Мошенничество в платежной сфере

Бизнес-энциклопедия

Коллектив авторов
Алексей С. Воронин

Мошенничество в платежной сфере. Бизнес-энциклопедия

Серия «Библиотека Центра исследований платежных систем и расчетов»

Издательский текст
http://www.litres.ru/pages/biblio_book/?art=14981155
Мошенничество в платежной сфере. Бизнес-энциклопедия: Центр исследований платежных систем и расчетов. Интеллектуальная Литература; М.; 2016
ISBN 978-5-9907223-2-3

Аннотация

Активное использование информационных технологий в платежной сфере привело к появлению разнообразных специфических форм мошенничества, основанных на применении достижений современных ИТ. Мошенничество с банковскими картами, электронными деньгами и при обслуживании клиентов в системах дистанционного банковского обслуживания; способы борьбы с противоправными действиями

злоумышленников; вопросы нормативного регулирования – эти и многие другие аспекты данной проблематики рассматриваются в бизнес-энциклопедии «Мошенничество в платежной сфере».

Все материалы для книги подготовлены практикующими специалистами – экспертами в финансово-банковской сфере.

Авторы: Леонид Лямин, Николай Пятиизбянцев, Антон Пухов, Павел Ревенков, Илья Сачков, Валерий Баулин, Дмитрий Волков, Максим Кузин, Ирина Лобанова. Редактор-составитель, руководитель проекта Алексей Воронин. Менеджер по рекламе Елена Балакшина.

Содержание

Коллектив авторов Мошенничество в платежной сфере. Бизнес-энциклопедия

Предисловие

Платежная сфера – важнейшая область экономики и жизни социума в целом. А поскольку современная социальная жизнь во всех ее проявлениях – и бизнес, и личный план, и медийное пространство – все более базируется на информационных технологиях, вполне ожидаемо в сторону ИТ мутировали и способы мошенничества и его инструменты. Эволюционировало и само преступное сообщество, создавшее настоящую мошенническую индустрию, собственный рынок, на котором можно купить не только специальный инструментарий, но и заказать взлом любой системы или массированную атаку на тот или иной информационный ресурс. Поэтому информационная безопасность, защита информации становится все более острой проблемой, требующей особого внимания со стороны здоровых общественных сил. Различным аспектам обеспечения информационной безопасности, методам противодействия преступлениям в платежной сфере и посвящена бизнес-энциклопедия «Мошенничество в платежной сфере».

Представляем авторский коллектив книги с указанием наименований разделов, написанных каждым из авторов:

• *Леонид Лямин* (начальник отдела электронных банковских технологий департамента банковского надзора Банка России) – «Использование современных форм платежей для

легализации преступных доходов и организация противодействия»;

• *Николай Пятиизбянцев* (начальник отдела по управлению инцидентами департамента защиты информации Газпромбанка) – «Уголовно-правовые аспекты борьбы с противоправными деяниями в сфере банковских карт», «Гражданско-правовые вопросы в случае несанкционированного использования платежных карт», «Безопасность банкоматов»;

• *Антон Пухов* (директор по развитию Центра исследований платежных систем и расчетов) – «Процедуры минимизации рисков при работе с платежными картами»;

• *Павел Ревенков* (д.э.н., профессор кафедры экономического анализа и бухгалтерского учета Одинцовского гуманитарного университета) – «Электронные платежи: риск возможного использования для легализации преступных доходов»;

• *Илья Сачков* (генеральный директор Group-IB), *Валерий Баулин* (руководитель лаборатории компьютерной криминалистики и исследования вредоносного кода Group-IB), *Дмитрий Волков* (руководитель отдела расследования инцидентов информационной безопасности Group-IB) – «Практика мошенничества в системах ДБО», «Распространенные виды мошенничества в сфере электронных денег» (в *соавторстве*);

• *Максим Кузин* (главный архитектор продукта БПЦ) –

«Методы и инструменты оценки рисков на базе мониторинга карточных транзакций»;

• *Ирина Лобанова* (руководитель департамента исследований банковского сектора Национального агентства финансовых исследований) – «Исследование опыта и осведомленности населения по мошенничеству в сфере платежных карт».

С уважением,
Алексей Воронин,
руководитель проекта, редактор-составитель (ЦИПСиР)

Глава 1
Мошенничество в системах дистанционного банковского обслуживания (ДБО) и электронных денег

1.1. Практика мошенничества в системах ДБО

Рост количества и сумм безналичных операций естественно привлек внимание сначала компьютерной, а потом уже организованной преступности к этому рынку.

Первые масштабные хищения начались в России в 2007 г. Когда суммы хищений стали достигать миллионов долларов, участники преступных групп, которые занимались обналичиваем денежных средств, привлекли внимание организованной преступности, так как на «обнал» уходили очень крупные суммы и процент за вывод денежных средств мог достигать 50 %.

Анализ работы больших преступных групп, задержанных в 2011–2013 гг., показывает, что это большие, хорошо ор-

ганизованные формирования, которым сложно противостоять даже юридически-уголовным путем. Такие факторы, как огромные доходы, несовершенство законодательства и возможности обналичивания денежных средств привели к росту на 100–200 % в год этого типа преступлений. Анализ технических и организационных методов данных преступлений является первостепенной необходимостью для борьбы с этим явлением.

В данной главе представлена необходимая информация, позволяющая специалистам в области безопасности финансовых операций получить основной набор знаний для противодействия подобным типам инцидентов. Глава написана ведущими экспертами-криминалистами Group-IB, которые принимали участия в большинстве резонансных расследований в РФ и СНГ.

В цивилизованном мире регулятором прав и обязанностей, ограничений и мер принуждения является закон. Однако появление и активное развитие информационно-коммуникационных технологий и сферы компьютерной информации доказали обществу, насколько рабочим может быть принцип ubi jus incertum, ibi nullum («если закон не определен – закона нет»).

Этот принцип можно применить к ситуации с разделом законодательства, регулирующим сферу компьютерной информации в РФ: пробелы в действующих законах, отсутствие понятийного аппарата или его некорректное обозначе-

ние препятствуют должному применению закона или не допускают его вовсе.

Используя пробелы в законодательстве, ошибки в реализации программного обеспечения и применяя простейшие способы социальной инженерии, мошенникам удалось украсть в сфере интернет-банкинга $ 446 млн (результаты получены из ежегодного отчета компании Group-IB за 2013 г.). Общее количество похищенных денежных средств за 2013 г. представлено на рисунке 1.1.

Рис. 1.1. *Оценка объемов рынка киберпреступности в РФ, категория «интернет-мошенничество»*

Мошенничество в системах дистанционного банковского обслуживания основано на получении несанкционированно-

го доступа к пользовательской информации, необходимой для работы и авторизации.

Принципиально методы совершения хищения денежных средств различаются способом получения доступа к ключам электронно-цифровой подписи (ЭЦП) для авторизации в системе ДБО: инсайд или злонамеренные действия третьих лиц (внешнего злоумышленника).

Остановимся более подробно на наиболее распространенных методах совершения преступлений, связанных с системами ДБО.

Инсайд. В случае сговора сотрудников, имеющих доступ к системе ДБО, или по инициативе одного сотрудника, проводятся операции, как правило платежи с использованием легитимных ключей и аутентификационных данных. Также инсайдер может завладеть ключами ЭЦП и логином/паролем как физически, например в случае несоблюдения сотрудниками компании правил политики парольной защиты, так и с помощью применения специализированного программного обеспечения для слежки за действиями пользователей (кейлоггер) на автоматизированном рабочем месте.

Лица, имеющие доступ к данным аутентификации в системе ДБО, это чаще всего: бухгалтер, генеральный директор, системный администратор, а также любой сотрудник, имеющий доступ к ПК, с которого производится работа с системой ДБО.

Внешний злоумышленник действует с помощью спе-

циализированных вредоносных программ, которые зачастую недоступны широкой массе людей. Выбор вредоносной программы злоумышленником зависит от того, как будет происходить подтверждение платежа (с помощью SMS-сообщения или электронного носителя с заранее записанным сертификатом), в каком банке находится клиент и какими возможностями должна обладать вредоносная программа.

Внешние злоумышленники для совершения хищений денежных средств используют следующие популярные способы распространения вредоносных программ: электронную почту, покупку загрузок и эксплуатацию уязвимостей на тематических сайтах. Рассмотрим особенности каждого из способов.

Электронная почта. Данный метод актуален для проведения целевых «заражений», когда у злоумышленника имеются адреса электронных почт лиц, работающих с системой интернет-банкинга. Схема распространения следующая:

• злоумышленник готовит электронное письмо с вложением. В тексте письма указываются причины для открытия файла, прилагаемого к письму. Например, с просьбой проверки документов финансовой отчетности (в частности, актов сверки);

• после открытия файла из вложения вредоносная программа устанавливается в систему и сообщает на удаленный сервер злоумышленника свой статус об успешной установке («отстукивается»);

• злоумышленник проверяет на сервере появление новых событий от распространяемых им программ.

