведении операций через традиционные каналы

предоставления банковских услуг. В связи с этимБазельский комитет по банковскому надзору формулирует еще четыре принципа управления рисками, которым рекомендуется следовать банкам, оказывающим услуги интернет-банкинга.

Группа принципов «Усиление контроля правовых и репутацион-ных рисков» включает:

1. достоверность и полноту раскрытия информации для обслуживания в рамках электронного банкинга;

2. конфиденциальность информации о клиентах;

3. планирование производительности, непрерывности операций на случай непредвиденных обстоятельств для обеспечениядоступности систем и обслуживания в рамках интернет-банкинга;

4. планирование реагирования на непредвиденные события.

Рекомендации Базельского комитета по банковскому надзору были учтены и Банком России при разработке принципов управления рисками интернет-банкинга для российских банков, которые имеют рекомендательный характер.В рекомендациях Банка России по организации управления рисками, возникающими при осуществлении операций с применением систем интернет-банкинга, подчеркивается, что обеспечение эффективного управления ими является одной из целей внутреннего контроля. Согласно этим рекомендациям, оптимальная модель управления рисками в данной сфере должна включать следующие компоненты:

• квалифицированная политика информатизации, в том числе внедрения и развития технологий интернет-банкинга, проводимая руководством кредитной организации и обеспечивающая полнофункциональность системы – выполнение предполагающихся функций банковского обслуживания;

• тщательно продуманная архитектура автоматизированной банковской системы;

• адекватные меры по обеспечению информационной безопасности по всему информационному контуру интернет-банкинга, гарантирующие доступность и непрерывность банковского обслуживания, а также защиту информации от несанкционированного доступа, модификации либо уничто-жения;

• организация внутрибанковских процессов и процедур, со-ответствующих масштабу, технологической и технической сложности предоставляемого обслуживания клиентов посредством интернет-банкинга;

• отлаженная система внутреннего контроля, охватывающая всю технологическую цепочку интернет-банкинга и организационную структуру, начиная с руководства банка;

• эффективная система финансового мониторинга, оказывающая противодействие попыткам использования системы интернет-банкинга в противоправных целях;

• содержательное и всеобъемлющее организационное, информационное, методическое и консультационное обеспечение клиентов;

• оптимальные, с точки зрения минимизации сопутствующих рисков, взаимоотношения кредитной организации со своими провайдерами и вендорами.

Рекомендации Банка Россииучитывают и трансграничный характер услуг интернет-банкинга. Так, банкам рекомендуется выявлять возможные дополнительные источники рисков, возникающих в связи с нарушением законодательства зарубежных государств или территорий, а также дополнительные факторы рисков, относящихся к иным юрисдикциям, в том числе к соблюдению рекомендаций межправительственной организации «Группа разработки финансовым мер борьбы с отмыванием денег(ФАТФ)» (The Financial Action Task Force (FATF) 40 Recommendations).Соблюдение основного постулата организации риск-ориентированной системы контроля, а именно ее независимости от бизнес-процессов, будет способствовать минимизации рисков интернет-банкинга.

Особенности интернет-банкинга требуют применения более гибких и динамичных подходов надзора, способных постоянно модифицироваться с учетом быстро происходящих изменений в среде информационных технологий.

Таким образом, новые электронные технологии способствуют повышению уровня конкурентоспособности банков и одновременно выступают источником информационных угроз. В связи с этим возникает необходимость создания и развития системы безопасности банковской деятельности как совокупности специальных органов, служб, средств, методов, взаимосвязанных мероприятий правового характера, осуществляемых в целях защиты банка от внутренних и внешних угроз (реальных или потенциальных противоправных действий физических или юридических лиц).

Глава 2. Организация и управление безопасностью в финансово-кредитных организациях

2.1. Концептуальные основы функционирования системы экономической безопасности банков

Экономическая безопасность является главной составляющей национальной безопасности и трактуется как качественная характеристика экономической системы, которая определяет ее способность поддерживать нормальные условия работоспособности системы, развитие в рамках целей, поставленных перед ней, а в случаях возникновения различных угроз (внешних и внутренних) – способность системы противостоять им и восстанавливать свою работоспособность.

Выделяют несколько уровней экономической безопасности:

1) международная безопасность (глобальная, региональная);

2) национальная безопасность – государства, отрасли, региона, общества;

3) частная безопасность - предприятия, домашнего хозяйства или личности.

Финансовая безопасность является подсистемой экономической безопасности государства. Финансовая безопасность государства -это такое состояние финансовой, денежно-кредитной, валютной, банковской, бюджетной и налоговой систем, которое характеризуется сбалансированностью, устойчивостью к внутренним и внешнимнегативным влияниям, способностью обеспечить эффективное функционирование национальной экономической системы и ее рост.

Банковская система является важнейшей составляющей финансово-кредитной сферы государства. Именно состояние банковского сектора и определяет уровень финансово-кредитной безопасности, а, следовательно, во многом и уровень финансовой безопасности государства.

Понятие экономической безопасности банковской системы, как правило, определяется как состояние, при котором финансовая стабильность и репутация банковских учреждений не может быть утрачена из-за целенаправленных действий определенной группы лиц или организации как внутри, так и за границами государства, а также из-за негативных макроэкономических и политических факторов. Таким образом, экономическая безопасность банка - это состояние, при котором обеспечивается экономическое развитие и стабильность деятельности банка, гарантированная защита его финансовых и материальных ресурсов, способность адекватно и без существенных потерь реагировать на изменения внутренней и внешней ситуации.

Безопасность как система основана на противодействии существующим угрозам. Она характеризует состояние объекта в целом и обеспечивается для защиты от:

1. нарушения нормального хода воспроизводительного процесса;
2. преступного мира;

3. нарушений закона;
4. недобросовестной конкуренции;
5. некомпетентных и противоправных действий собственных сотрудников.

Угрозы финансовым ресурсам банка проявляются в виде:невозврата кредитных ссуд; мошенничества со счетами и вкладами; подложных платежных документов и пластиковых карт; хищения финансовых средств из касс и инкассаторских машин; резкого изменения экономической ситуации в стране (экономические кризисы); банкротства деловых партнеров банка.

Угрозы информационным ресурсам проявляются в виде:разглашения коммерческой тайны; утечки конфиденциальной информации через технические средства обеспечения производственной деятельности различного характера и исполнения; несанкционированного доступа к охраняемым сведениям со стороны конкурентных организаций и преступных формирований; уничтожение или порча носителей стратегически важной информации вследствие злонамеренных действий или несчастных случаев; ведение "информационной войны" против банка, наносящий существенный ущерб его деловой репутации.

Проблемы банковской сферы являются одновременно и проблемами финансовой безопасности государства. Стабильность и надежность банковской системы, усовершенствование банковского менеджмента и укрепление его стратегической составляющей могут обеспечить финансовую безопасность государства.В целом можно констатировать, что проблемам обеспечения финансовой безопасности банковских учреждений посвящено достаточно небольшое количество исследований. Этим, в частности, объясняется отсутствие единого общепринятого подхода к определению данного понятия. Также нужно отметить, что довольно большое количество авторов вообще игнорируют вопросы финансовой безопасности и, как правило, рассматривают либо экономическую безопасность банка, либо безопасность вообще.

Безопасность банковской системы необходимо рассматривать в двух аспектах:

1)с точки зрения финансовых последствий деятельности банков длястраны в целом и отдельных клиентов и контрагентов;

2) с точки зрения недопущения и предотвращения явных и потенциальных угроз финансовому состоянию всей банковской системы страны, Центрального Банка РФ и отдельных банковских учреждений.

Задача методического обеспечения банковской безопасности актуальна в двух плоскостях. Во-первых, ее решение позволяет сохранить финансовую стабильность конкретного банка, а во-вторых, решение задачи на более высоком государственном уровне призвано обезопасить экономику страны, сократить количество финансовых махинаций и уменьшить влияние теневого сектора экономики. Наряду с решением системных задач по управлению деятельностью банка возникает необходимость в разрешении ряда специфических вопросов, посвященных защите интересов банка от

различного рода противозаконных посягательств путем выполнения функций обеспечения банковской безопасности.

В более узком смысле обеспечение банковской безопасности можно рассматривать как системную деятельность по предотвращению или снижению тяжести последствий противоправных действий, затрагивающих интересы банка.

Поскольку кредитно-финансовые операции являются основным источником дохода современного банка, основная угроза банковской безопасности непосредственно вызвана противоправными действиями, совершаемыми в плоскости кредитно-финансовой деятельности.

В современных условиях развития информационных технологий большую опасность для банка представляют так называемые интеллектуальные мошенники, которые используют в своей деятельности достижения современных технологий. Поэтому на данном этапе развития современного общества следует отождествлять термин "банковская безопасность", прежде всего, именно с защитой от интеллектуальных атак.Таким образом, наряду с задачами по обеспечению основной кредитно-финансовой деятельности возникают особые задачи по защите интересов банка путем выполнения функций обеспечения банковской безопасности, направленных на упреждение или снижение тяжести последствий противоправных действий, которые нежелательны для банка.

Безопасность отдельного банка тесно связана с безопасностью банковской системы в целом. Они оказывают влияние друг на друга. С одной стороны, проблемы, возникшие в одном банке, способны вызвать "эффект домино" и привести к системному банковскому кризису, что объясняется самой природой банковской деятельности. С другой стороны, структурные проблемы банковского сектора подрывают доверие к любому отдельно взятому банку. Все это объясняет ту важную роль, которую играет обеспечение финансовой безопасности банков.

Таким образом, под экономической безопасностью банка в широком смысле следует понимать обеспечение наиболее эффективного использования всех ресурсов банка для предотвращения угроз и создания условий стабильного функционирования всех его подразделений. При этом к источникам угроз относятся нежелательные изменения финансовой конъюнктуры на рынках, технологические инновации, форс-мажорные обстоятельства.

Исходя из различных трактовок сущности безопасности в банковской деятельности, проанализированных нами выше, можем выделить следующие ключевые характеристики безопасности банков:

1. обеспечивает равновесное и устойчивое финансово-экономическое состояние банка;
2. способствует эффективной деятельности банка; позволяет на ранних стадиях определить проблемные места в деятельности банка;
3. нейтрализует кризисы и предупреждает банкротство.

При этом для обеспечения безопасности банка необходимо решить такие задачи, как:

1. обеспечение достаточной финансовой устойчивости и независимости банка;
2. поддержание технологической независимости и конкурентоспособности, формирование высокого технического и технологического потенциала;
3. оптимизация организационной структуры, постоянное усовершенствование выполнения функций менеджмента;
4. правовая защита всех видов деятельности банка;
5. создание защиты информационной среды банка, его коммерческой тайны;
6. формирование условий для безопасной работы сотрудников банка;
7. сохранение и эффективное использование финансовых, материальных и информационных ресурсов банка.

Основная цель безопасности банка состоит в непрерывном и устойчивом поддержании такого состояния, которое характеризуется сбалансированностью и устойчивостью к влиянию внешних и внутренних угроз.

Перед службами безопасности банков стоят следующие задачи:

1) идентификация рисков и связанных с ними потенциальных опасностей и угроз;
2) определение индикаторов безопасности банка;
3) внедрение системы диагностики и мониторинга состояния безопасности;
4) разработка мероприятий, направленных на обеспечение безопасности банка как в краткосрочном, так и в долгосрочном периоде;
5) контроль выполнения запланированных мероприятий;
6) анализ выполнения мероприятий, их оценка, корректировка;
7) идентификация опасностей и угроз банку и корректировка индикаторов в зависимости от изменения состояния внешней среды, целей и задач банка;
8) участие в уголовном и административном преследовании виновных в посягательстве на интересы банка в соответствии с законодательством РФ.

Функции службы безопасности банка:

• участвовать в плановых и внеплановых проверках деятельности подразделений банка методами оперативного, административного и финансового контроля;

• проводить внутренние (служебные) расследования по фактам причинения ущерба интересам банка;

• готовить материалы к направлению в правоохранительные органы для решения вопроса о возбуждении уголовного дела в соответствии с УПК РФ;

• собирать и представлять следственным органам документы (в том числе, материалы фото- и киносъемки, аудио- и видеозаписи и иные носители

информации) и предметы для приобщения их к уголовному делу в качестве доказательств;

• использовать в этих целях средства и методы криминалистики.

2.2. Правовые, организационные и технико-технологические основы обеспечения экономической безопасности банка

Правовые аспекты безопасности банка включают процесс реализации законодательства, регламентирующего полномочия, обязанности и ответственность органов государственной власти, Банка России, представительных и исполнительных органов банка, связанные с обеспечением его безопасного функционирования. Правовую основу банковской безопасности составляют: федеральные законы, указы Президента РФ, постановления Правительства РФ, ведомственные нормативные акты; нормативные акты Банка России в форме указаний, положений и инструкций, а также его рекомендации и официальные разъяснения по вопросам применения федеральных законов и иных нормативных правовых актов; локальные нормативные акты банка. Правовые основы безопасности деятельности банка определяют соответствующие положения Конституции Российской Федерации, Федеральный закон от 2 декабря 1990 г. N 395-I «О банках и банковской деятельности, Федеральный закон от 25 февраля 1999 г. N 40-ФЗ «О несостоятельности (банкротстве) кредитных организаций», Федеральный закон от 10 июля 2002 г. N 86-ФЗ «О Центральном банке Российской Федерации (Банке России)», Федеральный закон от 23 декабря 2003 г. N 177-ФЗ «О страховании вкладов физических лиц в банках Российской Федерации», Федеральный закон от 07.02.2011 N 3-ФЗ «О полиции», Федеральный закон от 25.12.2012 №267-ФЗ «О национальной платежной системе», Федеральный закон от 12 августа 1995 г. №144-ФЗ «Об оперативно-розыскной деятельности», Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных», Закон РФ от 11 марта 1992 г. 2487-I в ред. от 3.07.2016 «О частной детективной и охранной деятельности», Указ Президента Российской Федерации от 31 декабря 2015 года N 683 "О Стратегии национальной безопасности Российской Федерации", Доктрина информационной безопасности Российской Федерации (утв. Президентом Российской Федерации 9 сентября 2000 г. № Пр – 1895), Положение ЦБ РФ от 16.12.2003 г. № 242-П «Порядок обеспечения и защиты банковской информации», Стандарт Банка России СТО БР ИББС -1.0 – 2010 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» и др.

Локальные нормативные акты банка в сфере безопасности включают:

1. Акты общего характера, регламентирующие технологию осуществления банковских операций, распределяющие функции и полномочия между подразделениями и сотрудниками банка, определяющие процедуру принятия решений, регулирующие деятельность службы внутреннего контроля и службы безопасности.

2. Акты по вопросам обеспечения безопасности: объектовый режим безопасности банка; режим защиты сведений ограниченного доступа (перечень информации, составляющей коммерческую (банковскую) тайну, положение об организации защиты информации ограниченного доступа и компьютерной информации, инструкция о распределении доступа пользователей к информации ограниченного доступа, к осуществлению операций в автоматизированной банковской системе, а также к базам данных в компьютерных системах); порядок организации и функционирования службы безопасности (положение о службе безопасности, инструкция о проведении внутренних расследований по фактам нарушений порядка обеспечения безопасности банка).

Организационные и технико-технологические основы обеспечения экономической безопасности банка формируются службой безопасности банка.