Покупка загрузок. Данный метод является одним из самых простых, но наименее эффективных, поскольку установленные таким способом вредоносные программы быстро удаляются и зачастую продавцы не могут обеспечить требуемую целевую аудиторию. Схема распространения следующая:

• злоумышленник ищет лиц, у которых уже имеется сеть зараженных компьютеров с загруженной и установленной вредоносной программой (бот-сеть);

• владелец зараженной бот-сети дает необходимому количеству компьютеров команду на загрузку вредоносного программного обеспечения, которое он получил от злоумышленника;

• вредоносная программа загружается и запускается, а затем сообщает на удаленный сервер злоумышленника свой статус об успешной установке;

• злоумышленник проверяет на сервере появление новых событий от распространяемых им программ.

Эксплуатация уязвимостей на тематических сайтах. Данный метод является наиболее эффективным, поскольку дает возможность осуществлять массовое распространение вредоносного программного обеспечения, а также вы-

бирать целевую аудиторию для распространения. Схема распространения следующая:

• осуществляется компрометация тематического сайта (например, buhgalter.ru);

• в сайт встраивается вредоносный код (iframe), который вместе с содержимым сайта загружает вредоносные компоненты;

• при посещении пользователями такого сайта осуществляется анализ установленных компонентов (браузера и его плагинов) и их версий в системе. В случае обнаружения осуществляется загрузка и запуск заданной вредоносной программы;

• после запуска вредоносной программы на удаленный сервер злоумышленника сообщается статус об успешной установке;

• злоумышленник проверяет на сервере появление новых событий от распространяемых им программ.

Изображение панели управления связки эксплойтов Black Hole показано на рисунке 1.2. Основным параметром, характеризующим связку эксплойтов, является коэффициент «пробива» – это отношение количества загрузок вредоносной программы к количеству пользователей/хостов, посетивших вредоносную ссылку. На изображении коэффициент «пробива» равен 15,1 % за весь период его использования.

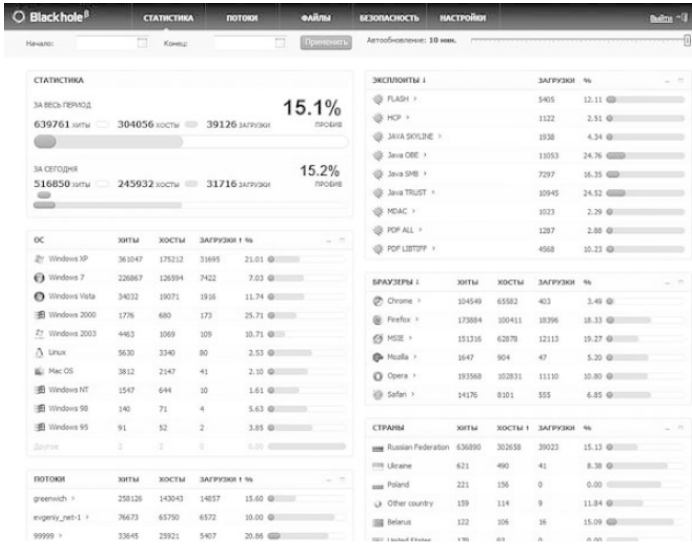

Рис. 1.2. *Панели управления связки эксплойтов Black Hole*

Наиболее приоритетными программными компонентами (плагинами) для эксплуатации уязвимостей являются: Java, Flash, Internet Explorer и Adobe Acrobat Reader.

Компанией Group-IB приведена обзорная статистика уязвимостей веб-приложений, полученная в ходе оказания услуг по аудиту информационной безопасности и проведения тестов на проникновение в 2012 г. и в I квартале 2013 г. Стоит отметить, что в ходе проводимых исследований оценивалась защищенность не только целевого приложения, но и всей инфраструктуры, в рамках которой было развернu-

то целевое приложение. Таким образом, поверхность атаки включала в себя всё стороннее ПО, а также компоненты, используемые веб-приложением и размещенные на одной с приложением площадке.

Чаще всего специалистами Group-IB выявлялись уязвимости, связанные со следующими недостатками:

- недостаточная проверка входных данных;
- раскрытие чувствительной информации;
- использование паролей недостаточной сложности.

По результатам отчета компании Group-IB за 2013 г. (http://report2013.group-ib.ru/), самые распространенные уязвимости в компонентах, используемые злоумышленниками, представлены на рисунке 1.3.

В результате успешного использования вредоносных программ все дальнейшие действия злоумышленников будут направлены на закрепление в системе, дальнейшее хищение ключевой информации, а также получение удаленного управления компьютером.

Существуют две основные схемы, с помощью которых осуществляется кража денежных средств: специализированное вредоносное программное обеспечение, похищающее пароли, сертификаты, ключи ЭЦП, и фишинг.

В настоящее время можно выделить несколько основных способов совершения хищений в системах ДБО при помощи вредоносных программ, рассмотрим их далее.

Рис. 1.3. *Статистика уязвимостей приложения, используемых злоумышленниками*

Троянская программа на компьютере жертвы. Самый распространенный способ. Возможно хищение из любого банка, как у юридических, так и у физических лиц, а также проведение платежа в автоматическом режиме (автозалив). Блок-схема, пошагово описывающая процесс совершения хищений, представлена на рисунке 1.4.

Троянская программа на компьютере жертвы для перенаправления на фишинговый сайт. В данном случае троянская программа используется только для перенаправления пользователей на фишинговый сайт. Применяется для хищения денежных средств только у физических лиц. Данный способ зачастую требует осуществить звонок пользователю зараженной машины. Блок-схема, пошагово описывающая процесс совершения хищений, представлена на

рисунке 1.5.

Троянская программа на компьютере жертвы – перевыпуск SIM-карты. Способ аналогичен двум предыдущим. Отличием является лишь то, что злоумышленник осуществляет перевыпуск SIM-карты, используя фальшивые документы и доверенность. Блок-схема, пошагово описывающая процесс совершения хищений, представлена на рисунке 1.6.

Троянская программа на компьютере и мобильном устройстве жертвы. Наименее популярный способ. В основном он предназначен для хищения денежных средств у физических лиц. Блок-схема, пошагово описывающая процесс совершения хищений, представлена на рисунке 1.7.

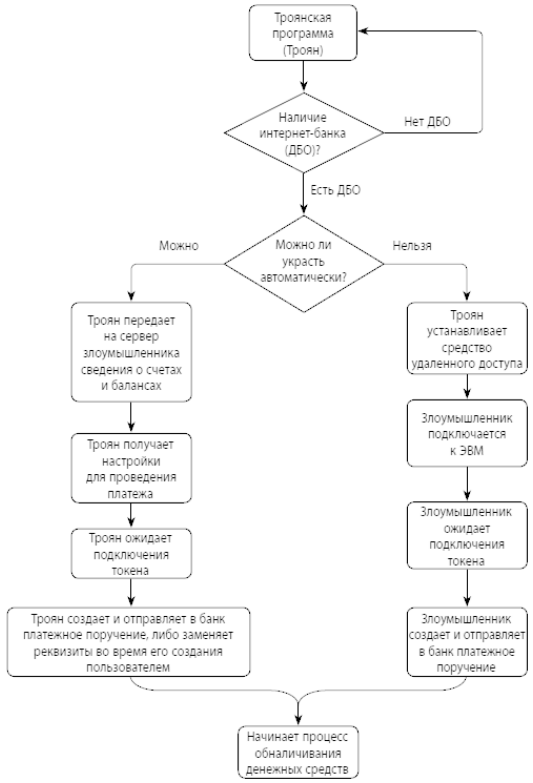

Рис. 1.4. *Блок-схема хищения денежных средств с помощью троянской программы*

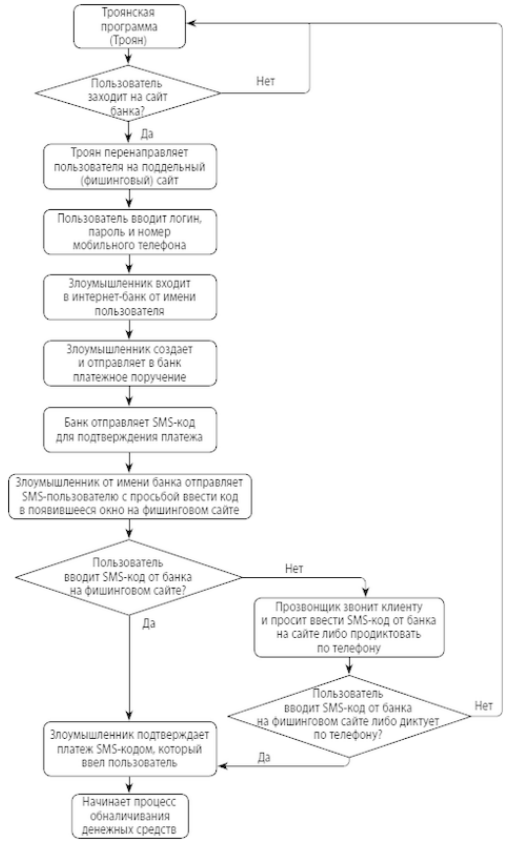

Рис. 1.5. *Блок-схема хищения денежных средств с помощью троянской программы* (*фишинговый сайт*)