Основные направления деятельности службы безопасности банка включают:

• Защиту от преступлений, посягающих на собственность банка: хищения денежных средств при совершении кредитных и расчетно-кассовых операций; мошенничество в сфере корпоративного и потребительского кредитования; хищения денежных средств с использованием платежных поручений, требований, чеков, векселей и аккредитивов.

• Защиту от преступлений, посягающих на порядок функционирования банка: злоупотребление полномочиями, коммерческий подкуп, посягательства на сведения банка, составляющие банковскую, коммерческую и иную тайну, посягательства в сфере компьютерного обеспечения деятельности банка, посягательства на кадровое обеспечение банка, посягательства на нематериальные активы банка.

• Организацию противодействия отмыванию преступных доходов и финансированию терроризма.

Организационные методы включают в себя специальные методы осуществления управленческой, финансовой, коммерческой, кадровой и иной функциональной деятельности банка, имеющие целью предупредить причинение ущерба как в результате умышленных и неосторожных противоправных действий, так и вследствие ошибки. В рамках этих методов формируются специальные подразделения контроля и защиты интересов банка; проводится совершенствование структуры банка; принимаются решения об ограничении полномочий должностных лиц в отношении объема и состава банковских операций, в распоряжении денежными средствами и иным имуществом банка; определяются полномочия по осуществлению расчетно-кассовых операций и пассивно-активных операций; устанавливается ответственность за обеспечение процедур выполнения отдельных операций и порядка хранения ценностей; организуется система контроля, отчетности и работы с персоналом.

Функциональные методы обеспечения безопасности банка включают:

1. Технологические методы (технологические решения, закрепленные распорядительными документами) основываются на рекомендациях Банка России, разработках подразделений банка, рекомендациях экспертов.

2. Методы обеспечения конфиденциальности информации: закрытие свободного доступа к информации, отнесенной к охраняемой законом тайне; защита информации в каналах связи и средствах вычислительной техники; предупреждение и пресечение попыток неправомерного завладения сведениями и документами.

3. Методы административного контроля: проверка правильного функционирования системы подбора и расстановки кадров, наличия и исполнения должностных инструкций сотрудников.

4. Методы финансового контроля обеспечивают проведение операций в строгом соответствии с принятой и закрепленной документами политикой банка применительно к разным видам финансовых операций и услуг и их адекватного отражения в учете и отчетности.

Криминалистические методы обеспечения безопасности банка включают:

1. Технико-криминалистические средства, которые используются для предупреждения преступлений и административных правонарушений. Их применение: а) затрудняет или исключает возможность совершения посягательства; б) создает благоприятные условия для формирования и сбора доказательственной информации.

2. Приемы криминалистической тактики, которые используются для построения и контроля функционирования системы безопасности банка. Применяются: построение версий о видах и характере потенциальных угроз и способах защиты от них; планирование мероприятий по выявлению причин и условий, способствующих совершению посягательств; «следственный» эксперимент по проверке надежности мер защиты интересов банка; экспертное исследование материалов.

3. Рекомендации криминалистической методики используются для создания методик предотвращения, пресечения и внутреннего расследования отдельных видов противоправных посягательств.

Криминалистическая характеристика противоправного посягательства – это система описания присущих тому или иному виду посягательства особенностей, позволяющих обеспечить эффективное предупреждение, пресечение и расследование этих посягательств и обусловливающих применение соответствующих методов, приемов и средств.

Элементы криминалистической характеристики:

– предмет противоправного посягательства;

– типичные способы совершения и сокрытия посягательства;

– обстоятельства подготовки и совершения посягательства (время, место, условия, участники и т.п.);

– характерные механизмы следообразования;

– типология личности виновного и потерпевшего.

Основу эффективности деятельности по информационному обеспечению безопасности банка составляет процесс поиска, получения, накопления, анализа и использования необходимой информации. Качество информационного процесса является основным критерием оценки профессионализма службы безопасности банка и ее отдельных работников. Добываемая информация должна быть четко «привязана» к конкретным объектам защиты и предполагаемым видам противоправных посягательств, обеспечивать возможность применения на ее основе норм правовой защиты и соответствовать установленным законодательством условиям ее собирания и использования. В современных условиях эффективными являются специальные аналитические технологии для предупреждения и расследования противоправных посягательств на безопасность банка, использующие широкий спектр баз данных, включая Интернет.

Таким образом, безопасность банка является важной составляющей национальной безопасности и представляет собой такое состояние банковского учреждения, которое характеризуется сбалансированностью и устойчивостью к влиянию внешних и внутренних угроз, его способностью достигать поставленные цели и генерировать достаточный объем финансовых ресурсов для обеспечения устойчивого развития.Недостаточное внимание обеспечению безопасности банков может привести к проблемам в деятельности финансовых учреждений.

2.3. Защита от преступлений, посягающих на порядок функционирования банка

Информационная безопасность не является самоцелью, ее обеспечение необходимо для снижения рисков и экономических потерь, связанных со всевозможными угрозами имеющимся информационным ресурсам банка. С этой целью необходимо поддерживать главные свойства информации, а именно:

1. доступность – свойство, характеризующееся способностью своевременного беспрепятственного доступа к информации субъектов, имеющих на это надлежащие полномочия;

2. конфиденциальность – свойство, указывающее на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации, и обеспечиваемое способностью системы (среды) сохранять указанную информацию в тайне от субъектов, не имеющих полномочий на доступ к ней;

3. целостность – свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию).

В целях обеспечения достаточно надежной системы информационной безопасности необходима постоянная регулировка ее параметров, адаптация для отражения новых опасностей, исходящих из внешней и внутренней среды. Не должно существовать каких-либо препятствий при внесении изменений в стандарты, процедуры или политику информационной

безопасности банка (далее – Политика) по мере возникновения такой необходимости.

Выделяются следующие этапы цикла управления информационной безопасностью (модель PDCA: PlanDo-Check-Act):

Plan – планирование (разработка) – анализ рисков, определение Политики, целей, задач, процессов, процедур, программно-аппаратных средств, относящихся к управлению рисками и совершенствованию информационной безопасности для получения результатов в соответствии с общей стратегией и целями банка;

Do – реализация (внедрение и эксплуатация) – внедрение и эксплуатация Политики, механизмов контроля, процессов, процедур, программно- аппаратных средств;

Check – проверка (мониторинг и анализ) – оценка и там, где это применимо, измерение характеристик исполнения процессов в соответствии с Политикой, целями и практическим опытом, анализ изменения внешних и внутренних факторов, влияющих на защищенность информационных ресурсов, предоставление отчетов руководству для анализа;

Act – корректировка (сопровождение и совершенствование) – принятие корректирующих и превентивных мер, основанных на результатах внутренних и внешних проверок состояния информационной безопасности, требований со стороны руководства, иных факторов, в целях обеспечения непрерывного совершенствования системы информационной безопасности.

Построение системы обеспечения информационной безопасности Банка и ее функционирование должны осуществляться в соответствии со следующими основными принципами:

1. законность – любые действия, предпринимаемые для обеспечения информационной безопасности, осуществляются на основе действующего законодательства, с применением всех дозволенных законодательством методов обнаружения, предупреждения, локализации и пресечения негативных воздействий на объекты защиты информации банка;

2. ориентированность на бизнес – информационная безопасность рассматривается как процесс поддержки основной деятельности. Любые меры по обеспечению информационной безопасности не должны повлечь за собой серьезных препятствий деятельности банка;

3. непрерывность – применение средств управления системами защиты информации, реализация любых мероприятий по обеспечению информационной защиты банка должны осуществляться без прерывания или остановки текущих бизнес-процессов банка;

4. комплексность – обеспечение безопасности информационных ресурсов в течение всего их жизненного цикла, на всех технологических этапах их использования и во всех режимах функционирования;

5. обоснованность и экономическая целесообразность – используемые возможности и средства защиты должны быть реализованы на соответствующем уровне развития науки и техники, обоснованы с точки зрения заданного уровня безопасности и должны соответствовать

предъявляемым требованиям и нормам. Во всех случаях стоимость мер и систем информационной безопасности должна быть меньше размера возможного ущерба от любых видов риска;

6. приоритетность – категорирование (ранжирование) всех информационных ресурсов Банка по степени важности при оценке реальных, а также потенциальных угроз информационной безопасности;

7. необходимое знание и наименьший уровень привилегий – пользователь получает минимальный уровень привилегий и доступ только к тем данным, которые являются необходимыми для выполнения им деятельности в рамках своих полномочий;

8. специализация – эксплуатация технических средств и реализация мер информационной безопасности должны осуществляться профессионально подготовленными специалистами банка;

9. информированность и персональная ответственность – руководители всех уровней и исполнители должны быть осведомлены обо всех требованиях информационной безопасности и несут персональную ответственность за выполнение этих требований и соблюдение установленных мер информационной безопасности;

10. взаимодействие и координация – меры информационной безопасности осуществляются на основе взаимосвязи соответствующих структурных подразделений банка, координации их усилий для достижения поставленных целей, а также установления необходимых связей с внешними организациями, профессиональными ассоциациями и сообществами, государственными органами, юридическими и физическими лицами;

11.подтверждаемость – важная документация и все записи – документы, подтверждающие исполнение требований по информационной безопасности и эффективность системы ее организации, должны создаваться и храниться с возможностью оперативного доступа и восстановления.

Основными объектами обеспечения информационной безопасности в банке признаются следующие элементы:

1. информационные ресурсы, содержащие сведения, отнесенные в соответствии с действующим законодательством и внутренними нормативными документами банка к банковской тайне, коммерческой тайне банка, любая иная информация, необходимая для обеспечения нормального функционирования банка (далее – защищаемая информация);

2. средства и системы информатизации (средства вычислительной техники, информационно-вычислительные комплексы, сети, системы), на которых производится обработка, передача и хранение защищаемой информации;

3. программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение) автоматизированной системы банка, с помощью которых производится обработка защищаемой информации;

4. процессы банка, связанные с управлением и использованием информационных ресурсов;

5. помещения, в которых расположены средства обработки защищаемой информации;

6. рабочие помещения и кабинеты работников банка, помещения банка, предназначенные для ведения закрытых переговоров и совещаний;

7. персонал банка, имеющий доступ к защищаемой информации;

8. технические средства и системы, обрабатывающие открытую информацию, но размещенные в помещениях, в которых обрабатывается защищаемая информация.

Подлежащая защите информация может:

1. размещаться на бумажных носителях;

2. существовать в электронном виде (обрабатываться, передаваться и храниться средствами вычислительной техники, записываться и воспроизводиться с помощью технических средств);

3. передаваться по телефону, телефаксу, телексу и т.п. в виде электрических сигналов;

4. присутствовать в виде акустических и вибросигналов в воздушной среде и ограждающих конструкциях во время совещаний и переговоров.

Основными мерами по обеспечению информационной безопасности банка являются:

1. административно-правовые и организационные меры;

2. меры физической безопасности;

3. программно-технические меры.

Административно-правовые и организационные меры включают (но не ограничены ими):

1. контроль исполнения требований законодательства РФ и внутренних документов;

2. разработку, внедрение и контроль исполнения правил, методик и инструкций, поддерживающих Политику безопасности банка;

3. контроль соответствия бизнес-процессов требованиям Политики;

4. информирование и обучение работников банка работе с информационными системами и требованиям информационной безопасности;

5. реагирование на инциденты, локализацию и минимизацию последствий;

6. анализ новых рисков информационной безопасности;

7. отслеживание и улучшение морально-делового климата в коллективе;

8. определение действий при возникновении чрезвычайных ситуаций;

9. проведение профилактических мер при приеме на работу и увольнении работников банка.

Меры физической безопасности включают:

1. организацию пропускного и внутриобъектового режимов;

2. построение периметра безопасности защищаемых объектов;

3. организацию круглосуточной охраны охраняемых объектов, в том числе с использованием технических средств безопасности;

4. организацию противопожарной безопасности охраняемых объектов;

5. контроль доступа работников банка в помещения ограниченного доступа. Программно-технические меры включают (но не ограничены ими):

6. использование лицензионного программного обеспечения и сертифицированных средств защиты информации;

7. использование средств защиты периметра (firewall, IPS и т.п.);

8. применение комплексной антивирусной защиты;

9. использование средств информационной безопасности, встроенных в информационные системы;

10. обеспечение регулярного резервного копирования информации;

11. контроль за правами и действиями пользователей, в первую очередь, привилегированных;

12. применение систем криптографической защиты информации;

13 обеспечение безотказной работы аппаратных средств;

14. мониторинг состояния критичных элементов информационной системы.

Таким образом, в качестве задач, решаемых службой безопасности банка, выступают: защита прав банка, его структурных подразделений и сотрудников; сохранение и эффективное использование финансовых, материальных и информационных ресурсов; своевременное выявление и устранение угроз, причин и условий, способствующих нанесению ущерба, нарушению нормального функционирования и развития банка; отнесение информации к категории ограниченного доступа к различным уровням уязвимости;создание механизма и условий оперативного реагирования на угрозы безопасности и проявления негативных тенденций функционирования; эффективное пресечение посягательств на ресурсы и угроз персоналу на основе комплексного подхода к безопасности; создание условий для максимально возможного возмещения и локализации наносимого ущерба неправомерными действиями для ослабления негативных влияний последствий нарушения безопасности на достижение стратегических целей.

Глава 3 Структура и содержание методики расследования преступлений, совершаемых с использованием банковских технологий в современной экономике

3.1. Композиционная функциональная модель противоправных действий в отношении субъектов, управляющих своими активами через системы дистанционного банковского обслуживания

В Российской Федерации существуют различные инициативы по противодействию совершению несанкционированных операций через системы дистанционного банковского обслуживания.

1. По инициативе Банка России была начата деятельность по разработке национального стандарта финансовых операций на основе стандарта ISO 20022, который является принятой в международной практике методологией описания процедур осуществления финансовых операций и форматов финансовых сообщений. В декабре 2010 года в соответствии с приказом Федерального агентства по техническому регулированию и метрологии на добровольной основе создан заинтересованными организациями Технический комитет по стандартизации № 122 «Стандарты финансовых операций» (далее – ТК № 122)[1] в целях организации и проведения работ по национальной, межгосударственной и международной стандартизации финансовых операций. В 2011 году была утверждена организационная структура и основные направления его деятельности. В настоящее время ТК № 122 состоит из пяти подкомитетов: ПК № 1 «Безопасность финансовых (банковских) операций», ПК № 2 «Технологии операций на финансовых рынках», ПК № 3 «Технологии основных финансовых (банковских) операций», ПК № 4 «Процедуры и технологии расчетов с использованием банковских карт и иных инструментов розничных платежей» (далее – ПК № 4) и ПК № 5 «Мобильные платежи» (далее – ПК № 5). Помимо Банка России, в ТК № 122 участвуют более 50 организаций, представляющих органы государственной власти, кредитные организации и их ассоциации, инфраструктурные организации финансовых рынков и иные заинтересованные стороны, в том числе представители рынка розничных платежных услуг. К приоритетному направлению деятельности ПК № 4 и ПК № 5 можно отнести выработку национального стандарта по предотвращению совершения несанкционированных операций с использованием электронных средств платежа (далее – ЭСП), включая разработку подходов к организации единой базы данных по несанкционированным операциям, а также соответствующих общероссийских стандартов сбора, обработки, хранения и обмена информацией о совершенных несанкционированных операциях. Кроме того, целью деятельности ПК № 4 и ПК № 5 является повышение уровня раскрываемости случаев несанкционированных операций в сфере розничных услуг и разработка соответствующих рекомендаций кредитным организациям и пр.

[1]URL: www.tk122.ru 13

2. В рамках «Ассоциации Российских членов Европей» (АРЧЕ), «Ассоциации российских банков» (АРБ) и «Сообщества ABISS» в 2009 году реализован проект по созданию межбанковского информационного ресурса, обеспечивающего закрытый канал обмена данными по инцидентам с платежными картами и информационной безопасностью (условное название «горячая линия») и позволяющего банкам: быстро и с большой точностью выявлять места компрометации карт; своевременно блокировать карты, подвергшиеся компрометации; получать дополнительную, достоверную информацию при рассмотрении заявлений клиентов; выявлять новые схемы совершения несанкционированных операций и вырабатывать меры противодействия; обмениваться практическим опытом в области противодействия мошенникам и статистической информацией; вести профессиональный диалог с правоохранительными органами и информировать банковское сообщество о соответствующих судебных решениях и пр. В настоящее время сертифицированными пользователями «горячей линии» являются около 450 представителей более 150 крупнейших банков России, Украины, Белоруссии и Казахстана.

Международная и российская практика организации и проведения мероприятий, направленных на предотвращение несанкционированных операций в сфере розничных платежных услуг в различных ее сегментах, свидетельствует о необходимости: создания информационной системы сбора и предоставления участниками национальной платежной системы сведений о фактах хищения денежных средств; создания механизма мониторинга и обмена информацией между заинтересованными участниками рынка розничных платежных услуг о случаях совершения несанкционированных операций с использованием платежных карт; предоставления всеми участниками рынка розничных платежных услуг информации о несанкционированных операциях с платежными картами; разработки требований к обеспечению безопасного предоставления кредитными организациями ДБО, в том числе с использованием инновационных технологий, в сфере розничных платежных услуг; разработки рекомендаций по взаимодействию операторов по переводу денежных средств с целью блокировки операций в случае выявления фактов хищения при переводах денежных средств с использованием электронных средств платежа (ЭСП); комплексного анализа и подготовки экспертных оценок эффективности механизмов противодействия совершению несанкционированных операций; разработки проектов и учебных программ по повышению финансовой грамотности населения по вопросам безопасности использования ЭСП, а также проведения работы по разъяснению позиции Банка России по указанным вопросам и доведения до участников рынка розничных платежных услуг и широкой общественности соответствующей информации.

Для эффективного предотвращения мошеннических операций необходимо учитывать российскую специфику:

- низкая техническая подготовка клиента, граничащая с технической и финансовой безграмотностью;

- правовой нигилизм и халатность клиентов.

По имеющимся оценкам, из общего числа фактов, мошенничество в сфере электронных платежей возможно из-за потери данных. Утечка информации из финансово-кредитной сферы происходит с помощью подкупа, шантажа, переманивания служащих в 43 % случаях, копирования программного продукта – 24 %, проникновения в компьютер – 18 %, кражи документации – 10 %, подслушивания телефонных переговоров – 5 %[2].

Эффективность обеспечения безопасности по отношению к ДБО может быть повышена путем технологических и организационных методов.К первым относятся совершенствование выпуска карт и повышение уровня безопасности использования банкоматов.Учитывая это, банкам необходимо прилагать наибольшие усилия в противодействии использованию мошенниками банкоматов в качестве технических средств получения/ дублирования секретной информации (ее носителя).

Для совершенствования информационных систем требуется выполнение следующих требований:

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

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

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

4. Оповещение операторов системы о фактах мошенничества для принятия соответствующих мер (SMS и E-mailинформирование, генерация оповещений)[3].

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

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

[2]Выборнов А. Устранение уязвимостей // BIS journal. 2014. № 4.

[3]Смольянинова Е.Н., Фурманов Д.В. Проблемы безопасности расчетов при использовании пластиковых карт //Актуальные вопросы экономических наук. 2012. № 24 (2). С. 46–50.

мошеннические действия, формирование доказательной базы.

Итак, противодействие мошенничеству в области ДБО - это реализация системы противодействия как внешнему, так и внутреннему мошенничеству, так называемые решения антифрод, работающие в реальном времени. Другими словами, это комплекс организационных и технических мер, обеспечивающих дополнительную защиту автоматизированных банковских систем и систем дистанционного банковского обслуживания. Такие системы содержат наборы правил, позволяющие с высокой долей вероятности обнаружить транзакции, сформированные мошенниками. Это, например, «черные» и «белые» списки. В «черные» списки попадают те получатели платежей, которые уже были уличены в участии в мошеннических схемах, в «белые» – те, которым клиент платил и не обжаловал этот платеж[4]. Возможно также создание профиля пользователя, учитывающего различные параметры выполняемых операций: запрашиваемую сумму, дату и время, географию – и определяющего уровень риск для каждой транзакции по этому профилю. Транзакции с высоким уровнем рисков можно запрещать или ограничивать по сумме, или требовать дополнительной авторизация для выполнения операции[5].

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

3.2. Методы диагностирования мошеннических сделок в практике управления банковскими рисками

Декомпозиция задачи обеспечения банковской безопасности с учетом использования банком интернет-технологий позволяет уточнить состав функций, выполняемых структурными подразделениями кредитной организации. При этом представляется необходимым возложить функции внутреннего финансового мониторинга на специализированный отдел, который должен обеспечивать противодействие легализации (отмыванию) доходов, полученных преступным путем. Методическая функция предусматривает разработку методических документов, обобщение и распространение опыта проведения работы по противодействию легализации доходов, полученных преступным путем, обучение работников банка вопросам финансового мониторинга в рамках выполнения ими служебных

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

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

обязанностей и др. Контрольные функции включают проведение проверок подразделений банка и его филиалов по вопросам соблюдения правил проведения внутреннего финансового мониторинга в банке. Практические функции предусматривают реализацию программ внутреннего контроля.

Работники отдела анализируют и обобщают информацию, которая поступает из информационных подсистем. К числу признаков, вызывающих подозрение о сомнительном характере финансовых операций, относятся:

1. Признаки, не свойственные имущественно-денежным отношениям;
2. Признаки наличия схем легализации.

Как правило, выявление признаков первой группы, не свойственных имущественно-денежным операциям, возможно на уровне организации, осуществляющей указанные операции. Обнаружение признаков наличия схемы легализации возможно, как правило, только после осуществления цепочки связанных операций, реализующих указанную схему с учетом информации, доступной уполномоченному органу финансовой разведки. Признаки нетипичности операции указывают на потенциальную возможность применения имущественно-денежной операции в схемах по легализации незаконных доходов, но не указывают наличия самой схемы. Нетипичность операции устанавливают, исходя из комбинации параметров ее признакового пространства, к которым могут относиться:

1. Вид основной деятельности компании, участвующей в операции.
2. Характер самой операции.
3. Географический фактор операции.
4. Особенности организационно-правовой формы участников.
5. События, предшествующие непосредственно операции (изменение состава собственников компании, получение компанией крупного кредита).
6. История движения денежных средств и др.

Примерами нетипичных финансовых операций могут выступать:

1. Экономически необоснованные операции (технологически или экономически неоправданные покупки, продажи по заниженным ценам и др.).
2. Операции с участием излишне крупных сумм или с нарушением привычного для деятельности организации ритма инкассации денежных средств и др.

Отнесение операции к типичным или нетипичным может основываться на историческом анализе для контрагентов операции и(или) сопоставительном – по виду деятельности, по виду операции.

Информационными технологиями, которые позволяют реализовать поиск нетипичных операций, выступают: кластерный анализ; анализ временных рядов, регрессионное моделирование. В первом случае кластеры с незначительным числом объектов, а также граничные точки кластеров интерпретируются как «нетипичности» для рассматриваемого множества операций. Во втором случае роль нетипичности выполняют выбросы

значений моделируемой переменной, например, сумма операций или частотные характеристики операций за определенный период.

Для больших объемов данных используются современные аналитические методы – деревья решений, нейронные сети, которые заключаются в построении оценочных алгоритмов, обучающихся на исторической информации.

Признаки наличия схемы легализации определяются на цепочках взаимосвязанных операций. Для цепочек операций, реализующих схему легализации, характерны следующие признаки:

1. Закрепление за участниками схемы легализации определенных ролей.
2. Наличие определенной последовательности исполнения операции (сценария).
3. Синхронизация операций по времени (логистика его исполнения).
4. Согласованность суммы операции.

В связи с наличиеммножества вариантов схем легализации доходов их обнаружение осуществляется с использованием метода прямого перебора с существенно большим количеством возможных схем легализации. Информационные технологии, используемые в ходе управляемого вычислительно-поискового запроса, относятся к методам добывания данных, включающих методы анализа ассоциаций, выявления последовательности событий, анализа связей, поиска аналогий с использованием «правдоподобных рассуждений» и др.

При выявлении финансовых операций, которые имеют признаки легализации доходов, полученных преступным путем, работники отдела финансового мониторинга проводят их регистрацию и готовят сообщения в государственные органы финансового мониторинга об их источниках и содержании. При выявлении финансовых операций, которые имеют признаки необходимости внутреннего финансового мониторинга, изучается их суть и цель, а также готовятся материалы для принятия решений ответственными лицами.

Отдел технических средств защиты банка решает следующие задачи:

1. Разработка основных направлений использования в банке технических и программных средств и способов защиты электронной банковской информации;
2. Генерация, учет и сохранение ключей и документов в подразделениях и филиалах банка;
3. Проведение анализа и организация работы по выявлению возможных каналов утечки информации с помощью технических средств защиты.

Защитные меры реализуются на законодательном (соответствие управленческих решений, технологий и программно-аппаратных средств нормам законодательства), административном (разработка и реализация Политики безопасности) и программно-техническом (совокупность

взаимосвязанных мер по управлению системой объединенных серверов безопасности) уровнях.

Отдел защиты технологий платежных карточек банка обеспечивает выполнение требований национальной и международных платежных систем повопросам выпуска, обслуживания платежных карт работниками банка, а также принимает участие в планировании и реализации программ обеспечения безопасности при производстве, транспортировании, хранении, персонализации и обслуживании платежных карт. Отдел выявляет противоправные действия сотрудников банка с использованием пластиковых карт, которые принимают форму:

1. Неправомерного увеличения кредитного лимита на конкретную карточку и последующее хищение средств;
2. установление в авторизированной системе специального статуса счета, который разрешает в определенных границах использовать деньги с карточки (разновидность кредитного лимита);
3. Несанкционированный выпуск новых пластиковых карт;
4. Выпуск равноценной карточки-двойника;
5. Несанкционированное пополнение счета карточки.

Система контроля над операциями с пластиковыми карточками реализуется в двух направлениях: внешнем и внутреннем. В первом направлении отслеживаются операции с пластиковыми карточками вне банка, что предусматривает ведение и публикацию специального банковского реестра с номерами блокированных пластиковых карточек. Задача второго направления – контроль над расчетами непосредственно в подразделениях, которые осуществляют выпуск карточек и расчеты с их пользователями. С целью реализации системы контроля работники отдела по указаниям руководства банка проводят служебные расследования в случаях мошенничества и злоупотреблений клиентов банка с использованием платежных карточек. При этом проводятся мероприятия по установлению местонахождения лиц, которые имеют овердрафтные задолженности при использовании платежных карточек и оказывают содействие в возвращении денежных средств банка.

Таким образом, банковская безопасность обеспечивается с использованием совокупности мер, включающих меры по предупреждению физических угроз и угроз в сфере информационных технологий.

3.3. Методика расследования преступлений, связанных с криминальным использованием пластиковых платежных средств и направления ее совершенствования

Одним из самых распространенных видов высокотехнологичного мошенничества является мошенничество с использованием платежных карт, что обусловлено их обширным распространением среди населения, низкой культурой использования; сравнительной легкостью получения данных карты жертвы, сложность идентификации мошенника и сбора доказательств его вины. Это предопределило выделение мошенничества с использованием

платежных карт в качестве разновидности мошенничества, что повлекло за собой включение в Уголовный кодекс Российской Федерации отдельной статьи, предусматривающей уголовную ответственность за совершение данного деяния (ст. 159.3 УК РФ).

Введение в Уголовный кодекс РФ статьи, предусматривающей ответственность за совершение мошенничества с использованием платежных карт, - это абсолютная новелла для российского права, несмотря на то, что в работах ряда исследователей киберпреступлений неоднократно указывалось на необходимость введения такого состава в российское уголовное право[6]. Подобные составы давно включены в уголовное законодательство многих зарубежных государств.

Согласно статистике Центрального банка РФ, общее количество эмитированных банковских карт за последние 10 лет возросло более чем в 2 раза.Так, если в 2008 г. количество банковских карт составляло 118 101тыс.ед., то уже по состоянию на 1 января 2015 г. их количество возросло до 240 521тыс.ед., ежегодно их количество возрастало на 7%[7]. Как правило, платежная карта выпускается банком для клиентов с целью доступа к своим денежным средствам и осуществления иных услуг. Подобные карты привязываются напрямую к собственному расчетному счету клиента или к кредитному счету, связанному с использованием в определенном количестве денежных средств банка, на условиях возвратности. В соответствии с Положением Центрального Банка от 24.12.2004 № 266 «Об эмиссии платежных карт и об операциях, совершаемых с их использованием» (далее положение ЦБ от 24.12.2004 № 266), кредитная организация осуществляет эмиссию расчетных (дебетовых) карт, кредитных карт и предоплаченных карт для физических лиц, юридических лиц и индивидуальных предпринимателей. Расчетная небанковская кредитная организация осуществляет эмиссию расчетных (дебетовых) карт для юридических лиц, индивидуальных предпринимателей, предоплаченных карт - для физических лиц, юридических лиц, индивидуальных предпринимателей[8].

Платежная небанковская кредитная организация осуществляет эмиссию предоплаченных карт для физических лиц, юридических лиц, индивидуальных предпринимателей. В зависимости от условий предоставления банком-эмитентом платежной карты клиенту с помощью этого инструмента возможно: получать денежные средства как напрямую в кредитных организациях, так и через программно-технический комплекс, предназначенный для автоматизированной выдачи и приема наличных

---

[6]См., например: Добрынин Ю. Классификация преступлений, совершаемых в сфере компьютерной информации. URL: http://www.russianlaw.net/law/computer_crime/a158/ (дата обращения: 20.07.2017).

[7]По данным Центрального Банка Российской Федерации [Электронный ресурс] URL: https://www.cbr.ru/.(дата обращения:20.07.2017.

[8]См.: Положение об эмиссии платежных карт и об операциях, совершаемых с их использованием: утв. Банком России 24.12.2004 № 266-П: ред. от 14.01.2015 // Вестник Банка России. 30.03.2005.№ 17.

денежных средств (банкомат, банковский автомат); либо использовать ее в качестве средства платежа, в том числе и через Интернет. Платежная карта в диспозиции ст. 159.3 УК РФ выступает в качестве родового понятия, объединяющего конкретные виды карт: кредитные, расчетные и иные карты. Кредитная карта предполагает, что банк-эмитент обязуется предоставлять денежные средства клиенту в зависимости от установленных тарифов в течение определенного срока и в определенных пределах. В соответствии с положением ЦБ от 24.12.2004 № 266 предусматриваются два порядка осуществление операций с использованием кредитных карт. В первом случае денежные средства поступают непосредственно на банковский счет клиента, а во втором случае они предоставляются клиенту с использованием банковского счета. В случае, если клиент является нерезидентом РФ, то денежные средства ему предоставляются в валюте, в остальных случаях физическим лицам предусматривается выдача в валюте РФ[9].