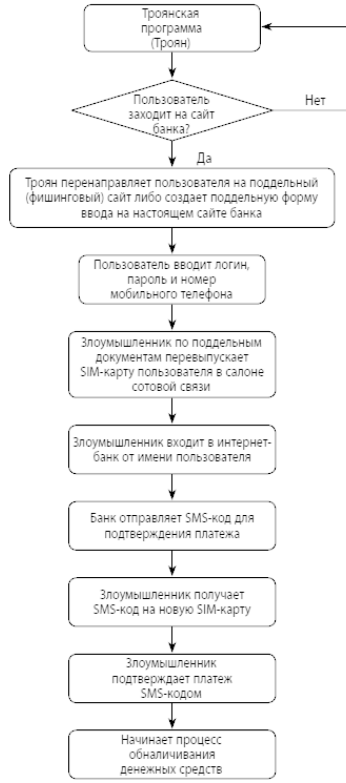

Рис. 1.6. *Блок-схема хищения денежных средств с помощью троянской программы, перевыпуск SIM-карты*

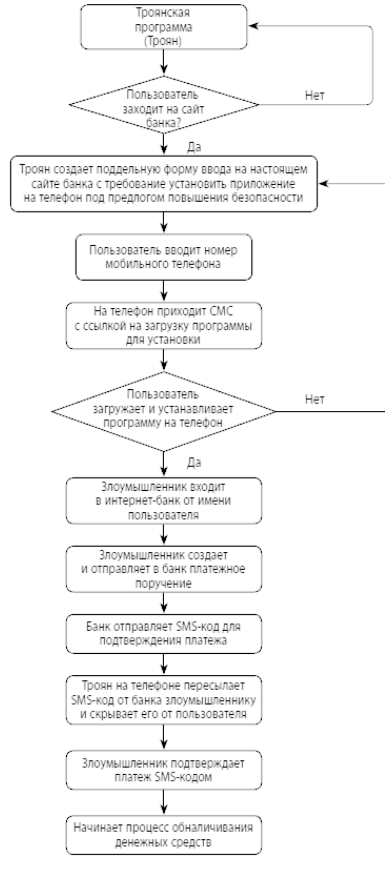

Рис. 1.7. *Блок-схема хищения денежных средств с помощью троянской программы на компьютере и мобильном устройстве*

Троянская программа на мобильном телефоне

жертвы.

В основном данный способ направлен на хищение денежных средств у физических лиц либо у банков, поддерживающих перевод денег по SMS. Размер хищений ограничен лимитами банка на проведение таких операций. Блок-схема, пошагово описывающая процесс совершения хищений, представлена на рисунке 1.8.

Троянская программа на мобильном телефоне жертвы – фишинговый сайт. Используется для хищений денежных средств у физических лиц любого банка. Отличается от предыдущего способа тем, что нет таких жестких лимитов, как для SMS-банкинга. Блок-схема, пошагово описывающая процесс совершения хищений, представлена на рисунке 1.9.

Компрометация системы банка. Данный способ наиболее сложный и редко встречается на практике. Хищение возможно как со счетов самого банка, так и со счетов клиентов этого банка. Блок-схема, пошагово описывающая процесс совершения хищений, представлена на рисунке 1.10.

Процесс обналичивания похищенных денежных средств является завершающей стадией хищения. Он, как правило, выполняется преступной группой, не входящей в состав той, которая похитила денежные средства с банковского счета. Если процесс обналичивания успешно завершен, то группе, которая похитила денежные средства с банковского счета, возвращается от 40 до 60 % от обналиченной суммы. Про-

цент зависит от условий работы и оговаривается в начале взаимодействия.

На рисунке 1.11 представлено несколько основных вариантов движения денежных средств в зависимости от похищаемой суммы. Однако схема может быть представлена значительно сложнее, если процессом обналичивания занимаются несколько разных групп и единовременный объем хищений, как правило, более 5 млн рублей.

1.2. Российский рынок электронных денег

Чтобы получить представление о механизмах мошеннических схем и методах борьбы с ними в сегменте электронных денег, необходимо рассмотреть подробнее этот рынок, а также поведение и «портрет» пользователей электронных кошельков.

Рис. 1.8. *Блок-схема хищения денежных средств с помощью троянской программы на мобильном устройстве*

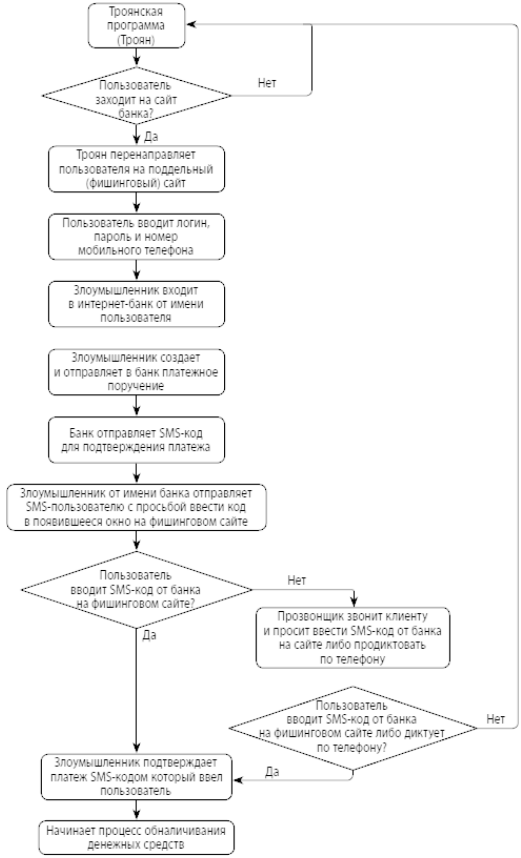

Рис. 1.9. *Блок-схема хищения денежных средств с помощью троянской программы на мобильном устройстве* (*фишинговый сайт*)

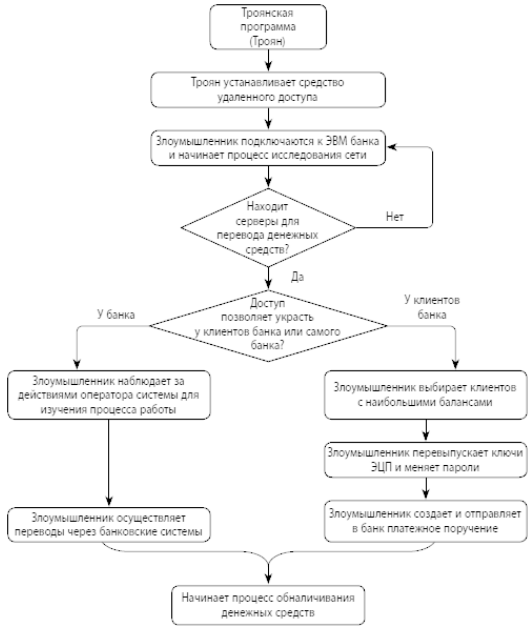

Рис. 1.10. *Блок-схема хищения денежных средств через компрометацию системы банка*

Российский рынок электронных денег демонстрирует устойчивый рост: по данным J'son & Partners Consulting, в первом полугодии 2014 г. объем платежей, проходящих через российские электронные платежные сервисы, вырос на 38 % по сравнению с тем же периодом прошлого года. Эксперты прогнозируют дальнейшее увеличение числа пользователей онлайн-кошельков, рост количества и размера тран-

закций. Это обусловлено целым рядом причин.

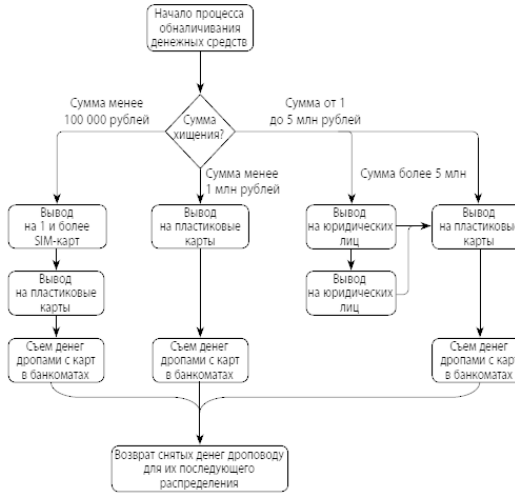

Рис. 1.11. *Процесс обналичивания похищенных денежных средств*

Во-первых, рост доли крупных платежей через электронные кошельки, таких как погашение кредитов, денежные переводы, платежи за ЖКУ и пр. Технологии онлайн-платежей становятся привычными для пользователей и доверие к ним растет.

Во-вторых, активно развивается онлайн-торговля: российский рынок интернет-коммерции – один из самых быстрорастущих в мире. Причем текущая экономическая ситу-

ация в России может явиться и стимулирующим фактором для его дальнейшего развития. С одной стороны, многие компании сфокусируются на онлайн-реализации, чтобы снизить издержки: уже сейчас многие компании, чья продукция традиционно продавалась в обычных торговых сетях, активно продвигают собственные онлайн-площадки. С другой, покупатели будут более взвешенно подходить к выбору нужных товаров. Интернет-магазины и аукционы предоставляют широкие возможности для поиска наиболее экономичных вариантов, к которым можно также отнести получение скидок и участие в акциях. Так, 24 % онлайн-покупателей пользуются скидочными купонами. Онлайн-шопинг открывает и возможности покупок за рубежом: 40 % интернет-покупателей делали заказы в зарубежных магазинах.

Вместе с тем растет финансовая грамотность населения. Уже сейчас электронными деньгами при оплате интернет-покупок пользуется почти каждый четвертый покупатель из нашей страны.

Кроме того, существенное влияние на рост объемов интернет-коммерции оказывает развитие новых технологий. Около 85 % пользователей Интернета в России пользуются мобильными телефонами для выхода в Сеть, 38 % просматривают сайты интернет-магазинов с целью покупки товара, используя мобильные устройства (данные Synovate Comcon, OnLife, ноябрь 2014 г.).

Российские платежные сервисы предлагают приложения

для всех типов мобильных устройств, через которые можно быстро и удобно оплатить покупки. Популярность смартфонов, позволяющих использовать возможности платежных приложений, быстро растет. По данным Synovate Comcon, 40 % жителей городов-миллионников являются владельцами этих гаджетов, в городах с населением от 100 000 человек аналогичный показатель достигает 32 %.

При этом жители некрупных городов активнее замещают свои телефоны более современными коммуникаторами: в 2014 г. число владельцев смартфонов выросло на 60 % по сравнению с 2013 г., в мегаполисах— на 40 % (данные Synovate Comcon, РосИндекс, 2014 г.).

Наконец, растет уровень проникновения Интернета, активно развиваются мобильные интернет-технологии. В 2014 г. доля пользователей, которые выходят в Сеть с помощью сотовых телефонов, выросла почти вдвое по сравнению с 2013 г.

Все эти факторы позволяют прогнозировать дальнейшее стабильное развитие рынка электронных денег. Кроме того, можно с уверенностью предположить, что в ближайшем будущем онлайн-торговля и электронные платежи все чаще будут производиться с использованием мобильных устройств. Следует ожидать значительного расширения ассортимента технологий и мобильных приложений, связанных с дистанционными продажами и платежами, а также совершенствования уже имеющихся.

1.3. Портрет пользователя электронных денег, потребительское поведение

Согласно результатам исследования Synovate Comcon, по состоянию на конец 2014 г. более 14 % всего населения России (от 16 до 54 лет) как минимум один раз в три месяца пользуется электронными кошельками. При этом среди активных интернет-пользователей, регулярно совершающих интернет-покупки, услугами электронных платежных систем пользуются 58 %.

Большинство пользователей электронных кошельков (47 %) живут в городах-миллионниках.

Самой многочисленной части пользователей (30 %) 25–34 года. У 55 % владельцев электронных кошельков высшее или неоконченное высшее образование.

Что же оплачивают пользователи электронными деньгами? Значительная часть владельцев электронных кошельков регулярно платит с их помощью за телекоммуникационные услуги: 53 % опрошенных сообщили, что пополняют баланс мобильного телефона, 28 % оплачивают домашний Интернет, 13 % – коммерческое телевидение. 36 % используют электронные деньги для оплаты покупок в интернет-магазинах и товаров по каталогам, 20 % оплачивают электронными

деньгами онлайн-игры.

Существенное количество пользователей совершает через электронные кошельки крупные бытовые платежи, такие как оплата ЖКУ и погашение кредитов (по 14 % опрошенных). Денежные переводы и перевод средств на банковские счета совершают по 21 % владельцев электронных кошельков.

Отдельно стоит выделить сервис перевода денег между кошельками – его используют 23 % опрошенных. Эта возможность активно набирает популярность как легкий и быстрый способ передать деньги в любой удобный момент.

На российском рынке представлено несколько электронных платежных сервисов. Согласно данным опроса пользователей, при выборе определенного электронного кошелька главную роль играет доверие. Это наиболее важный атрибут имиджа любой марки электронных способов оплаты, сильнее всего влияющий на ее общую оценку. В то же время доверие – это собирательное понятие, состоящее в первую очередь из таких характеристик марки, как соответствие своим пользователям («для таких людей, как я»), намерение рекомендовать («я буду рекомендовать эту марку друзьям»), соотношение цены и качества услуг («предлагает оптимальное соотношение цены и качества услуг»), надежность и стабильность сервиса, безопасность платежей («обеспечивает максимальную безопасность и защищенность моих платежей»).

Если спросить пользователей напрямую, какой из пере-

численных атрибутов для них важен при выборе электронного способа оплаты (по 10-балльной шкале), 73 % пользователей различных электронных платежных систем утверждают, что безопасность и защищенность платежей – это наиболее важный признак (оценки 9 и 10 высказыванию «обеспечивает максимальную безопасность и защищенность моих платежей»). Безопасность – это один из ключевых параметров, влияющих на общую оценку (входит в топ-10 атрибутов по влиянию на общую оценку).

Отсюда можно сделать вывод о том, что в категории электронных кошельков безопасность платежей должна быть превыше всего. При этом важно не только гарантировать защищенность и безопасность платежей при помощи электронного кошелька, но и реально ее обеспечивать, пресекая мошенничество и использование электронных кошельков незаконно.

1.4. Схемы мошенничества, способы информирования пользователей и методы профилактики

Мошеннические схемы в сфере электронных денег условно можно разделить на технические и «социальные» – рассчитанные на доверчивость пользователей.

Платежные сервисы совместно с ведущими отечественными и международными компаниями разрабатывают и внедряют алгоритмы предотвращения мошеннических операций с использованием электронных платежных средств. Помимо этого, они постоянно совершенствуют внутренние многоуровневые системы безопасности, позволяющие анализировать все операции в системе, выявлять подозрительные действия и оперативно принимать соответствующие меры. В частности, критериями определения подозрительных операций могут быть нетипичные признаки поведения электронного счета: другие IP-адреса, смена физического устройства, с которого происходит авторизация, нехарактерные транзакции для этого счета и пр.

Комплекс технических мер, внедряемый платежными сервисами для обеспечения безопасности электронных кошельков, минимизирует вероятность хищения средств с использованием уязвимостей сервиса.

Устройства владельцев электронных кошельков в этом плане гораздо более уязвимы, и платежные сервисы регулярно информируют клиентов о ряде правил, которые нужно соблюдать для обеспечения безопасности средств.

1.4.1. Вредоносное ПО

Ряд вредоносных программ, нацеленных на похищение паролей пользователей и получения доступа к электронным кошелькам, проникает на пользовательские компьютеры и мобильные устройства.

Вирусные программы для смартфонов могут перехватывать SMS-сообщения, так что под угрозу попадают все платежные приложения, где реализована функция платежей с помощью SMS-команд.

Единственные способы защиты от вредоносных программ – установить и регулярно обновлять антивирусное ПО, не скачивать программы из непроверенных источников, не запускать незнакомые приложения, загруженные из Интернета. О троянских программах и правилах безопасности осведомлено большинство пользователей электронных кошельков, но эта мошенническая схема до сих пор продолжает работать.

1.4.2. Фишинг

Не менее распространенная мошенническая схема – это хищение персональных данных с помощью фишинговых сайтов: клиент переходит по ссылке на поддельный сайт платежного сервиса, где ему предлагается ввести свои данные. Указав на таком сайте логин, пароль и любую другую конфиденциальную информацию, пользователь фактически предоставляет злоумышленникам доступ к своим средствам.

Чтобы отличить поддельный от оригинального сайта, достаточно внимательно посмотреть его название в адресной строке.

Оно обычно написано неправильно, с подменой одного или нескольких знаков. Все сайты или их разделы, на которых указывается конфиденциальная информация, используют безопасный протокол передачи данных https, защищенный от мошенников. При этом в адресной строке браузера присутствует символ «замок». Если браузер выдает предупреждение, что сертификату безопасности сайта нельзя доверять, пользователю необходимо немедленно покинуть этот сайт.

Для обеспечения безопасности электронных кошельков платежные сервисы внедрили ряд опций, таких как SMS-подтверждения платежей и других значимых действий с электронным кошельком, а также привязка электронного ко-

шелька к e-mail. Используя эти сервисы, клиенты получают возможность в случае компрометации личных данных оперативно выявлять признаки попыток доступа к электронным средствам и принимать меры: смену пароля, обращение в службу безопасности платежного сервиса. Пароли для электронных кошельков должны быть уникальными (то есть не повторяться на других ресурсах) и достаточно сложными.

1.4.3. Методы, рассчитанные на доверие пользователей

По данным Synovate Comcon, для 70 % активных интернет-пользователей определяющим критерием выбора онлайн-магазина является выгодная стоимость товаров. Пользуясь стремлением покупателей сэкономить, злоумышленники создают поддельные сайты или группы в социальных сетях, предлагая товары по низкой цене и указывая в качестве средства оплаты электронные деньги. Оформляя предоплату на подобных ресурсах, покупатели рискуют как минимум получить некачественный товар, а то и остаться и без покупки, и без средств.