Важным условием является обязательность возврата клиентом денежных средств кредитной организации. Расчетная карта (дебетовая карта) является средством платежа, привязанным напрямую к счету клиента, и обеспечивает ему беспрепятственный доступ к своим денежным средствам (аналог дорожного чека). В качестве иных карт может выступать, например, предоплаченная платежная карта. Последняя является электронным средством платежа и используется для осуществления перевода электронных денежных средств, возврата остатка электронных денежных средств в пределах суммы предварительно предоставленных держателем денежных средств кредитной организации-эмитенту в соответствии с требованиями ФЗ от 27.06.2011 № 161 «О национальной платежной системе»[10] (далее ФЗ от 27.06.2011 № 161) (телефонные карты, электронный проездной и т.д.).

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

[9]Положение об эмиссии платежных карт и об операциях, совершаемых с их использованием: утв. Банком России 24.12.2004 № 266-П: ред. от 14.01.2015 // Вестник Банка России. 30.03.2005.№ 17.

[10]Положение об эмиссии платежных карт и об операциях, совершаемых с их использованием: утв. Банком России 24.12.2004 № 266-П: ред. от 14.01.2015 // Вестник Банка России. 30.03.2005.№ 17.

принимаются данные карты (Visa, MasterCard, DinersClub, AmericanExpress, JCB и ChinaUnionpay).

В настоящий момент в РФ на основании ФЗ от 27.06.2011 № 161 создана российская национальная система платежных карт (НСПК). В качестве субъектов, участвующих в этих отношениях, можно выделить держателя карты, собственника карты и владельца. Держателем карты является лицо, на чье имя она непосредственно выпущена, т.е. тот, кто является субъектом права пользования данной картой. Денежные средства на счете карты принадлежат непосредственно держателю, и банк не имеет на них никаких прав. Основанием для приостановления операций по счету может являться наличие решения суда. В качестве собственника выступает банк-эмитент. При этом банк-эмитент не пользуется полномочиями собственника через признанную классическую триаду, установленную в ст. 209 ГК РФ. Эти права лишь распространяются на саму карту как физический предмет, но не в отношении ее содержимого, т.е. того счета, к которому она привязана, если это только не денежные средства самого банка или иной кредитной организации. В ряде случаев признано необходимым выделять владельца карты, т.е. то лицо, в чьем владении находится карта. При этом в качестве такого владельца может выступать и не держатель карты. При выпуске платежной карты и в случаях ее использования кредитная организация обязана идентифицировать ее держателя в соответствии с ФЗ от 07.08.2001 № 115 «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма». Следовательно, каждая карта подлежит процедуре персонализации, в соответствии с которой ей присваивается определенный номер, имя держателя, срок действия. При совершении каких-либо операций с картой денежные средства могут поступать как с одного счета, к которому привязана карта (кредитная или расчетная), так и с нескольких счетов клиента, к которым эта карта также привязана. Для юридических лиц и индивидуальных предпринимателей предусматриваются определенные ограничения на снятие наличных денежных средств в течение одного операционного дня. Для физических лиц банки и иные кредитные организации устанавливают собственные денежные лимиты. Норма о мошенничестве с использованием пластиковых карт (ст. 159.3 УК РФ) призвана обеспечивать помимо охраны собственности, также и нормальную деятельность банков и иных кредитных организаций, связанную с беспрепятственным доступом клиентов к своим денежным средствам в необходимый момент.

Платежные карты сложно назвать предметом преступления, поскольку сама по себе карта никакой ценности не представляет, кроме как затрат по себестоимости при ее изготовлении. В результате завладения платежной картой субъект преступления стремится получить доступ к денежным средствам на счете, к которому привязана данная карта. Диспозиция части 1 статьи 159.3 УК сформулирована следующим образом: мошенничество с использованием платежных карт, то есть хищение чужого имущества,

совершенное с использованием поддельной или принадлежащей другому лицу кредитной, расчетной или иной платежной карты путем обмана уполномоченного работника кредитной, торговой или иной организации. Непосредственным объектом указанного преступления, как видно из диспозиции, является собственность, то есть общественные отношения, связанные с владением, пользованием и распоряжением имуществом. Объективная сторона преступления заключается в обмане, в результате которого уполномоченный работник кредитной, торговой или иной организации, будучи введенным в заблуждение относительно того факта, что перед ним находится держатель карты, принимает предоставленную платежную карту в качестве средства платежа. Лицо, предоставляющее данную карту, в подтверждение своего обмана в личности, расписывается на товарном чеке, совершает иные юридически значимые действия, указывающие на то, что именно он якобы является держателем карты.

Мошенничество с использованием платежных карт рассматривается в ст. 159.3 УК РФ как форма хищения. Следовательно, преступление считается оконченным с момента, когда лицо, получив платежную карту, имело реальную возможность воспользоваться ею как средством платежа или обналичить денежные средства через уполномоченного сотрудника кредитной организации[11]. Если же деятельность субъекта этого вида мошенничества была пресечена при попытке использования платежной карты, то реальной возможности у лица воспользоваться ею не представилось. Такие действия необходимо квалифицировать как покушение на совершение преступления. Если же лицо просто владеет или приобрело поддельную карту, то речь может идти лишь о приготовлении к мошенничеству с использованием платежных карт. При этом сущность мошенничества как хищения чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием сохраняется и в рамках данного состава преступления. Под хищением, в соответствии с примечанием 1 к статье 158 УК, понимается совершенные с корыстной целью противоправные безвозмездное изъятие и (или) обращение чужого имущества в пользу виновного или других лиц, причинившие ущерб собственнику или иному владельцу этого имущества.

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

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

никто не удостоверяет, является ли данное лицо правомочным держателем карты или нет. Списание денежных средств происходит до того момента, как владелец карты ставит свою подпись на чеке.

Наглядную аналогию проводит Л.В. Боровых, сравнивая банковскую карту с ключом от квартиры или иного помещения, где находится имущество. Самостоятельно ключ не представляет никакой ценности для преступника, большее значение имеет то, к чему может открыть доступ этот ключ[12]. Если держатель карты добровольно передает ее лицу, но при этом не передает соответствующие права на ее использование, то в этом случае лицо не становится законным владельцем этой карты, когда пользуется ею в торговой организации, расписываясь за держателя. Подобные действия должны квалифицироваться аналогичным образом как кража по соответствующей части ст. 158 УК РФ. Определенные подтверждения этому можно найти и на практике[13], когда действия были квалифицированы как кража (п. «а», ч.3, ст. 158), поскольку способ совершения преступления был тайным[14].

В соответствии с п.16 постановления Пленума Верховного Суда РФ от 27.12.2002 № 29 разграничиваются понятия совокупности и продолжаемого хищения[15]. По мнению специалистов по вопросам мошенничества в банковской сфере с использованием электронных платежных пластиковых карт[16], вышеприведенный пример указывает на тот факт, что виновный дважды стремился получить денежные средства Ф., при этом источник этих денежных средств был в обоих случаях одинаковый. Поэтому несмотря на несколько эпизодов хищения дополнительная квалификация по ст. 159.3 УК РФ является излишней. Так, С. совершил хищение денежных средств с

---

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

[13]Приговор Ленинского районного суда г. Новосибирска от 08.12.2015. Дело № 1-1128/2015 URL:http://sudact.ru/regular/doc/F5Kun42Viw5w/ (дата обращения: 20.07.2017).

[14]Как тайное хищение чужого имущества (кража) следует квалифицировать действия лица, совершившего незаконное изъятие имущества в отсутствие собственника или иного владельца этого имущества, или посторонних лиц либо хотя и в их присутствии, но незаметно для них (О судебной практике по делам о краже, грабеже и разбое: постановление Пленума Верховного Суда РФ от 27.12.2002 № 29 // Российская газета. 2003.18 января).

[15]От совокупности преступлений следует отличать продолжаемое хищение, состоящее из ряда тождественных преступных действий, совершаемых путем изъятия чужого имущества из одного и того же источника, объединенных единым умыслом и составляющих в своей совокупности единое преступление (О судебной практике по делам о краже, грабеже и разбое: постановление Пленума Верховного Суда РФ от 27.12.2002 № 29 // Российская газета. 2003.18 января).

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

банковской карты, принадлежащей К., совершив 123 разные операции, и его действия были квалифицированы по ч. 3 ст. 159.3 УК РФ[17].

Ряд авторов считает, что ввиду вышесказанного представляется излишним относить данный вид хищения к специальным видам мошенничества, а абз. 2п. 13, п. 14 постановления Пленума Верховного Суда РФ от 27.12.2007 № 514 следует пересмотреть, чтобы специально подчеркнуть, что любое хищение чужих денежных средств путем использования заранее похищенной или поддельной кредитной (расчетной) карты следует квалифицировать по соответствующей части ст. 158 УК РФ[18]. Исполнение объективной стороны мошенничества с использованием платежных карт идет вразрез с концепцией добровольности передачи имущества собственником или иным владельцем.

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

Криминалистическая характеристика мошенничества с использованием платежных карт представлена в статье Антонова И.О. и Шалимова А.Н. «Способы мошенничества с использованием платежных карт как элемент криминалистической характеристики данного вида преступлений»[19].

В криминалистическом смысле мошенничество с использованием платежных карт можно определить как систему действий по подготовке, совершению и сокрытию хищения чужого имущества, основным содержанием которой (системы) является использование поддельной или принадлежащей другому лицу кредитной, расчетной или иной платежной карты для осуществления обмана уполномоченного работника кредитной, торговой или иной организации. Фактически в этом случае, как и в других видах мошенничества, содержанием мошеннических действий остается в той или иной степени качественная или количественная замена предмета и средств совершения мошенничества[20].

---

[17]Приговор Кировского районного суда г. Кемерово, Кемеровской области от 12.11.2015. Дело № 1-395/15.URL:http://sudact.ru/regular/doc/Y1E4KZB0MKoV/ (дата обращения: 20.07.2017).

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

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

[20]Волохова О.В. Расследование преступлений,связанных с обманом. М.:Юрлитинформ,

Классификации способов мошенничества с использованием платежных карт по самым различным основаниям представлены в работах ряда авторов, среди которых труды В.Б.Вехова, М.Н.Филиппова, Н.Н.Федотова и др.[21] Анализируя действующее законодательство с учетом произошедших изменений, вышеуказанные работы, а также сложившуюся практику расследования данной разновидности криминального обмана, можно выделить ряд классификаций, которые имеют наибольшее значение в криминалистическом смысле.

В самой статье 159.3 УК РФ фактически представлен ряд оснований для классификации способов мошенничества с использованием платежных карт. Так, их можно классифицировать в зависимости от того, какая разновидность платежной карты была задействована мошенниками для совершения преступления. Соответственно, имеет смысл говорить о способах, в которых были использованы: а) кредитная карта; б) расчетная карта; в) иная платежная карта (УК РФ).

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

1) криминальный обман уполномоченного работника кредитной организации;

2) криминальный обман уполномоченного работника торговой организации;

3) криминальный обман уполномоченного работника иной организации (ст. 159.3 УК РФ).

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

Организованные преступные группы кардеров нередко совершают несколько эпизодов мошенничества. При этом для совершения мошенничества преступники используюти специальное оборудование по изготовлению поддельных пластиковых карт[22]. Несколько эпизодов мошенничества было на счету группы лиц, которая использовала

2008. С.33.

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

[22]Попова Н. Российские банкоматы оказались в ливанской петле//АН-online. 2012. 11 фев. URL: http://argumenti.ru/crime/2012/02/156477, свободный (дата обращения: 20.07.2017).

похищенную у владельца банковскую карту для приобретения товаров в магазинах[23].

Специалисты отмечают, что, как и другие киберспреступления, преступления с использованием платежных карт нередко совершаются членами разветвленных, хорошо организованных преступных групп, участники которых имеют свою преступную специализацию[24]. Криминальная специализация в группе может выглядеть следующим образом: одни члены группы осуществляют сбор информации по платежным картам, другие – обрабатывают собранную информацию и передают их тем, кто занимается изготовлением поддельных карт. Подготовленное таким образом хищение осуществляют лица, специализирующиеся на «вещевом» кардинге – именно они используют платежную карту для обмана работников торговой организации.

Еще одним основанием для классификации способов мошенничества с использованием платежных карт является технологическое решение, задействованное преступниками при совершении преступления. В статье 159.3 УК РФ указаны два способа совершения такого мошенничества: с использованием поддельной (1) или принадлежащей другому лицу (2) платежной карты (УК РФ). Примером последнего является дело, в ходе расследования которого было установлено, что К., совершив тайное хищение имущества, завладел платежной картой потерпевшего и решил использовать ее для осуществления мошенничества. С целью реализации своего умысла К. неоднократно использовал похищенную платежную карту для приобретения различных товаров[25].

По данному основанию, кроме указанных выше способов, исследователи выделяют и другие разновидности криминального обмана в зависимости от того, используется ли для его реализации конфиденциальная информация о реквизитах подлинных карт и их держателях (3) или несовершенство аппаратно-программного обеспечения технологии обращения платежных карт (4)[26].

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

---

[23] Приговор Верхнепышминского городского суда от 21 февр. 2012 г. по уголовному делу № 1-50/12. URL:http://docs.pravo.ru/document/view/22393765/ (дата обращения: 20.07.2017).

[24]Козловский В. Масштабы кибермошенничества растут//Российская газета. 2012. 29нояб.URL: http://www.rg.ru/2012/11/29/karti-site.html, свободный(дата обращения: 20.07.2017).

[25] Приговор Верхнепышминского городского суда от 7 июня 2011 г. по уголовному делу № 1-152/11.URL:http://docs.pravo.ru/document/view/18392970/ (дата обращения: 20.07.2017).

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

задействуют для получения конфиденциальной информации о реквизитах подлинных платежных карт и их держателях.

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

Считывание секретной информации, хранящейся на карте, может производиться разными способами. Наиболее распространенный из них – сговор мошенников с сотрудниками магазинов, отелей, ресторанов, других торговых и развлекательных предприятий. Через такие компании проходит большое количество транзакций с пластиковыми картами, информация о которых сохраняется в компьютерных базах данных компании или на слипах (бумажных документах, подтверждающих факт осуществления платежа). Результатом такого сговора является передача информации о реквизитах карточек представителям криминальных структур. В этом случае происходит так называемый скиминг. Настоящую платежную карту пропускают через специальное устройство (скимер) и считывают данные, которые хранятся на ее магнитной полосе. Скиммеры (от англ. *skimming* – снятие сливок) – приборы, монтируемые на банкомат для несанкционированного считывания конфиденциальной информации непосредственно с карты; накладные клавиатуры, размещаемые на клавиатуре банкомата и используемые для копирования вводимых на настоящую клавиатуру данных; миниатюрные видеокамеры, установленные таким образом, что в их объектив попадает информация, которая вводится в банкомат посредством клавишного набора[27].