Не реже происходят случаи, когда фальшивые «продавцы» в телефонном разговоре предлагают покупателю создать и пополнить электронный кошелек. Далее, пользуясь неопытностью покупателя, провоцируют его сообщить пароль и таким образом получают доступ к средствам пользо-

вателя.

Существуют и так называемые методы социальной инженерии, когда злоумышленник связывается с владельцем электронного кошелька под видом сотрудника какой-либо организации – например, технического специалиста сотового оператора. Под различными предлогами (проверка корректности работы сервиса, подтверждение личности владельца для проведения транзакции и пр.) он может спровоцировать пользователя на компрометацию паролей – в телефонном разговоре, по SMS или e-mail.

В правилах безопасности платежных сервисов содержится предупреждение о том, что пользователь никому не должен сообщать пароли и одноразовые коды. То же самое напоминание, как правило, приходит в сервисных SMS-сообщениях от системы.

Относительно новый способ мошенничества появился с развитием сервиса выставления счетов между пользователями интернет-кошельков. Злоумышленник может выставить счет на сравнительно небольшую сумму, сопроводив его комментарием о том, что это оплата комиссии или сервисный сбор за какие-либо услуги. Такие поддельные счета легко определить по реквизитам отправителя – как правило, это незнакомое частное лицо.

Наконец, давно известные, но продолжающие работать поддельные розыгрыши ценных призов от имени известных компаний. Мошенники предлагают оплатить с помощью

электронных денег «налог на выигрыш» или стоимость пересылки приза. Пользователям необходимо проверять информацию о подобных выигрышах, обращаясь за подтверждением к предполагаемому организатору.

Кроме того, не следует доверять различным лотереям и финансовым пирамидам, организованным в Интернете.

1.5. Распространенные виды мошенничества в сфере электронных денег

Как известно, электронные деньги как платежное средство, используемое при оплате товаров (услуг) и имеющее такую же ценность, как и настоящие деньги, появилось сравнительно недавно. Тем не менее электронные деньги сразу же обратили на себя пристальное внимание мошенников, поскольку имеют несколько явных преимуществ перед классическим мошенничеством с настоящими деньгами. Во-первых, завладение электронными деньгами происходит удаленно. Мошенник и его жертва могут находиться на расстоянии сотен и тысяч километров друг от друга. Во-вторых, система электронных денег сегодня дает преимущественно большую анонимность получателю денег. И, в-третьих, этими системами пользуются огромное количество технически безграмотных людей.

Наиболее популярными схемами мошенничества с использованием электронных денег являются:

• **Фальшивые письма и фишинговые сайты.** Основная цель фишинговых писем – заставить получателя перейти по ссылке на поддельный (фишинговый) сайт, где будут украдены учетные данные его электронного кошелька. Та-

кие письма тщательно маскируют под официальное письмо той платежной системы, которой пользуется получатель. При переходе по ссылке в письме происходит попадание на поддельную страницу, сходную со страницей платежной системы. Но уже при вводе учетных данных профиля осуществляется передача логина и пароля мошенникам, которые в дальнейшем получат доступ к самому кошельку.

• «**Волшебные кошельки**» **и другие пирамиды.** На одном из многочисленных форумов помещается сообщение, в котором приводится список электронных кошельков (обычно три-семь штук) и настоятельно рекомендуется отправить $ 1 на каждый из них. Затем предлагается продублировать это сообщение и разместить его на более чем 200 форумах. При этом в списке номеров кошельков вместо последнего необходимо поставить свой номер. Далее приводится подробный расчет, как в течение двух-пяти месяцев на электронный кошелек попадет многократно умноженная сумма. Эта мошенническая схема преследует одну цель – забрать деньги всех участников сразу. В эту категорию также входят письма со следующим содержанием: «Я работал в системе (указывается платежная система) и случайно узнал, что существуют специальные кошельки. Если на них послать некоторую сумму денег, то они возвращают деньги отправителю в трехкратном размере. Меня несправедливо уволили, и чтобы отомстить им, я даю номер одного из кошельков». Главная их цель и итог – незаконный увод денег.

• **Генераторы.** Мошенники предлагают программное обеспечение, которое, по их утверждению, позволит увеличить сумму на кошельке в n раз и без уплаты взносов. После установки такой программы происходит потеря всех денег, находившихся на кошельке.

• **Компьютерный шантаж.** Данный тип мошенничества зачастую происходит в результате посещения сайта, который заражен вредоносным программным обеспечением. Пользователь включает свой компьютер и видит сообщение-окно со следующим содержанием: «Не пытайтесь убрать программу с вашего компьютера, так как можете его повредить. Чтобы возобновить его работу, отправьте SMS **** со следующем содержанием ******** два раза, и мы вышлем вам код доступа для разблокировки системы». Очевидно, что при отправке SMS с мобильного счета абонента произойдет только списание существенной суммы. Встречаются случаи, когда вредоносное программное обеспечение, проникая в систему, осуществляет шифрование файлов определенного расширения (doc, docx, pdf, файлы электронной почты, файлы базы 1С, MySQL, MSSQL и др.). Дальнейшая цель – выманить у пострадавшего денежные средства в обмен на ключ для дешифрования файлов.

• **Поддельные обменные пункты.** Продавцы утверждают, что с их помощью можно обменять WMZ на WMR (или наоборот) по выгодному курсу и без уплаты каких-либо процентов. Никакого обмена не происходит: зачастую мошен-

ники указывают, что на сайте проводятся технические работы и требуется время на осуществление обмена. Но в итоге ничего не происходит и жертва остается ни с чем.

Глава 2
Электронные платежи: риск возможного использования для легализации преступных доходов

Прежде чем приступить к рассмотрению проблематики, напомним о ее актуальности в цифрах – согласно данным Управления ООН по наркотикам и преступности, объем незаконной деятельности, включая чисто экономические преступления, ежегодно составляет порядка $2,1 трлн. Это примерно 3,6 % мирового ВВП, из которых ежегодно «отмывается» примерно $1,6 трлн[1]. По оценкам Банка России, в 2012 г. объем вывода капитала за рубеж по сомнительным основаниям составил $39 млрд, за девять месяцев 2013 г. – около $22 млрд[2].

---

[1] См. подробнее: Чиханчин Ю.А. Международное сотрудничество в сфере борьбы с легализацией доходов, полученных преступным путем, и финансированием терроризма как фактор укрепления глобальной и региональной безопасности // Финансовая безопасность. № 1. Июнь 2013 г.

[2] Из выступления Председателя Банка России Э.С. Набиуллиной на конференции «Актуальные вопросы реализации государственной политики в сфере противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» 18 декабря 2013 г. (http://cbr.ru/pw.aspx?file = /press/press_centre/Nabiullina_18122013. htm).

2.1. Общая модель отмывания денег

Процедура легализации преступных доходов (другими словами – отмывание денег) имеет решающее значение для деятельности практически всех форм транснациональной и организованной преступности. Это функция присуща практически всем действиям по созданию прибыли преступными сообществами[3]. Она способствует коррупции, деформирует процесс принятия экономических решений, усугубляет социальные проблемы и подрывает финансовые институты. Банковская система способна быстро и в любом объеме перемещать финансовые средства практически в любую точку мира и поэтому стала весьма привлекательна для криминальных структур и, как следствие, особенно уязвима.

Одними из основных факторов, способствующих беспрепятственному осуществлению легализации преступных доходов, являются:

– несовершенство механизмов контроля и мониторинга за деятельностью финансовых институтов, несоблюдение международных стандартов регулирования финансовой деятельности, разработанных специализированными международ-

[3] Уголовный кодекс США содержит больше 100 статей, нарушение которых относится к категории преступлений, связанных с отмыванием денег. Эти преступления охватывают области деятельности от торговли наркотиками и финансового мошенничества до похищения и шпионажа. В Уголовном кодексе Российской Федерации подобных статей значительно меньше.

ными организациями;

– распространение коррупции среди государственных исполнительных, правоохранительных и судебных органов власти;

– невозможность или ограничение возможности обмена финансовой информацией с иностранными правоохранительными органами.

Различные меры экономического характера, призванные исключить или ограничить возможность использования преступниками приобретенных незаконными путями доходов, представляют собой важнейший компонент программ по борьбе с преступностью.

Одна из самых распространенных (встречающаяся как в отечественных, так и в зарубежных источниках) схема отмывания денег включает три стадии: размещение (placement), расслоение (layering) и интеграция (integration). Указанные стадии могут осуществляться одновременно или частично накладываться друг на друга – это зависит от разработанного механизма легализации и от требований, предъявляемых преступной организацией.