Довольно распространен способ, когда криминальные структуры организуют свои собственные магазины. Цель существования подобных

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

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

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

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

Широкое общественное информирование о ставших известными способах выведывания мошенниками конфиденциальной информации снизило эффективность фишинговых атак, что привело к изобретению преступниками так называемого фарминга (англ. *pharming* – производное от *phishing* и *farming*). Этот вид интернет-мошенничества представляет собой процедуру скрытого перенаправления потенциальных жертв мошенничества на ложные IP-адреса в сети Интернет. Для фарминга может быть использован компьютер владельца платежной карты, на который незаметно для пользователя размещается специальная программа («троян»). Фарминг может быть осуществлен и непосредственно на DNS сервере интернет-провайдера владельца карты. Для получения конфиденциальной информации мошенники делают все возможное, чтобы потенциальная жертва была в полной уверенности, что пользуется услугами банка. После того как владелец карты выполнит стандартную процедуру ввода платежных реквизитов, он перенаправляется на официальный сайт банка.

Самым распространённым мошенничеством по данным

международной платёжной системы является мошенничество с утерянными картами. Ущерб от него составляет почти половину от всех случаев мошенничества с кредитными картами,поскольку вовремя не заблокированная потерянная или украденная карта может послужить преступнику отличным средством для оплаты по счету там, где не требуется ввода никаких паролей[28]. С 1 января 2014 года вступила в силу поправка в Федеральный закон от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе». В частности, теперь гражданам предоставляется десять дней вместо ранее установленного одного дня для того, чтобы обнаружить пропажу денежных средств и обратиться с заявлением в банк. По вступившим поправкам в закон банки обязаны сообщать клиентам обо всех операциях, которые проводятся с их картами, теми средствами, которые указаны в договоре.

Мошенничества с использованием платежных карт, совершаемые перечисленными выше способами, нередко очень тесно связаны с предусмотренными уголовным законодательством РФ преступлениями в сфере компьютерной информации (ст. 272–274 УК РФ), мошенничеством в сфере компьютерной информации (ст. 159.6 УК РФ), а также изготовлением или сбытом поддельных кредитных или расчетных карт и иных платежных документов (ст. 187 УК РФ)[29].

Представленные классификации способов мошенничества с использованием платежных карт позволяют более точно оценить возможные корреляционные связи между элементами криминалистической характеристики этого рода мошенничества. Не подлежит сомнению, что среди закономерностей криминальной деятельности особенно большое значение должно уделяться изучению зависимости вида, способа и механизма преступного поведения от особенностей связи правонарушителя с предметом преступного посягательства, обстановкой, сложившейся в месте совершения преступления и вокруг него; следует также учитывать влияние на эту связь личностно-типологических свойств субъекта преступления, степени организованности, разветвленности и состава преступной группы (при наличии таковой) и др.[30]

Исследование современных способов мошенничества с использованием платежных карт имеет конечной целью поддержание в актуальном работоспособном состоянии криминалистической характеристики данного вида мошенничества. Она является составной частью методики расследования указанных преступлений и во многом предопределяет качество предварительного расследования. Результаты изучения способов совершения преступлений указанного вида также могут быть востребованы при разработке оптимального методического

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

[29]Там же.

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

обеспечения механизма противодействия мошенническим посягательствам в национальной платежной системе.

Характеристика личности преступника, совершившего общественно опасные деяния в сфере проведения безналичных расчетов, производимых с использование банковских карт, представлена в статье Васюкова С.В. «Криминологическая характеристика личности преступника, совершающего общественно опасные деяния в сфере проведения безналичных расчетов с использованием банковских карт»[31].

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

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

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

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

Проведенные исследования показали, что личность преступника, совершающего преступления в этой сфере, отличается рядом характерных особенностей. Данные уголовной статистики и материалов уголовных дел свидетельствуют о том, что среди преступников достаточно высок удельный вес мужчин – около 78%. Доля женщин среди лиц, совершивших хищения и мошенничества с банковскими картами, значительно ниже и составляет всего около 22%, и в отличие от обычного мошенничества (где они выполняют роли организаторов и непосредственных исполнителей), их роль чаще всего сводится к оказанию содействия при совершении преступлений (например, помощи в обналичивании денежных средств). Вместе с тем указанный показатель значительно выше среднестатистического показателя удельного

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

веса преступниц женского пола в целом, который в последние годы колеблется от 12 до 15%[32].

В структуре лиц, совершивших экономические преступления в сфере проведения безналичных расчетов, производимых с использованием банковских карт, достаточно высок удельный вес иностранных граждан (около 20%), представленных гражданами стран ближнего и дальнего зарубежья (КНР, КНДР и др.). Среди всех иностранцев, совершивших преступления с помощью банковских карт, удельный вес последних составил не более 15%[33].

Наиболее криминогенной возрастной категорией являются лица 26-39 лет: их доля в структуре преступности доходит до 54%, далее следует возрастная группа осужденных за данное деяние: 39-50 (около 26%), от 18 до 26 лет (около 18%), 50 и старше (2%). Преобладание в структуре организованного мошенничества более зрелого контингента преступников обуславливается наличием жизненного опыта, свидетельствующего о способности лица максимально использовать свои физические и интеллектуальные возможности для обеспечения результативности и скрытности осуществления преступной деятельности. Весьма неблагоприятные прогнозы имеет группа лиц в возрасте до 29 лет. Практически это молодые, но уже вполне профессиональные преступники, связавшие повышение уровня своего материального благосостояния, да и положение в обществе в целом, с криминалом[34].

Изучаемый вид преступного поведения требует наличия определенного уровня знаний, умений и навыков в области информационных технологий, а также способности оказать психологическое воздействие. Изучение статистических и фактологических данных, характеризующих субъектный состав осужденных за мошеннические действия по уровню образования, показывает, что он не изменяется в последние годы. Анализ материалов уголовных дел показал, что около 34% мошенников имели среднее общее образование, 25% – среднее специальное, 27% – высшее и неоконченное высшее, 14 % – неполное среднее. При этом отдельные лица (около 2%) имели по два высших образования[35].

Анализ субъектного состава осужденных за совершение преступлений, предусмотренных ст. 159 УК РФ, по роду профессиональной деятельности показал, что среди них: трудоспособные без определенных занятий

---

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

[33] Васюков С.В. Предупреждение преступлений, совершаемых в сфере проведения безналичных расчетов, проводимых с использованием банковских карт». Автореферат диссертации на соискание ученой степени кандидата юридических наук: Специальность12.00.08 - Уголовное право и криминология; уголовно-исполнительное право. М., 2013. С. 20-23.

[34] Там же.

[35]Там же.

составляют 49,3%, государственные и муниципальные служащие - 3,7 %, служащие коммерческих или иных организаций - 10,3%, частные предприниматели - 2,5%, учащиеся и студенты - 2,9%, рабочие - 21,8%, лица прочих занятий - 9,5%[36].

Анализ материалов судебно-следственной практики показывает, что 45% мошенников, совершивших уголовно наказуемые деяния в составе организованной группы или преступного сообщества, в браке не состояли. В законных отношениях находились 55% участников мошеннических организованных структур, из них представители мужского поля составили 75%[37].

Изучение абсолютных показателей лиц, совершивших организованные мошенничества, позволяет сделать вывод о том, что уровень ранее судимых лиц, совершивших мошенническое посягательство, изменяется практически пропорционально числу привлеченных к ответственности за данное уголовно наказуемое деяние. В среднем каждый пятый (около 20%) привлеченный к ответственности за мошенничество ранее был судимым, из них подавляющее большинство были осуждены условно[38].

Итак, противодействие мошенничеству с использованием пластиковых карт - это реализация системы противодействия как внешнему, так и внутреннему мошенничеству, так называемые решения антифрод, работающие в реальном времени. Другими словами, это комплекс организационных и технических мер, обеспечивающих дополнительную защиту автоматизированных банковских систем и систем дистанционного банковского обслуживания.

3.4. Методика расследования изготовления или сбыта поддельных денег или ценных бумаг

В Российской Федерации денежные знаки и ценные бумаги используются как один из регуляторов экономических отношений, формирования их в направлении, необходимом для достижения государственных, общественных и личных интересов. Подделка денег или ценных бумаг нарушает естественные, нормальные условия существования общества, поэтому обладает признаком общественной опасности. Подделка денег или ценных бумаг наносит вред юридическим и физическим лицам, отрицательно влияет на уровень инфляции, что способствует изменению цен и наносит вред финансовой системе страны; состав преступления, предусмотренный статьей 186 УК РФ, имеет низкую раскрываемость; общественная опасность подделки денег или ценных бумаг признана на национальном и международном уровнях.

[36] Васюков С.В. Указ.раб.
[37] Там же.
[38] Там же.

Предметом фальшивомонетничества являются банковские билеты Центрального банка Российской Федерации и металлические монеты, которые являются материальными объектами, обладающими функцией меры стоимости, подлежащие обмену на сегодняшний день. Безналичные деньги не могут быть предметом данного преступления; предметом фальшивомонетничества являются государственные ценные бумаги и другие ценные бумаги в валюте Российской Федерации. Под ценной бумагой понимается документ, удостоверяющий (с соблюдением установленной формы и обязательных реквизитов) имущественные права, осуществление и передача которых возможны только при предъявлении данного документа.

Бездокументарные ценные бумаги не могут быть предметом данного преступления; к предмету преступления, предусмотренного статьей 186 УК РФ, относится иностранная валюта, под которой понимаются казначейские билеты, денежные знаки в виде банкнот, монеты, являющиеся законными платежными средствами в соответствующем иностранном государстве или группе государств и находящиеся в обращении, а также изъятые из обращения, но подлежащие обмену денежные знаки; к предмету преступления предусмотренного статьей 186 УК РФ, относятся ценные бумаги в иностранной валюте, под которыми понимаются платежные документы и другие долговые обязательства.

Таким образом, объективная сторона преступления, предусмотренного статьей 186 УК РФ, заключается в четырех альтернативных действиях: изготовление, хранение, перевозка в целях сбыта и сбыт.Квалификация преступления, предусмотренного статьей 186 УК РФ, не может находиться в зависимости от нахождения поддельной купюры в обращении.Распространенным способом совершения преступления является, изготовление фальшивых денежных знаков с помощью полиграфического оборудования либо копировальной техники. Наиболее распространённым местом преступлений являются районы наибольшего скопления людей, которые расположены в относительном отдалении от места проживания преступников; благоприятными условия для совершения преступления являются не оборудованные специальными аппаратами точки торговли. Наиболее распространенным способом передачи фальшивых денежных средств является обмен на товары.

Специальной целью субъективной стороны преступлений, предусмотренных статьей 186 УК РФ, является желание сбыть данные поддельные купюры в качестве подлинных; изготовление явно схожих с подлинными поддельных денежных знаков не всегда указывает на направленность у подозреваемого лица целей сбыт. Изготовление денежных знаков с иными целями не является фальшивомонетничеством.Преступление, предусмотренное статьей 186 УК РФ, чаще всего совершается мужчинами, небольшой процент преступлений совершается в алкогольном опьянении.

Эффективность расследования по делам фальшивомонетничества во многом зависит оттого, насколько основательны знания следователя и оперативного сотрудника об особенностях субъекта преступления, процесса

изготовления им денег, признаков способа подделки, отображающихся в следах преступления. Поскольку предметом фальшивомонетничества являются наличные деньги либо ценные бумаги, выпуск и обращение которых регламентируются законодательством РФ, а также деньги и ценные бумаги других государств, именно на их изготовление и (или) сбыт направлен умысел виновных.

Выпуск денег в обращение (эмиссия) является исключительным правом государства. Банкноты производятся на государственных полиграфических предприятиях, оборудованных специальными машинами, обеспечивающими применение различных способов защиты от подделки и получение печатной продукции высокого качества. Технология печати денежных знаков унифицирована, так как требования, предъявляемые к банкнотам, везде одинаковы. Она должна обеспечить их практичность, невозможность (или трудоемкость) подделки, а также выполнение идентичности миллиардных тиражей в течение многих лет.

К наиболее распространенным способам подделки денежных знаков относятся: рисование, способы полиграфической печати (офсетный, фотоцинкографский способ, фототипия), способы копирования, фотографические способы, комбинированный способ. Своевременное возбуждение уголовного дела является одним из важнейших условий, обеспечивающих быстрое и полное раскрытие фальшивомонетничества. Действительно, успех в раскрытии и расследовании указанного преступления определяется своевременным возбуждением уголовного дела, качеством осмотра предъявленных поддельных денежных знаков и места преступления, проведенных экспертиз, других неотложных следственных действий и оперативно-розыскных мероприятий. Как показывает практика, значительное число дел рассматриваемой категории остаются нераскрытыми. Поэтому важно на первоначальном этапе расследования наметить и реализовать тот круг мероприятий, который поможет быстро раскрыть преступление и изобличить преступника

3.5. Уголовно-правовые и криминологические меры противодействия преступлениям, совершаемым в сфере банковской деятельности, связанной с оборотом наличных денежных средств

В Российской Федерации правовой основой противодействия нелегальному обороту преступных доходов являются Конституция Российской Федерации, общепризнанные принципы и нормы международного права, международные договоры Российской Федерации, Федеральный закон от 7 августа 2001 г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», и другие нормативные правовые акты.

Федеральный закон от 7 августа 2001 г. «О противодействии легализации (отмыванию) доходов, полученных преступным путём» закрепляет официальное понятие данного вида преступления. Согласно

статье 3 данного закона легализация определяется как придание правомерного вида владению, пользованию или распоряжению денежными средствами или иным имуществом, полученными в результате совершения преступления. С точки зрения права, основными целями легализации (отмывания) денежных средств и имущества, полученных преступным путём, являются:

1. попытка скрыть первоисточник происхождения и принадлежности незаконно полученных доходов;

2. придание правомерного вида владению, пользованию и распоряжению;

3. обеспечение за счет легализованных средств терроризма или иных организованных форм преступной деятельности.

Возможности легализации незаконных доходов во многом зависят от состояния и качества нормативно-правового регулирования и осуществления финансового контроля со стороны уполномоченных организаций. Это обусловлено, прежде всего, разницей в подходах к организации контроля за имущественным положением и расходами физических лиц в Российской Федерации и в экономически развитых странах. Таким образом, поскольку понятие легализации (отмывания) денежных средств и имущества, полученных преступным путём, – это процесс придания незаконно приобретенным денежным средствам и имуществу статус легальности, основным целевым назначением преступно полученных средств является стремление извлечь прибыль путем вложения незаконных средств в легальный бизнес[39].

В теории и практике криминологической деятельности данный процесс подразделяют на три стадии или фазы.

Первая – стадия размещения (placement), в которой доходы, происходящие непосредственно от преступления (например, от продажи наркотиков, оружия), в первый раз вкладываются в финансовые учреждения или используются для скупки разного рода активов и ценных бумаг.

Вторая – стадия укрытия («маскировки» - layering), в которой предпринимается первая попытка сокрытия или маскировки источника происхождения грязных денег и идентичности их владельца.

Третья - стадия легализации (интеграции – integration), в которой грязные деньги вводятся в легальные хозяйственные структуры и финансовые системы с целью их окончательной ассимиляции со всеми имеющимися в них средствами. Любая из перечисленных стадий включает в себя признаки состава преступления «отмывание денег»[40].

Данное преступление часто ограничивается одной лишь из таких

[39]Зубков В.А., Осипов С.К. Международные стандарты в сфере противодействия отмыванию преступных доходов и финансированию терроризма: учебное пособие. М.: Международный учебно-методический центр финансового мониторинга, 2013. С. 4, 156.

[40]Волеводз А.Г. Финансовые механизмы легализации (отмывания) денежных средств, полученных преступным путем, связанные с их переводом за границу // Банковское право. 2012. № 3. С. 64-77.