На стадии размещения (placement) необходимо изменить форму денежных средств с целью сокрытия их нелегального происхождения. Например, поступления от незаконной торговли наркотиками чаще всего представляют собой мелкие купюры. Конвертирование их в более крупные

купюры, чеки или иные финансовые документы часто производится с помощью предприятий, имеющих дело с большими суммами наличных денег (рестораны, гостиницы, казино, мойки машин), используемых в качестве прикрытия. Ответственным сотрудникам финансовых учреждений, в чьи обязанности входит осуществление мер, направленных на противодействие легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма (ПОД/ФТ), необходимо хорошо представлять, что легче всего выявлять противозаконные операции на стадии размещения. В связи с этим в кредитных организациях на вооружении риск-подразделений, служб внутреннего контроля и подразделений (отдельных сотрудников), занимающихся ПОД/ФТ, должны быть необходимые методики для выявления источников рисков, связанных с отмыванием денег.

На стадии расслоения (layering) лица, отмывающие деньги, стараются еще больше замести следы, по которым их могут обнаружить. Для этого одни сложные финансовые сделки наслаиваются на другие. Например, для отмывания больших денежных сумм создаются фиктивные компании в странах, отличающихся строгими законами о банковской тайне или слабыми механизмами обеспечения соблюдения законодательных положений, касающихся отмывания денег. Затем «грязные» деньги переводятся из одной фиктивной компании в другую до тех пор, пока не приобретут видимость законно полученных средств.

Вышеупомянутые операции должны быть замаскированы так, чтобы в конечном счете раствориться в совершаемых каждый день законных сделках. Общепринятыми техническими приемами здесь служат различные варианты выдачи «обратных ссуд»[4] и «двойного выставления счет-фактур»[5].

Другие технические приемы наслоения связаны с покупкой дорогостоящих предметов (ценных бумаг, легковых автомобилей, самолетов и яхт), которые часто записываются на имя другого человека (с целью еще больше отдалить преступника от нелегально полученных средств). В последнее время на данной стадии стали активно использоваться технологии ДБО и системы, осуществляющие электронные платежи (рис. 2.1). Отличие заключается в том, что при ДБО клиентов требуется открытие банковского счета, а электронные платежи могут совершаться без открытия банковского счета (например, системы мобильных платежей позволяют производить платежи со счета мобильного телефона).

---

[4] При использовании обратной ссуды преступник вкладывает деньги в офшорное предприятие, находящееся под его тайным контролем, а затем «ссужает» сам себе сумму вложенных им средств. Этот технический прием срабатывает, поскольку в некоторых странах трудно определить, кто на самом деле контролирует счета.

[5] Двойное выставлении счет-фактуры. Это мошенническая уловка ввоза (или вывоза) средств в ту или иную страну, где одно из офшорных предприятий ведет двойную бухгалтерию. Чтобы ввезти «чистые» деньги в другое государство, некое предприятие в стране назначает завышенную цену на определенный товар или услугу. Для вывоза средств (например, чтобы избежать уплаты налогов) предприятию выставляется завышенная счет-фактура.

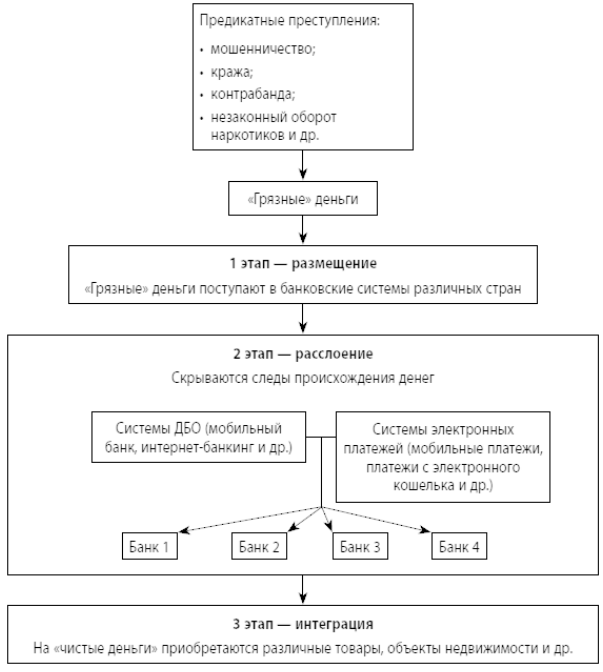

***Рис. 2.1**. Обобщенная схема отмывания денег с использованием технологии ДБО и систем, осуществляющих электронные платежи*

На стадии интеграции (integration) преступники пытаются трансформировать денежные доходы, полученные от противозаконной деятельности, в средства, имеющие внешне легальное происхождение (деньги обычно вкладываются

в бизнес, недвижимость, покупку драгоценностей и др.).

Поскольку процесс отмывания денег в определенной степени полагается на существующие финансовые системы и операции, то выбор преступниками конкретных механизмов ограничивается лишь их изобретательностью. Деньги отмываются через валютные и фондовые биржи, торговцев золотом, казино, компании по продаже автомобилей, страховые и торговые компании. Частные и офшорные банки, подставные корпорации, зоны свободной торговли, электронные системы и торгово-финансовые учреждения – все эти структуры могут скрывать незаконную деятельность.

Операции, связанные с отмыванием денег, способны значительно увеличить риск потери репутации для финансовых учреждений, **негативно влиять на курсы валют и процентные ставки.** В конечном счете эти деньги поступают в глобальные финансовые системы, где могут подрывать экономику и валюту отдельных стран, создавая серьезную угрозу для национальной и международной безопасности. В результате происходит **подрыв целостности финансовых рынков,** при котором финансовые институты, полагающиеся на доходы от преступных деяний, сталкиваются с дополнительными трудностями, стремясь адекватно управлять своими активами, обязательствами и операциями. Например, крупные суммы отмытых денег могут поступить в финансовое учреждение, но затем внезапно бесследно исчезнуть через электронные переводы в ответ на такие неры-

ночные факторы, как операции правоохранительных органов. Это может привести к проблемам с ликвидностью и перегрузкам в банках.

В некоторых странах с формирующейся рыночной экономикой незаконные доходы могут намного превосходить государственные бюджеты, что **приводит к утрате правительственного контроля над экономической политикой.** В ряде случаев огромная база активов, накопленная за счет отмывания денег, может использоваться для спекулятивной скупки рынков или даже целой экономики небольшой страны.

Операции, связанные с легализацией незаконно полученных доходов, могут также **отрицательно влиять на валюты и процентные ставки,** поскольку лица, отмывающие свои доходы, реинвестируют средства в те области, где менее вероятно раскрытие их схем, а не в те, где выше норма отдачи.

Операции, направленные на отмывание денег, **снижают налоговые доходы правительства** (тем самым наносят косвенный ущерб честным налогоплательщикам). Как правило, данная потеря доходов означает более высокие ставки налогообложения по сравнению с нормальной ситуацией, при которой преступные доходы были бы законными и облагались налогами. Следует отметить, что отмывание денег может проходить в форме приватизации. Преступники располагают финансовыми средствами, позволяющими давать за

предприятия, прежде находившиеся в государственной собственности, более высокие цены, чем легальные покупатели. Приватизационные инициативы часто бывают экономически выгодными, они могут также служить механизмом отмывания денег.

Для стран, участвующих в отмывании денег, возникает риск потери репутации. Его значимость возрастает в условиях современной глобальной экономики. Различные финансовые преступления (мошенничество в крупных размерах, хищения посредством операций с ценными бумагами на основе внутренней информации о деятельности компании-эмитента и др.) подрывают доверие к рынкам, а прибыль перестает быть показателем экономических возможностей. Создающаяся вследствие этого негативная репутация препятствует устойчивому росту экономики и одновременно привлекает международные преступные организации с сомнительной репутацией, преследующие краткосрочные цели. Для восстановления финансовой репутации страны необходимо вложение значительных государственных ресурсов, что можно было бы осуществить путем надлежащего контроля над отмыванием денег.

Рост количества операций, направленных на отмывание денег, ведет к увеличению государственных расходов на правоохранительные органы (создание специализированных подразделений) и здравоохранение (например, лечение наркотической зависимости) для преодоления возникающих се-

рьезных последствий.

Большинству финансовых транзакций свойственен некоторый след, однозначно привязывающий сумму к конкретной персоне. Преступники избегают использовать традиционные платежные системы типа чеков, кредитных карточек и т. д. именно в силу наличия этого следа. Они предпочитают использовать наличность (так как это анонимно). Физическая наличность имеет весьма существенные неудобства, связанные с большим объемом и массой[6], поэтому лица, специализирующиеся на отмывании денег, стараются использовать различные способы перемещения денежных средств, где можно избежать жестких требований к идентификации. И системы электронных платежей стали для них в какой-то степени просто находкой.

[6] Например, 44 фунта (примерно 20 кг) кокаина стоят около $1 млн. Вес наличности суммой $1 млн равен 256 фунтам (примерно 116 кг). Наличность почти в шесть раз превышает вес наркотиков.

2.2. Электронные платежи

За последние несколько лет системы электронных платежей (в том числе проводимые с помощью планшетов и смартфонов[7]) получили широкое распространение в развитых европейских и американских странах. В настоящее время данная технология расчетов стала активно использоваться в Африке и Азии. В своей основе электронные платежи базируются на платежных системах, поддерживающих электронную передачу наличных средств. Передача наличности в системах этого класса может осуществляться с использованием глобальной сети Интернет или с помощью физического перемещения высокономинальных смарт-карт с записанным значением наличной суммы денег. Новые технологии оплаты предназначены в основном для замены наличных денег в розничной торговле, а также в сделках уровня потребителя.