стадий. Это зависит, во-первых, от характера задачи, которую ставят в данном случае преступники или преступные группировки, а во-вторых, от результатов работы правоохранительных органов, от их способности разоблачать и пресекать подобные операции. Во множестве случаев каждая стадия отмывания денег четко и вполне естественно отделена от остальных стадий данного процесса. В других случаях, напротив, эти стадии могут протекать одновременно, чаще всего «накладываясь» одна на другую. Очередность зависит от стадии готовности механизма отмывания денег, а также от потребностей и целей, которые ставят перед собой преступные организации.

Вместе с тем встречается описание и двухступенчатой модели, состоящей из двух явлений, следующих друг за другом:

1) отмывание денег (moneylaundering)

2) возвращение их в оборот (recycling).

Рассмотрим отдельные фазы трехстадийной модели отмывания денег.

Целью первой из них – размещения – является стирание или заметание следов преступного происхождения имущества. Это действия, целеустремленно направленные на то, чтобы помешать идентификации и конфискации преступной добычи со стороны государства. Например, путем обмена «грязных» наличных и безналичных денег на иностранную валюту или другие ценности (акции, ценные бумаги, золото, драгоценные камни, недвижимость). Такую стадию иногда называют стадией предварительного отмывания, потому что в одних случаях она завершается вложением средств, не оставляющих следов, а в других – такие следы окончательно стереть не удается и у правоохранительных органов остается возможность разоблачить преступников. К случаям почти бесследного размещения преступных доходов можно отнести вложение «грязных» денег, во-первых, в движимое имущество; во-вторых, предоставление ссуд, и в-третьих, в анонимные или подставные фирмы. Здесь широко используются фиктивные обороты на предприятиях, где оборачиваются большие массы наличных денег: передвижные торговые точки по продаже мороженого, фруктов, а также пиццерии, бары, рестораны, пункты обмена валюты, казино, химчистки и подставные фирмы[41].

Отличительные черты первой стадии следующие:

- предметом отмывания выступают имущественные ценности, непосредственно полученные от первичного преступления;

- предметом отмывания чаще всего служат наличные деньги;

- действия отмывателей заключаются в краткосрочных финансовых операциях, отличающихся простотой и однообразием.

Результаты отмывания на первой стадии не дают, как уже отмечалось, преступникам гарантии, что следы их преступной деятельности запутаны или

[41]Волеводз А.Г. Финансовые механизмы легализации (отмывания) денежных средств, полученных преступным путем, связанные с их переводом за границу // Банковское право. 2012. № 3. С. 64-77.

стерты окончательно, и что преступная добыча не будет выявлена и конфискована. Поэтому они приступают ко второй стадии заметания следов грязных денег – стадии укрытия или маскировки. Основная ее цель – переместить, удалить незаконно полученные средства от места совершения преступления, придать им иной вид, сделать все для того, чтобы утаить связь отмываемых денег с источником их происхождения. Это, как правило, перевод грязных денег за границу, в любую страну мира, желательно туда, где соблюдение банковской тайны заходит настолько далеко, что не позволяет правоохранительным органам добраться до владельцев преступной добычи. Предпочтение также отдается странам, в которых отсутствуют или не соблюдаются строгие правила ведения бухгалтерского учета, а также территориям с облегченным налоговым режимом и почти полным отсутствием налогового контроля, каковыми являются налоговые гавани или оффшорные зоны. Впрочем, довольно часто преступники переводят деньги и в страны традиционного помещения, такие, как, например, Швейцария.

Наконец, на третьей стадии (легализации или интеграции) происходит долгосрочное «прокручивание» преступной добычи, уже прошедшей предварительное «отмывание» на предыдущих стадиях. Здесь грязные деньги окончательно выводятся из нелегального оборота и «растворяются» в активах, ценных бумагах, в движимом и недвижимом имуществе. Они становятся объектом налогообложения. Это не относится к тем суммам, которые на предыдущих стадиях отмывания были направлены на финансирование дальнейшей преступной деятельности.

Для легализации незаконных доходов используются все виды хозяйственной деятельности, которые связаны с большим оборотом наличных денег – таксопарки, кинотеатры, супермаркеты, дискотеки, ночные клубы, казино и т. п., где «оприходование» денежных средств преступного происхождения можно легко выдать за рост объема своей собственной предпринимательской деятельности.

Как в законодательной, так и в оперативно-розыскной деятельности постоянно предпринимаются попытки отыскать слабые звенья в длинной и подчас запутанной цепи торгово-посреднических и финансовых операций, определить тот самый момент в «деятельности» отмывателей, когда безошибочно и с наибольшими шансами на успех их можно «схватить за руку». Международный опыт свидетельствует, что наиболее часто такие возможности открываются на первой фазе отмывания грязных денег, особенно тогда, когда эти деньги связаны с распространением наркотиков. Прибыль от этого преступного промысла, так же, как и от других его видов, выступает, в основном, в форме наличности.

Под способом или технологией отмывания денег понимают совокупность устойчивых и повторяющихся признаков, характеризующих определенное поведение, которое связано с финансовыми операциями. Такие признаки заранее «программируют» объем, характер и возможности проведения таких операций в процессе отмывания денег.

Итак, основные формы интеграции легализованных преступных

доходов в финансовую систему следующие:

-операции с недвижимостью или произведениями искусства, аукционные сделки, где цену товара можно определить лишь условно. Используется заниженная или завышенная цена контракта. Разница с реальной ценой доплачивается неучтенными наличными денежными средствами;

- экспортно-импортные операции, при которых составляются реальный и фиктивный договоры (с завышенной суммой сделки). Разница между реальной и фиктивной ценой товаров, работ, услуг, оплаченная выведенными из легального денежного оборота деньгами, остается на счете фирмы-посредника;

- деньги депонируются на счете зарубежной фирмы и используются для выдачи ссуды, являющейся для заемщика легальными деньгами;

- учреждение зарубежной корпорации в офшорной зоне, открытие ее счета в иностранном банке с последующим использованием этого счета для предоставления ссуд, платежей по фиктивным договорам аренды или за фиктивные услуги;

- деньги преступного происхождения декларируются как легальный выигрыш в казино или лотерее.

В каждом отдельном случае могут применяться самые разные методы отмывания денег, но суть всех операций сводится к тому, чтобы придать незаконно полученным средствам вид дохода от законной деятельности. Анонимные денежные средства получают новый источник происхождения, и легализовавшийся доход перераспределяется в пользу преступника, совершившего основное преступление.

Банки представляют собой часть экономической системы, имеющей существенное значение для успешного развития рыночного механизма. Процессы, происходящие в сфере банковской деятельности, оказывают влияние на все стороны жизнедеятельности социума. Один из ключевых вопросов на этапе становления рыночных отношений в России — необходимость эффективного противодействия преступлениям, совершаемым в сфере банковской деятельности.

Среди таких преступных деяний можно выделить достаточное количество уголовных правонарушений, включенных в различные разделы Особенной части Уголовного кодекса РФ, одним из которых является легализация (отмывание) средств, полученных преступным путем.

Термин «отмывание денег» (moneylaundering) впервые был использован в 80-х гг. в США применительно к доходам от наркобизнеса и обозначает процесс преобразования нелегально полученных денег в легальные. Предложено много определений этого понятия. Президентская комиссия США по организованной преступности в 1984 г. привела следующую формулировку: «Отмывание денег — процесс, посредством которого скрывается существование, незаконное происхождение или незаконное использование доходов, и затем эти доходы маскируются таким

образом, чтобы казаться имеющими законное происхождение»[42]. Отмывание денег является конвертацией преступных доходов в активы, которые не могут быть возвращены к предикатному преступлению.

Согласно еще одному источнику, отмывание денег — придание правомерного вида владению, пользованию или распоряжению денежными средствами или иным имуществом, полученными в результате совершения преступления[43], т.е. их перевод из теневой, неформальной экономики в сферу официальной экономики для того, чтобы иметь возможность пользоваться этими средствами открыто и публично.

Понятие «легализация (отмывание) средств, полученных преступным путем» введено в юридическую литературу РФ посредством УК РФ. В современных условиях проведения экономических реформ вопрос криминализации общественных отношений приобретает особую актуальность. Несовершенство правовой базы способствует росту коррупции и формированию теневого сектора экономики в наиболее доходных сферах хозяйственной деятельности, а именно в кредитно-финансовой и банковской. Проблема преступности в банковской сфере не могла остаться без внимания ученых. Возникает потребность в обосновании действующих нормативных предписаний, их совершенствовании, в адаптации нормативных правил к реалиям действительности, в криминализации деяний, совершаемых в сфере банковской деятельности, имеющих в своей структуре все признаки преступлений, а также в декриминализации тех уголовных правонарушений, которые много лет не имеют фактических проявлений и судебная практика относительно которых отсутствует.

Комплексный подход к решению проблемы предотвращения постоянно трансформирующейся и приобретающей новые формы преступности в банковской сфере требует не только совершенствования существующей нормативной базы, но и в целом выработки новой действенной системы противодействия таким посягательствам на уровне существенного реформирования положений уголовного законодательства РФ по этим вопросам.

Снижение покупательной способности граждан связано с изменением общего социально-экономического фона в стране. Однако это обстоятельство не приводит к сокращению потребностей граждан в целом, наоборот, с развитием технологий и увеличением объема информации, которую потребитель получает через телевидение и Интернет, у него появляется ощущение необходимости приобретения значительного количества вещей, не всегда доступных из-за их высокой стоимости. Желание получения легких денег, в том числе с учетом соблазнов, которые навязывают нам средства массовой информации, чаще возникает у неустойчивых членов общества. С этим можно связать рост количества преступлений, направленных на

[42]President’s Commission on Organized crime. Theeachconnection, 1984. P. 7.

[43]Авдеев В.А. Проблемы реализации уголовной ответственности // Известия Иркутской государственной экономической академии. 2016. № 5 (50). С. 50–54.

получение денежных средств, в частности, случаев легализации (отмывания) средств, полученных преступным путем (далее — легализация средств).

В Конвенции Совета Европы «Об отмывании, поиске, аресте и конфискации доходов, полученных преступным путем, и о финансировании терроризма» понятие «доходы» означает любую экономическую выгоду, полученную в результате совершения преступлений[44]. Практически так же раскрыта сущность и сформулировано определение данного понятия в законе Российской Федерации «О противодействии легализации (отмыванию) доходов, полученных преступным путем» от 7 августа 2001 г. № 115-ФЗ[45].

Доходами в контексте определения легализации выступают:

1) денежные средства — валюта (монеты и бумажные деньги РФ или какой-либо другой страны, в том числе евро) в наличной или безналичной форме, ценные бумаги на предъявителя, в том числе с наследованием права собственности на них;

2) иное имущество — предметы материального мира, которые удовлетворяют потребности людей и относительно которых могут возникать гражданские права и обязанности (дома, строения, жилые помещения, земельные участки, оборудование, транспортные средства, ювелирные изделия, скот, произведения искусства и т.д.)[46].

Формулировка «деньги или иное имущество» означает, что законодатель рассматривает денежные средства как разновидность имущества. Такой подход основывается на определении понятия «имущество» в гражданском законодательстве. Так, согласно Гражданскому кодексу РФ, объектами гражданских прав являются вещи, в том числе деньги и ценные бумаги, иное имущество, имущественные права, результаты работ, услуги, результаты интеллектуальной, творческой деятельности, информация, а также другие материальные и нематериальные блага, т.е. ГК РФ определяет вещи, деньги и ценные бумаги как разновидность имущества, а деньги и ценные бумаги — как разновидность вещей.

Таким образом, исходя из норм гражданского законодательства деньги являются вещами. Однако полагаем, что подведение денег под подобное определение не совсем корректно. Среди ученых ведутся дискуссии относительно правовой природы денег, а именно наличия права собственности на безналичные деньги, что требует должного законодательного урегулирования. К изучению вопросов легализации средств, полученных преступным путем, обращались многие ученые. Однако относительно сферы банковской деятельности данный вопрос остается

---

[44]Конвенция Совета Европы об отмывании, поиске, аресте и конфискации доходов, полученных преступным путем, и о финансировании терроризма. URL: http:// search.ligazakon.ua/l_doc2.nsf/link1/MU05399.html (дата обращения: 20.07.2017).

[45] О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма: Федеральный закон от 07.08.2001 №115-ФЗ:редакция от 24.10.2016// КонсультантПлюс: ВерсияПроф. (дата обращения: 20.07.2017).

[46]Авдеев В.А. Проблемы реализации уголовной ответственности // Известия Иркутской государственной экономической академии. 2016. № 5 (50). С. 50–54.

открытым, поскольку такие преступления продолжают совершаться, что свидетельствует о недостаточной эффективности ранее предложенных методов их предупреждения.

Отмывание средств, полученных преступным путем, является достаточно сложной процедурой, которая состоит в том, что такие средства проводятся через финансовую систему с целью сокрытия их нелегального происхождения. Основное задание преступников при реализации подобных схем — придание таким средствам вида законно полученных на всех стадиях отмывания. Исследование криминологической характеристики легализации средств, полученных преступным путем, в сфере банковской деятельности и разработка методов предупреждения таких преступлений требуют краткого обращения к уголовно-правовой основе ответственности за совершение данного преступления.

ГК РФ предусматривает ответственность за легализацию (отмывание) средств, полученных преступным путем, а УК РФ закрепляет уголовную ответственность за умышленное нарушение требований законодательства о предотвращении легализации (отмывания) доходов, полученных преступным путем, или финансирования терроризма и о противодействии им.

Преступление, предусмотренное УК РФ, отличается своей непредсказуемостью, латентностью, использованием множества финансовых операций и сделок с имуществом. Непредсказуемость подобных действий проявляется и в применении различных неординарных способов достижения преступных целей. Преступники порой так умело скрывают следы, что среди большого количества проведенных банковских операций и неоднократно переведенных на различные счета средств обнаружить первоначальный источник их поступления бывает достаточно сложно. Так, могут проводиться многократные зачисления денег на один счет в течение дня множеством лиц; перечисления наличных на счета подставных лиц незначительными суммами; в некоторых случаях внесение больших сумм на счет наличными также может указывать на противоправность действий клиента банка.

С целью эффективной борьбы с легализацией средств в сфере банковской деятельности необходимым является мониторинг основных качественно-количественных показателей указанного преступления. Легализация средств представляет собой сложное явление, результат действия многих социальных факторов, которые влияют на ее уровень, структуру и динамику. Усложнение общественных отношений в процессе их развития, многообразие и разнообразие норм, регулирующих эти отношения, обусловливают разного рода конфликты, среди которых наиболее опасными для общества представляются преступления.

Именно они дезорганизуют его нормальную жизнедеятельность, создавая нежелательные общественно опасные последствия. Преступность как социальное явление имеет ряд признаков, которые отображаются рядом показателей, присущих также преступлениям, связанным с легализацией средств в сфере банковской деятельности: уровнем преступности, структурой преступности, динамикой преступности, географией преступности. Так

называемая беловоротничковая преступность, а именно преступления, совершаемые в финансово-кредитной системе, составляет около 1,0–1,5 % от общеуголовных преступлений и 10–15 %— в структуре экономических правонарушений.

Случаи легализации средств в сфере банковской деятельности, как правило, имеют значительный резонанс в обществе, а потому факты их совершения крайне редко скрываются от регистрации и учета. Хотя возникают ситуации, в которых банковские учреждения, особенно в условиях, когда ущерб не был причинен (неудачное посягательство, преступник получил сопротивление т.п.), не оповещают об этом правоохранительные органы, поскольку не заинтересованы в распространении данной информации, могущей негативно повлиять на авторитет банка. Однако, учитывая общественную опасность этих преступлений, считаем, что статистические данные в целом отражают достоверный уровень данной преступности в стране и регионах[47]. Надежный и развитый банковский сектор играет чрезвычайно важную роль в стабилизации экономики государства. В 2015 г. начался процесс реформирования банковской системы, основными задачами которого являются восстановление доверия, повышение уровня защищенности прав кредиторов и потребителей, развитие инфраструктуры. Значительное количество банковских учреждений было признано неплатежеспособными, т.е. было установлено, что существование таких банков является абсолютно экономически нецелесообразным. Национальный банк «очищает» банковскую систему от неплатежеспособных банков путем вывода их с рынка.

Таким образом, на рынке остаются наиболее стабильные банковские учреждения, которые обеспечивают широкий спектр надежных банковских услуг, в том числе и гарантирование денежных вкладов граждан. С другой стороны, реформирование банковской системы должно иметь комплексный характер, который бы предусматривал совершенствование системы защиты банков от преступных посягательств.

Эффективными в этом смысле могут стать поиск новых мер уголовно-правового воздействия, криминализация преступных посягательств, направленных на банковскую систему, формирование соответствующей системы уголовно-правовых норм, часть из которых должна быть выделена из преступлений, совершаемых в сфере хозяйственной деятельности. Очевидно, что новые экономические условия, в которых сегодня находится государство, требуют того, чтобы посягательства на банковскую систему не рассматривались как часть уголовно-правовых норм в системе преступлений в сфере экономической деятельности, а были включены в отдельный раздел УК «Преступления в сфере банковской деятельности».

По нашему мнению, к преступлениям в сфере банковской деятельности

[47]Авдеев В.А. Проблемы реализации уголовной ответственности // Известия Иркутской государственной экономической академии. 2016. № 5 (50). С. 50–54.

следует относить общественно опасные деяния, посягающие на общественные отношения в сфере защиты интересов вкладчиков и собственников кредитных организаций, а также на установленный государством порядок функционирования банковских учреждений. Таким образом, нормы УК РФ, предусматривающие ответственность за совершение преступлений в сфере банковской деятельности, можно разделить на две условные подгруппы:

1) направленные на защиту установленного государством порядка функционирования банковских организаций. Сюда можно отнести незаконную банковскую деятельность (ст. 172 УК), легализацию (отмывание) денежных средств или иного имущества, приобретенных преступным путем (ст. 174, 174.1 УК);

2) направленные на защиту интересов вкладчиков и собственников кредитных организаций. Это мошенничество (ст. 159 УК), незаконное получение кредита (ст. 176 УК), злостное уклонение от погашения кредиторской задолженности (ст. 177 УК), преднамеренное банкротство (ст. 196 УК), фиктивное банкротство (ст. 197 УК).

В.В. Селезнев преступления в сфере бизнеса и экономики называет экономическими. Следует заметить, что формулировка «экономические преступления» является в данном контексте не совсем корректной. Согласно ФЗ РФ «О банках и банковской деятельности»[48], банки обязаны разрабатывать, внедрять и постоянно обновлять правила внутреннего финансового мониторинга и программы его проведения с учетом требований законодательства о предотвращении легализации (отмывания) средств, полученных преступным путем.

Национальный банк при осуществлении надзора за деятельностью банков проводит проверку банков по вопросам соблюдения ими требований соответствующего законодательства.

Для осуществления более полного криминологического анализа данного уголовного правонарушения необходимо также обратить внимание на причины и условия его совершения. Анализируя условия легализации средств в сфере банковской деятельности, следует сосредоточиться на двух группах условий.

Первая группа — условия, формирующиеся в качестве предшествующего звена социально-психологического явления преступности и преступлений, а также способствующие проявлению преступности и преступлений и наступлению преступных результатов. Так, нестабильная экономическая обстановка в государстве приводит к росту безработицы и расслоению населения по уровню доходов, что для потенциальных преступников выступает условием совершения преступных посягательств на денежные средства граждан.

Другая группа условий — отсутствие действенной системы

[48] О банках и банковской деятельности: Федеральный закон от 02.12.1990 №395-1: редакция от 24.10.2016// КонсультантПлюс: ВерсияПроф. (дата обращения: 20.07.2017).

профилактики таких уголовных правонарушений. Обе группы условий играют свою отрицательную роль и создают благоприятные обстоятельства для преступных проявлений[49].

Можно также выделить общие и специальные причины и условия, способствующие осуществлению легализации средств в сфере банковской деятельности. Так, под общими причинами следует подразумевать нестабильность банковской системы, недостатки в работе правоохранительных органов, слабое их взаимодействие с банками, коммерческими, государственными органами, высокий уровень латентности рассматриваемого вида преступлений.

Среди специальных причин необходимо обозначить отсутствие должного практического опыта расследования преступлений данного вида, существование оффшорных зон, банковской тайны. Следует отметить также стремительное развитие телекоммуникаций, которое не могло не затронуть и финансовую сферу.

Мощный рост числа банковских сделок, осуществляемых в веб-пространстве, также привел к новым формам легализации денежных средств через использование интернет-технологий. Легализации способствуют и новые виды интернет-каналов, такие, как онлайн-казино и виртуальные аукционы, а также появление виртуальных денег.

К рассмотренным причинам легализации можно добавить и такие, как несовершенство законодательства, высокая доходность внешнеторговых операций, связанная с различием структуры мировых и внутренних цен, длительное отсутствие действенной системы валютного и экспортного контроля. Преступники выбирают уязвимый объект (банковское учреждение) и используют различные способы совершения противоправных действий. Наиболее распространенными способами легализации преступных доходов в банковской сфере являются:

- перевод средств через банковские счета по фиктивным договорам;
- получение в банках средств со счетов на фиктивных основаниях;
- перевод средств на банковские счета за границу на основании фиктивных сделок;
- заключение договоров банковского вклада;
- осуществление валютообменных операций; заключение кредитных договоров[50].

В способе в значительной мере находят выражение как фактические, так и социальные черты и свойства преступления, а также лица, его совершившего. В первом случае, при переводе средств через банковские счета по фиктивным договорам, лицо, которое намеревается легализовать средства, заключает договор банковского счета и расчетно-кассового

[49]Алиев Я.Л., Вихров А.А., Сальников П.П. Теневая экономика и организованная преступность в социальной системе России // Правовое поле современной экономики. 2015. № 1. С. 31-43.

[50]Сухонос В.В. Легализация преступных доходов в банковской сфере и борьба с ней / В.В. Сухонос // Правовой вестник академии банковского дела. 2012. № 1 (6). С. 1.

обслуживания. Возможен также вариант, когда подставная фирма заключает с банком договор об обслуживании по системе «Клиент-Банк». В подобных случаях легализаторы могут действовать с помощью соучастников среди сотрудников персонала банка, а иногда и самостоятельно, используя недостатки внутреннего контроля банковской системы. Процесс отмывания, как правило, продолжается в течение определенного периода. Сначала легализатор от имени фирмы предоставляет платежное поручение, которое может быть оформлено как в письменном, так и в электронном виде, о переводе денежных средств со счета одной подставной фирмы на счет другой в определенном банке. В такой цепочке может быть задействовано большое количество различных организаций. В платежном поручении ставится подпись номинального директора или подделываются подписи лиц, чьи данные используются. Основанием для перевода или платежа является выполнение различных соглашений. Чтобы переводы подставной фирмы выглядели достоверными, легализаторы составляют документы, отображающие финансово-хозяйственную деятельность предприятия. При этом суммы в финансовых отчетах значительно превышают реальные расходы.

Во втором случае, при получении в банках средств со счетов на фиктивных основаниях, достаточно часто используются кредитные организации. При этом разрабатываются разнообразные схемы перевода денег в наличные средства, например, на основании договоров страхования, выплаты дивидендов на счета физических лиц, которые и обналичивают эти средства. Перевод средств на банковские счета за границу на основании фиктивных сделок происходит таким образом. Банки России имеют право самостоятельно осуществлять работу по корреспондентским счетам в заграничных банках. При наличии таких счетов банки-корреспонденты по указанию соответствующих банков-собственников производят расчетные платежи по международным счетам.

Существует несколько форм почтовых платежей:

- в банках-корреспондентах есть карты с примерами подписей, согласно которым заверяются подписи на полученных платежных документах;

- электронные (SWIFT) платежи (платежные поручения передаются электронной почтой, при этом перед текстом платежного документа проставляются кодированные данные о виде, валюте, ее количестве, времени платежа).

Таким видом платежа и пользуются легализаторы. Сначала денежные средства обмениваются на валюту в российском банке и на основании фиктивных договоров по платежному поручению со счета подставной фирмы в банке России переводятся на счет подставной фирмы в заграничном банке. За границей легализаторы имеют широкие возможности скрыть полученные преступным путем средства в оффшорных зонах. Легализаторы также составляют договор банковского вклада. Такой договор составляется от имени подставного лица для дальнейшего получения денежных средств или

перевода денег в виде банковских вкладов за границу, приобретения ценных бумаг и т.д. Еще один способ состоит в том, что легализаторы за счет подставных лиц в обменных пунктах банков покупают и продают иностранную валюту за рубли, продают валюту одного государства за валюту другого. Если проводится обмен валют, то это оформляется в виде документа, подтверждающего источник получения средств. Кроме вышеперечисленных, легализаторы используют такой способ, как заключение договора кредита. Получение большой суммы кредита в банках позволяет преступникам обеспечить его возврат средствами, которые были получены преступным путем. Этот способ реализуют вместе с сотрудниками банков, иногда, возможно, службы безопасности банков.

В.В. Сухонос придерживается мнения о том, что эти преступления совершаются во многих случаях организованными группировками, большинство из которых действует в трансграничном пространстве. Они преступным путем выкачивают ресурсы из украинской экономики и отмывают их за рубежом, в оффшорных зонах. Потом капитал возвращается в Россию, но преступники уже выступают в роли иностранных инвесторов. Это еще раз свидетельствует о сложности расследования указанных преступлений, а отсутствие надлежащих методических разработок еще более усложняет его[51].

География легализации средств в сфере банковской деятельности имеет свои особенности. Подобные уголовные правонарушения наиболее распространены в восточных регионах, где сконцентрирован основной производственный и финансовый потенциал.

Относительно характеристики лиц, совершающих указанные преступления, можно сказать следующее: подавляющее их количество — это руководители, бухгалтеры и другие должностные лица субъектов хозяйствования, а также служащие различных звеньев. Около 40 % — женщины, 70 % — лица в возрасте 30 лет и старше, около 40 % имеют высшее образование, 35 % — среднее, менее 3 % — лица, повторно совершившие преступление. Лица, совершающие преступления в теневом секторе экономики, в основном:

- значительно старше по возрасту лиц, совершающих общеуголовные преступления (28–45 лет — 82,3 %);

- большинство являются гражданами России (73,5 %);

- как правило, имеют положительные социальные характеристики, т.е. в целом положительно характеризуются по месту работы и жительства; занимают руководящие должности или те, которые связаны с допуском к работе с материальными ценностями (58,7 % виновных были руководителями предприятий, учреждений, организаций, 26,7 % — предпринимателями без образования юридического лица, 13,2 % — главными (старшими) бухгалтерами и т.п.); преимущественно женатые (76,3

[51]Сухонос В.В. Легализация преступных доходов в банковской сфере и борьба с ней // Правовой вестник академии банковского дела. 2012. № 1 (6). С. 1.

%);

- в большинстве случаев с высшим образованием (75,3 %), повышают уровень образования путем обучения в магистратуре (12,3 %) или получения второго высшего образования (23,6 %), чаще юридического или экономического;

- по характеру — целеустремленные, уравновешенные и волевые, к уголовной ответственности большинство из них не привлекались (87,4 %), за исключением дисциплинарной или административной; от 20 до 25 % совершают преступления в составе группы[52].

Уголовная ответственность представляет собой элемент уголовного правоотношения, в рамках которого она образуется, реализуется и прекращается. Предусмотренные санкцией УК дополнительные наказания, наряду с основными, позволяют суду в полной мере реализовать индивидуальный подход при назначении наказания виновному. Индивидуализация наказания иногда используется для обозначения процесса формирования приговора с целью достижения конкретных исправительных задач правосудия.

Противодействием легализации средств являются разнообразные меры финансового мониторинга, что предусматривает осуществление общегосударственного и внутрибанковского надзора за проведением финансовых операций. Директива 2005/60/ЕС Европейского парламента и Совета Европейского союза «О предупреждении использования финансовой системы с целью отмывания средств и финансирования терроризма»[53] направлена на предупреждение таких преступлений и обязует банки, агентов по недвижимости и др. предоставлять отчеты об использовании денежных средств в сумме свыше 15 тыс. евро.

В зависимости от особенностей организации деятельности банков и с учетом рисков, связанных с клиентами и их операциями, банки разрабатывают программы с целью противодействия легализации средств. Основным программами являются:

- осуществление идентификации и изучение клиентов банка («знай своего клиента»);

- выявление в деятельности клиентов сомнительных операций, которые подлежат обязательному контролю, и операций с денежными средствами или другим имуществом, которые могут быть связаны с легализацией средств, полученных преступным путем;

- проверка информации о клиенте или его операциях для подтверждения обоснованности или опровержения подозрения о том, что

[52]Алиев Я.Л., Вихров А.А., Сальников П.П. Теневая экономика и организованная преступность в социальной системе России // Правовое поле современной экономики. – 2015. № 1. С. 31-43.

[53]Directive 2005/60/EC of the European Parliament and of the Council of the European Union of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing. URL: http://eurlex.europa.eu/LexUriServ/LexUriServ. do?uri=OJ:L:2005:309: 0015:0036:EN:PDF (дата обращения: 20.07.2017).

клиент намеревается отмыть средства, полученные преступным путем;

- проведение документального фиксирования информации, необходимой для идентификации клиента и совершаемых им операций;

- сохранение информации и документов, полученных в результате реализации программ осуществления внутреннего контроля, с целью противодействия легализации (отмыванию) средств, полученных преступным путем;

- обучение сотрудников банка способам противодействия легализации (отмыванию) средств, полученных преступным путем.

Банкам необходимо предоставлять отчеты о подозрительных операциях, чтобы иметь достаточно информации о проведенных банковских операциях и клиентах с целью своевременного установления подозрительных действий. Это требует, чтобы банк «знал» своих клиентов, а именно владельца счета, какими операции клиента должны быть, источники его доходов. Как только установлена соответствующая информация о клиенте и необходимые в конкретном случае банковские операции, представители банка готовы определить, являются ли действия клиента подозрительными. На банки возложена большая ответственность, так как они являются субъектами первого уровня мониторинга и должны принимать меры внутреннего контроля.

Среди методов, которые обеспечивают стабильное функционирование банковской системы и дают возможность эффективно бороться с так называемыми экономическими преступлениями, необходимо отметить следующие:

- тесное сотрудничество банковского сектора и государственных органов с ведущими международными финансовыми учреждениями, положительный опыт которых возможно использовать в России;

- принятие единых правил, обеспечивающих равные условия работы для банков и предотвращение оттока клиентов;

- использование банками международных бухгалтерских стандартов, что позволит обеспечить прозрачное отображение информации на счетах клиентов[54].