В силу эффективности и простоты, с которой они заменяют наличность, системы электронных платежей несут в себе и новые риски, связанные с правовым обеспечением сделок. В результате возникают проблемы, которые должны быть разрешены в процессе развития систем этого класса, позво-

[7] По данным Российского отделения ЮС, во II квартале текущего года было поставлено около 1 960 000 планшетов, что, по оценкам ЮС, более чем вдвое превосходит аналогичный прошлогодний показатель (см. подробнее: Колесов А. Российский компьютерный рынок как отражение экономической ситуации/PC Week/RE. № 20. 20 августа 2013 г.).

ляющих гарантировать обнаружение и предотвращение проведения операций, направленных на легализацию преступных доходов.

Риски возможного использования систем электронных платежей для легализации преступных доходов – тема не новая. Еще в сентябре 1995 г. FinCEN[8] провело семинар по данной проблеме в Юридическом институте города Нью-Йорк. Далее в мае 1996 г. сотрудники FinCEN совместно с Национальным университетом обороны провели масштабные учения по отработке действий, связанных с выявлением незаконных операций по отмыванию денег, проводимых с использованием систем электронных платежей. В ходе этих учений отрабатывался ряд возможных сценариев использования систем электронных платежей для совершения незаконных операций.

Особенностям электронной оплаты также было уделено пристальное внимание со стороны Группы разработки финансовых мер борьбы с отмыванием денег (ФАТФ[9]), которая

---

[8] Управление по борьбе с финансовыми преступлениями (Financial Crimes Enforcement Network – FinCEN) было создано в 1990 г. Основная задача – содействие правоохранительным органам США в борьбе с легализацией доходов от криминальной деятельности как на национальном, так и на международном уровне.

[9] Международная организация Financial Action Task Force (FATF), созданная в 1989 г. странами «Большой семерки». Сейчас в ФАТФ входит более 30 государств. Российская Федерация является членом ФАТФ с июня 2003 г. 30 июня 2013 г. Норвегия передала России председательство в этой организации. Утверждение российской заявки на 2013–2014 гг. означало, что Россия находилась на

является межправительственным органом. Мандат ФАТФ предусматривает установление стандартов и содействие эффективному применению правовых, регулирующих и оперативных мер по борьбе с отмыванием денег, финансированием терроризма и финансированием распространения оружия массового уничтожения и иными связанными угрозами целостности международной финансовой системы. В сотрудничестве с другими заинтересованными международными участниками ФАТФ также работает над определением уязвимых мест на национальном уровне с целью защиты международной финансовой системы от злоупотреблений.

Рекомендации ФАТФ устанавливают комплексную и последовательную структуры мер, которые странам следует применять для противодействия отмыванию денег и финансированию терроризма, а также финансированию распространения оружия массового уничтожения. Страны имеют различные правовые, административные и оперативные структуры и различные финансовые системы, в связи с чем они не могут принимать идентичные меры по противодействию этим угрозам. Странам следует адаптировать к своим конкретным условиям Рекомендации ФАТФ, (представляющие собой международные стандарты) и на их основе разработать меры для того, чтобы:

– определять риски, связанные с недостатками в органи-

хорошем счету и имела высокий рейтинг своей антиотмывочной системы. Через год в права председателя вступила Австралия.

зации мер по противодействию легализации преступных доходов, разрабатывать единую политику по выполнению принятых мер и осуществлять координацию внутри страны между различными организациями;

– преследовать отмывание денег, финансирование терроризма и финансирование распространения оружия массового уничтожения;

– применять превентивные меры для финансового сектора и других установленных секторов;

– устанавливать полномочия и ответственность компетентных органов (например, следственных, правоохранительных и надзорных органов) и иные институциональные меры;

– укреплять прозрачность и доступность информации о бенефициарной собственности юридических лиц и образований;

– обеспечивать международное сотрудничество.

Первые 40 рекомендаций ФАТФ были разработаны в 1990 г. как инициатива по защите финансовых систем от лиц, отмывающих денежные средства, вырученные от продажи наркотиков. Затем они изменялись, дополнялись и в настоящее время содержат положения, имеющие прямое отношение к новым технологиям и электронным платежам (Рекомендации 15, 16). Так, в частности, в Рекомендации 15 упоминается, что странам и финансовым учреждениям

необходимо определять и оценивать риски отмывания денег или финансирования терроризма, которые могут возникать в связи с разработкой новых продуктов. В Рекомендации 16 указано, что странам необходимо обеспечить, чтобы финансовые учреждения включали требуемую и точную информацию об отправителе и получателе в электронный перевод и сопровождающие сообщения, а также чтобы эта информация сопровождала электронный перевод или передаваемое сообщение по всей цепочке платежа. Данная рекомендация была разработана с целью предотвращения свободного доступа террористов и других преступников к системам, осуществляющим электронные платежи. В частности, она призвана обеспечить, чтобы основная информация об отправителе и получателе электронных переводов была незамедлительно доступна:

– соответствующим правоохранительным органам и (или) органам прокуратуры для использования ими при выявлении, расследовании деятельности террористов, их преследовании, отслеживании их активов;

– подразделениям финансовой разведки для проведения анализа подозрительной или необычной деятельности отдельных лиц и организаций;

– отправляющим, транзитным и получающим финансовым учреждениям для облегчения идентификации и направления сообщений о подозрительных операциях (сделках), а также для выполнения требований предпринять действия

по замораживанию и соблюдению запретов на проведение операций (сделок) с установленными лицами и организациями в соответствии с обязательствами, изложенными в соответствующих резолюциях Совета Безопасности ООН (таких как резолюция 1267 (1999) и резолюциях в ее развитие и резолюция 1373 (2001), относящихся к предупреждению и предотвращению терроризма и финансирования терроризма).

Рекомендация 16 применяется к трансграничным и внутренним электронным переводам, в том числе серийным платежам[10] и платежам с маршрутной инструкцией[11].

Классические кредитные или дебетовые карты позволяют их владельцам купить товары и услуги без использования наличных денег, но при этом расчеты проходят при по-

---

[10] Серийный платеж относится к прямой последовательной цепочке оплаты, когда электронный перевод и сопровождающее его сообщение о платеже поступают вместе от отправляющего финансового учреждения к получающему финансовому учреждению непосредственно или через одно или более транзитных финансовых учреждений, например банки-корреспонденты (Рекомендации ФАТФ. Международные стандарты по противодействию отмыванию денег, финансированию терроризма и финансированию распространения оружия массового уничтожения / Пер. с англ. – М.: Вече, 2012.– С. 110).

[11] Платеж с маршрутной инструкцией относится к электронному переводу, который объединяет сообщение о платеже, направленное непосредственно отправляющим финансовым учреждением в получающее финансовое учреждение, с маршрутной инструкцией финансирования (сопровождение) от отправляющего финансового учреждения в получающее финансовое учреждение через одно или более транзитных финансовых учреждений (там же. С. 109).

средничестве финансового учреждения или эмитента кредитной карты (что позволяет идентифицировать владельцев карт). Основная же характеристика многих современных систем электронных платежей связана с устранением регулирующего третьего лица (например, банка) при передаче денежных средств между двумя (или более) объектами. Возможность передачи наличности через информационные сети без посредничества значительно понижает затраты на совершение сделок и создает серьезную конкуренцию коммерческим банкам.

Глобальные возможности подобных систем и тот факт, что передача наличности может иметь место с высокой скоростью и степенью анонимности, которая препятствует надлежащему контролю правительственными структурами, является серьезным поводом для беспокойства правительств ряда стран.

В анонимности платежных систем увидели угрозу после трагических событий в США 11 сентября 2001 г. В ходе проведенного тщательного расследования выяснилось, что «Аль-Каида» использовала электронные платежи для финансирования терактов[12]. Уже через несколько недель в США был принят Патриотический акт (закон, направленный на пресечение терроризма, который в числе прочего предло-

[12] См. подробнее: Королев В. Загадки 11 сентября. Почему упали башни? – М.: Вече, 2007 и Кузнецов Д. События 11 сентября 2001 года и проблема международного терроризма в зеркале общественного мнения. – М.: URSS, 2009.

жил новые инструменты борьбы с отмыванием денег). Финансовые учреждения обязали ставить в известность государство обо всех подозрительных операциях. Власти получили право запрашивать информацию о любом клиенте платежной системы. Аналогичные изменения произошли и в Европе[13].

[13] В 2001 г. Европарламент ввел требование обязательной идентификации клиентов, которое распространяется на операции, превышающие €150000.

2.3. Использование систем электронных платежей для отмывания денег

По своей природе системы электронных платежей имеют потенциал, позволяющий решить одну из самых серьезных проблем для теневого бизнеса – физическое перемещение больших количеств наличности.

Глобализация многих существующих систем электронных платежей дает возможность преступникам использовать особенности законодательства, действующего в каждом отдельно взятом государстве, а также национальные различия в стандартах защиты и правилах надзора, чтобы скрыть движение незаконных средств.