В 2015 году одним из приоритетных направлений совершенствования законодательства в сфере ПОД/ФТ являлось обеспечение доступа всех субъектов исполнения Федерального закона № 115-ФЗ “О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма” к информации о лицах, в отношении которых указанными субъектами были реализованы полномочия по отказу от заключения договора банковского счета (вклада), отказу в выполнении распоряжения клиента о совершении операции, а также по расторжению

[54]Алиев Я.Л., Вихров А.А., Сальников П.П. Теневая экономика и организованная преступность в социальной системе России // Правовое поле современной экономики. 2015. № 1. С. 31-43.

договора банковского счета (вклада)[55]. Доступ к указанной информации позволит финансовым организациям более качественно оценивать риски, связанные с приемом на обслуживание и обслуживанием недобросовестных хозяйствующих субъектов.

Таким образом, следует отметить необходимость дальнейшего совершенствования законодательно-нормативной базы по вышеуказанному вопросу, что может состоять в значительном реформировании соответствующих положений УК РФ. Также проведенный анализ осуществления легализации средств подтверждает необходимость разработки методических рекомендаций по расследованию уголовных дел указанной категории. Практика свидетельствует, что методика предупреждения преступлений в сфере банковской деятельности требует новых научных подходов и современных знаний о способах совершения указанных деяний, поскольку банковская сфера обеспечивает жизнедеятельность предприятий, организаций и в целом всего государства.

[55] О внесении изменений в Федеральный закон «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»:Федеральный закон от 30.12.2015 № 424-ФЗ: URL: http://www.consultant.ru/document/cons_doc_LAW_191473/. (дата обращения: 20.07.2017).

ЗАКЛЮЧЕНИЕ

Безопасность банка (банковская безопасность) - совокупность внешних и внутренних условий банковской деятельности, при которых потенциально опасные для банковской системы и отдельного банка действия (бездействия) или обстоятельства (риски и угрозы) предупреждены, пресечены либо сведены к такому уровню, при котором не способны нанести ущерб установленному порядку банковской деятельности (функционированию банка, сохранению и воспроизводству имущества и инфраструктуры банковской системы или отдельного банка) и воспрепятствовать достижению банком уставных целей. Надежность обеспечения безопасности банка оценивается по степени уязвимости от рисков и угроз защищаемых элементов его имущества и инфраструктуры.

Банковский риск - мера допустимых (риск с выгодой) или недопустимых (риск с потерей) опасных условий деятельности банка, неблагоприятные последствия которых возникают вследствие ошибочных или неосторожных действий (решений) или бездействия персонала и клиентов банка. Основной источник правового регулирования отношений, связанных с рисками, - гражданское, трудовое и административное законодательство. Угроза безопасности банка - уголовно или административно наказуемое умышленное противоправное деяние (действие либо бездействие), посягающее на имущественные и приравненные к ним права и интересы банка либо на порядок его функционирования. Угрозы – главный источник опасности для банка.

Объекты противоправного посягательства – это имущество банка или наличные и безналичные деньги, иностранная валюта, валютные ценности и ценные бумаги; имущественные права на объекты банковской деятельности (финансовые, кредитные и иные активы, предметы залога), а также здания, оборудование и инвентарь. Банковские технологии - упорядоченная совокупность функционально и информационно взаимосвязанных операций, действий, работ и процедур, обеспеченных необходимыми ресурсами (финансовыми, материальными, техническими, информационными, программно-математическими, кадровыми).

Система безопасности банка - совокупность действий уполномоченных лиц и структурных подразделений кредитной организации, реализующих своими силами и средствами меры правового (нормативного), организационного, технического и криминалистического характера в целях защиты имущества, инфраструктуры и порядка функционирования кредитной организации от противоправных посягательств. Главные структурные элементы системы безопасности банка - его службы безопасности (защиты интересов банка), внутреннего контроля и аудита. Организационные элементы - совокупность локальных нормативных документов банка, определяющих структуру, полномочия и ответственность персонала.

Задачи службы безопасности банка включают разработку и осуществление системы мер по предупреждению и пресечению

противоправных посягательств на интересы банка; выявление признаков готовящихся и совершенных противоправных посягательств на интересы банка и принятие мер по их предупреждению и пресечению; осуществление взаимодействия с правоохранительными органами, оказание им содействия в проведении предусмотренных законом мероприятий следственного, розыскного и профилактического характера; участие в уголовном и административном преследовании виновных в посягательстве на интересы банка в соответствии с законодательством РФ.

Организационные методы обеспечения безопасности банка включают в себя специальные методы осуществления управленческой, финансовой, коммерческой, кадровой и иной функциональной деятельности банка, имеющие целью предупредить причинение ущерба как в результате умышленных и неосторожных противоправных действий, так и вследствие ошибки.

Криминалистическая характеристика противоправного посягательства – это система описания присущих тому или иному виду посягательства особенностей, позволяющих обеспечить эффективное предупреждение, пресечение и расследование этих посягательств и обусловливающих применение соответствующих методов, приемов и средств. Элементы криминалистической характеристики: предмет противоправного посягательства; типичные способы совершения и сокрытия посягательства; обстоятельства подготовки и совершения посягательства (время, место, условия, участники и т.п.); характерные механизмы следообразования; типология личности виновного и потерпевшего.

Основу эффективности деятельности по обеспечению безопасности банка составляет процесс поиска, получения, накопления, анализа и использования необходимой информации. Качество информационного процесса является основным критерием оценки профессионализма службы безопасности банка и ее отдельных работников.

СПИСОК ЛИТЕРАТУРЫ

Нормативные правовые акты

1. Конституция Российской Федерации: принята всенародным голосованием 12.12.1993: с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 N 6-ФКЗ, от 30.12.2008 N 7-ФКЗ, от 05.02.2014 N 2-ФКЗ, от 21.07.2014 N 11-ФКЗ // Собрание законодательства РФ. - 2014. - N 31. - Ст. 4398.

2. О банках и банковской деятельности: Федеральный закон от 2 декабря 1990 г. N 395-I // Ведомости съезда народных депутатов РСФСР. 1990. - N 27. - Ст. 357.

3. О несостоятельности (банкротстве) кредитных организаций: Федеральный закон от 25 февраля 1999 г. N 40-ФЗ// Собрание законодательства Российской Федерации. - 1999. - N 9. - Ст. 1097.

4. О Центральном банке Российской Федерации (Банке России): Федеральный закон от 10 июля 2002 г. N 86-ФЗ// Собрание законодательства Российской Федерации. - 2002. - N 28. - Ст. 2790.

5. О страховании вкладов физических лиц в банках Российской Федерации: Федеральный закон от 23 декабря 2003 г. N 177-ФЗ// Собрание законодательства Российской Федерации. - 2003. - N 52 (часть I). - Ст. 5029.

6. О полиции: Федеральный закон от 07.02.2011 N 3-ФЗ: ред. от 18.06.2017// Официальный интернет-портал правовой информации.URL: http:// www.pravo.gov.ru, 18.06.2017, N 0001201706180007.

7. О национальной платежной системе: Федеральный закон от 25.12.2012 №267-ФЗ: .ред. от 18.07.2017 //Официальный интернет-портал правовой информации.URL: http:// www.pravo.gov.ru, 19.07.2017, N 0001201707190012.

8. Об оперативно-розыскной деятельности: Федеральный закон от 12 августа 1995 г. №144-ФЗ:.ред. от 06.07.2016 г.// Официальный интернет-портал правовой информации.URL: http:// www.pravo.gov.ru, 07.07.2016, N 0001201607070016.

9. О персональных данных: Федеральный закон от 27.07.2006 № 152-ФЗ// Официальный интернет-портал правовой информации.URL: http:// www.pravo.gov.ru, 03.07.2016 № 0001201607030010.

10. О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма: Федеральный закон от 07.08.2001 №115-ФЗ: ред. от 24.10.2016// КонсультантПлюс: ВерсияПроф. (дата обращения: 20.07.2017).

11. О внесении изменений в Федеральный закон «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»: Федеральный закон от 30.12.2015 № 424-ФЗ URL:http://www.consultant.ru/document/cons_doc_LAW_191473/. (дата обращения: 20.07.2017).

12. О частной детективной и охранной деятельности:Закон РФ от 11 марта 1992 г. 2487-I в ред. от 3.07.2016//Официальный интернет-портал

правовой информации URL: http:// www.pravo.gov.ru, 03.07.2016, N 0001201607030004.

13. О Стратегии национальной безопасности Российской Федерации:Указ Президента Российской Федерации от 31 декабря 2015 года N 683. URL:https://rg.ru/2015/12/31/nac-bezopasnost-site-dok.html. (дата обращения 20.07.2017).

14. Концепция долгосрочного социально-экономического развития Российской Федерации на период до 2020 года: утв. распоряжением Правительства Рос. Федерации от 17 нояб. 2008 г. № 1662-р. URL:http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=law;n=90601 (дата обращения: 20.07.2017).

15. Доктрина информационной безопасности Российской Федерации: утв. Указом Президента РФ от 05.12.2016 №646// Официальный интернет-портал правовой информации. URL: http://publication.pravo.gov.ru/Document/View/0001201612060002 (дата обращения 20.07.2017).

16. О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств (с изменениями на 14 августа 2014 года): Положение ЦБ РФ от 9.06.2012 года N 382-П. URL: http://base.garant.ru/70191962/ (дата обращения 20.07.2017).

17. Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных: Приказ Федеральной службы по техническому и экспортному контролю от 18.02.2013 № 21Официальный интернет-портал правовой информации. URL: http://www.consultant.ru/document/cons_doc_LAW_146520/ (дата обращения 20.07.2017).

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

19. О Стратегии развития банковского сектора Российской Федерации на период до 2020 года: распоряжение Правительства РФ №2043-р от 29.12.2008. URL: http://base.garant.ru/. (дата обращения: 20.07.2017).

20. Положение об эмиссии платежных карт и об операциях, совершаемых с их использованием: утв. Банком России 24.12.2004 № 266-П:зарегистрировано в Минюсте России 25.03.2005 № 6431 // Вестник Банка России. 2005.№ 17.

Материалы судебной практики

21. О судебной практике по делам о краже, грабеже и разбое: постановление Пленума Верховного Суда РФ от 27.12.2002 № 29 // Российская газета. 2003.18 января.

22. Приговор Верхнепышминского городского суда от 21 февр. 2012 г. по уголовному делу № 1-

50/12.URL:http://docs.pravo.ru/document/view/22393765/ (дата обращения: 20.07.2017).

23. Приговор Верхнепышминского городского суда от 7 июня 2011 г. по уголовному делу № 1-152/11.URL:http://docs.pravo.ru/document/view/18392970/ (дата обращения: 20.07.2017).

24. Приговор Кировского районного суда г. Кемерово, Кемеровской области от 12.11.2015. Дело № 1-395/15. URL:http://sudact.ru/regular/doc/Y1E4KZB0MKoV/(дата обращения: 20.07.2017).

25. Приговор Ленинского районного суда г. Новосибирска от 08.12.2015. Дело № 1-1128/2015.URL:http://sudact.ru/regular/doc/F5Kun42Viw5w/(дата обращения: 20.07.2017).

Специальная литература

26. Авдеев В.А. Проблемы реализации уголовной ответственности / В.А. Авдеев // Известия Иркутской государственной экономической академии. — 2016. — № 5 (50). — С. 50–54.

27. Акимов В. Оценка и прогноз стратегических рисков: теория и практика/ В.Акимов // Право и безопасность. - 2014. - №1.

28. Алиев Я.Л., Вихров А.А., Сальников П.П. Теневая экономика и организованная преступность в социальной системе России/Я.Л.Алиев, А.А.Вихров, П.П.Сальников// Правовое поле современной экономики. – 2015. – № 1. – С. 31-43.

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

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

31. Васюков С.В. Предупреждение преступлений, совершаемых в сфере проведения безналичных расчетов, проводимых с использованием банковских карт:автореферат диссертации на соискание ученой степени кандидата юридических наук на тему: Специальность12.00.08 - Уголовное право и криминология; уголовно-исполнительное право. М., 2013. 25 с.

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

33. Вехов В.Б. Особенности расследования преступлений,совершённых с использованием пластиковых карт и их реквизитов/В.Б.Вехов.- Волгоград: ВА МВД России, 2005. - 276 с.;

34. Волеводз А.Г. Финансовые механизмы легализации (отмывания) денежных средств, полученных преступным путем, связанные с их переводом за границу / А.Г.Волеводз// Банковское право. – 2012. - № 3. – С. 64-77.

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

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

37. Добрынин Ю. Классификация преступлений, совершаемых в сфере компьютерной информации / Ю.Добрынин. - URL: http://www.russianlaw.net/law/computer_crime/a158/ (дата обращения: 20.07.2017).

38. Зубков В.А. Международные стандарты в сфере противодействия отмыванию преступных доходов и финансированию терроризма:учебное пособие/ В.А.Зубков, С.К.Осипов. - М.: Международный учебно-методический центр финансового мониторинга, 2013.

39. Козловский В. Масштабы кибермошенничества растут/ В.Козловский//Российская газета. 2012. 29нояб. URL: http://www.rg.ru/2012/11/29/karti-site.html, свободный.(дата обращения: 20.07.2017).

40. Конвенция Совета Европы об отмывании, поиске, аресте и конфискации доходов, полученных преступным путем, и о финансировании терроризма. URL: http:// search.ligazakon.ua/l_doc2.nsf/link1/MU05399.html. (дата обращения: 20.07.2017).

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

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

43. Криминалистика / под ред. Н.П. Яблокова. - М.: Норма: ИНФРА-М, 2010.

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

45. Официальный сайт Центрального Банка Российской Федерации.- URL: https://www.cbr.ru/.(дата обращения 20.07.2017).

46. Попова Н. Российские банкоматы оказались в ливанской петле/Н.Попова//АН-online. – 2012. –11 фев. – URL: http://argumenti.ru/crime/2012/02/156477, свободный.(дата обращения: 20.07.2017).

47. Смольянинова Е.Н., Фурманов Д.В. Проблемы безопасности расчетов при использовании пластиковых карт/Е.Н.Смольянинова, Д.В.Фурманов//Актуальные вопросы экономических наук. - 2012. - № 24-2. - С. 46–50.

48. Сухонос В.В. Легализация преступных доходов в банковской сфере и борьба с ней / В.В. Сухонос // Правовой вестник Академии банковского дела. — 2012. — № 1 (6).

49. Федотов Н.Н. Форензика–компьютерная криминалистика/Н.Н.Федотов. - М.:Юрид.мир, 2007. - 359 с.

50. Филиппов М.Н. Расследование краж и мошенничеств,совершённых с использованиембанковских карт и их реквизитов: автореф. дис. … канд. юрид. наук/ М.Н.Филиппов.- М., 2012. - 30 с.

51. Хилюта В.В. Момент окончания хищения: практика применения теоретический концепций / В.В.Хилюта// Вестник Брянского государственного университета. Сер. 3. 2010. № 3.

52. Щербакова Г.Н. Анализ и оценка банковской деятельности (на основе отчетности, составляемой по российским и международным стандартам) /Г.Н. Щербакова.- М.: Вершина, 2012. 464 с.

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

54. Directive 2005/60/EC of the European Parliament and of the Council of the European Union of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing. URL: http://eurlex.europa.eu/LexUriServ/LexUriServ. do?uri=OJ:L:2005:309: 0015:0036:EN:PDF. (дата обращения: 20.07.2017).

55. President’s Commission on Organized crime. The each connection, 1984.