Возможному использованию систем электронных платежей для легализации преступных доходов было посвящено исследование, проведенное экспертами корпорации RAND[14].

Исследования позволили выявить множество особенностей в процессе осуществления операций в системах электронных платежей, которые правоохранительные органы

[14] RAND (англ. РЭНД – аббревиатура от Research and Development – «Исследования и разработка») – американский стратегический исследовательский центр. Является некоммерческой организацией.

должны внимательно изучить. Среди них:

– отказ от посредничества;

– банк или небанковское учреждение в качестве эмитента карт;

– операционная анонимность.

Рассмотрим каждую из них подробнее.

Отказ от посредничества. Исторически правоохранительная деятельность и организации, в чьи функции входит регулирование банковской деятельности, положились на посредничество кредитных организаций (и других регулируемых финансовых учреждений), чтобы обеспечить «точки перехвата», через которые денежные средства должны проходить и где возможно получить полный отчет об их происхождении. Отказ от посредничества фактически убирает из процесса перевода денежных средств от одного участника расчетов другому поднадзорные организации и тем самым дает возможность преступникам избежать традиционных методов отслеживания перемещения денежных средств.

Банк и небанковские учреждения в качестве эмитента карт. Банки и небанковские учреждения часто находятся в разном правовом поле и поэтому имеют различные правила для выполнения электронных платежей. В настоящее время в нескольких странах такие различия уже имеют место.

Операционная анонимность. В некоторых системах

электронных платежей, которые находятся на стадии становления, точка введения средств в систему непрозрачна и точно определить плательщика практически невозможно.

Далее рассмотрим обобщенные примеры по использованию систем электронных платежей для отмывания денежных средств.

На рисунке 2.2 приведена схема продажи наркотиков в обмен на одноразовые карточки номиналом до $100 000. Эти карточки собираются торговцем наркотиками и реализуются через подставные организации (как правило, компании, специализирующиеся на оказании различных услуг или предприятия розничной торговли). Эти организации передают данные по карточкам со своих терминалов в банк, затем переводят деньги на счет лица, которое занимается легализацией преступных доходов. Компании и предприятия, участвующие в таких схемах, получают определенную комиссию за проведение операций от организатора отмывочной схемы.

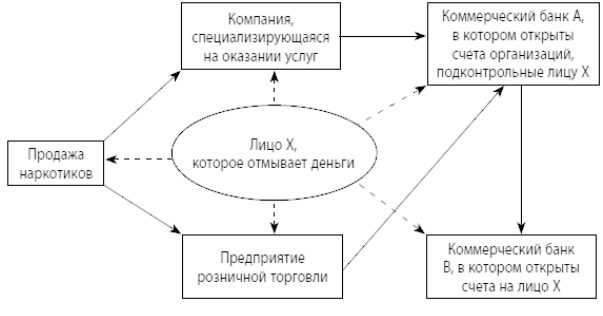

Рис. 2.2. *Схема легализации денежных средств от продажи наркотиков, с использованием одноразовых карт номиналом до $100*

Есть и другие способы реализации смарт-карт. Многие платежные системы позволяют с помощью Интернета переводить смарт-карты низкого номинала в смарт-карты высокого номинала, если в дальнейшем перед преступниками стоит задача передачи денежных средств, размещенных на смарт-картах. На рисунке 2.3 приведены два основных способа:

1) вывоз в другую страну (так как смарт-карты имеют небольшие размеры, их можно достаточно легко и надежно спрятать);

2) передача с помощью мобильного телефона (так как многие современные мобильные телефоны способны взаимодействовать с различными сервисами, выполняющими подобные операции).

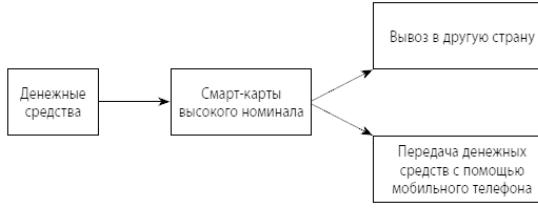

Рис. 2.3. *Схема передачи денежных средств с использова-*

нием смарт-карт высокого номинала

На рисунке 2.4 представлена схема легализации преступных доходов с использованием различных благотворительных фондов. Фонды, задействованные в подобных схемах, специально создаются совершенно для других целей, но бывают случаи, когда подобные фонды осуществляют параллельно и благотворительную деятельность. В данном случае для правоохранительных органов задача существенно осложняется, однако тщательный анализ поступающих денежных переводов и дальнейшее использование фондом денежных средств может значительно облегчить процесс выявления истинных целей создания таких фондов.

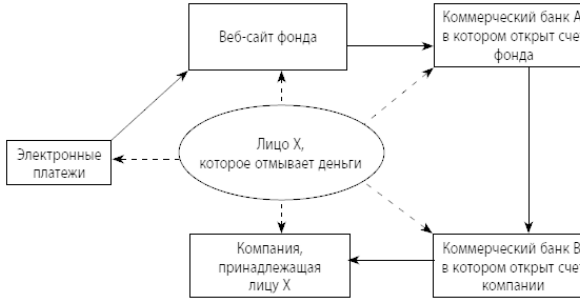

Рис. 2.4. *Схема легализации денежных средств с использованием благотворительного фонда*

2.4. Уроки Liberty Reserve

В конце мая 2013 г. прокуратура Нью-Йорка объявила о приостановке деятельности платежной системы Liberty Reserve[15]. Основанная в 2006 г. в Коста-Рике платежная система Liberty Reserve через собственную виртуальную валюту позволяла пользователям анонимно переводить денежные средства в любую точку мира за небольшую комиссию. Через систему прошло 55 млн платежей на сумму $6 млрд.

У Liberty Reserve был почти 1 млн клиентов из разных стран мира. По данным прокуроров, преступные группировки, пользовавшиеся услугами Liberty Reserve, базировались во Вьетнаме, Нигерии, Гонконге, Китае и США. Компания была «любимым банком преступного мира», говорится в обвинительном документе. Мошенников прежде всего привлекала анонимность. Для успешной регистрации, а затем проведения денежных операций было достаточно указать ад-

[15] Сайт платежной системы Liberty Reserve прекратил работу 24 мая 2013 г. Одновременно в Испании был арестован глава компании Артур Будовский, также известный как Артур Беланчук и Эрик Палц, а также финансовый менеджер платежной системы Аззедин эль-Амин. В тот же день в нью-йоркском Бруклине взяли под стражу бывшего совладельца Liberty Владимира Каца и программиста Марка Мармилева. Еще один технический сотрудник проекта, Максим Чухарев, был арестован в Коста-Рике. Двое подозреваемых, Ахмед Яссин Абдельгани и Аллан Эстебан Идальго Хименес, по-прежнему находятся в розыске. Кроме того, были закрыты еще пять сайтов и арестованы 45 принадлежавших владельцам платежной системы счетов в банках США. На них хранилось $25 млн.

рес электронной почты. Например, один из секретных агентов (как отметил прокурор Южного округа Нью-Йорка Прит Бхарара) зарегистрировался в Liberty Reserve под именем Джо Фальшивый (Joe Bogus) и дал столь же «красноречивое» имя своему счету «украсть все» (to steal everything), а свой адрес указал следующим образом: «123, Поддельная Главная Улица» в «Полностью Выдуманном Городе, США» – и его зарегистрировали[16].

Американские правоохранительные органы назвали Liberty Reserve «крупнейшим в истории отмыванием преступных денег посредством Интернета». Раньше мошенники, отмывавшие в Интернете деньги, были уверены, что здесь действует то же правило, что и в Лас-Вегасе: «То, что случается в Интернете, не выходит за пределы Интернета». Теперь так уже не скажешь…

Известная российская компания Group-IB провела свое расследование деятельности Liberty Reserve[17]. Так, по информации сотрудников компании Group-IB клиент мог сохранить инкогнито, даже перечисляя деньги из респектабельной системы вроде WebMoney, которая проверяет своих пользователей. Клиент также мог без проблем купить легально оформленный в таких системах кошелек (так называемый

---

[16] См. подробнее: Панов А. Джо Фальшивый может украсть все // Новая газета. № 58. 31 мая 2013 г.

[17] См. подробнее: Петрова С. Любимый банк криминального мира // Ведомости. № 129. 22 июля 2013 г.

аттестат[18]). В аттестате могли быть данные из украденных документов, но необязательно, так как существуют сервисы по продаже паспортных данных, которые честно куплены у владельцев документов. Людей, добровольно предоставляющих свои данные, называют «дропами» или «мулами» (их данные обычно используются для проведения сделок, приема товаров или банковских переводов, обналички и т. п.). У «дроповодов» можно было купить и электронный кошелек, привязанный к реальному банковскому счету с пластиковой картой, и с купленного счета осуществлять безналичные банковские проводки в ту же Liberty Reserve.

Liberty Reserve принимала площадки, которые ни один банк или процессинг не подключит: финансовые пирамиды, HYIP-фонды[19], продавцов ложных антивирусов и вредоносных кодов, распространителей мошеннических SMS-подписок, магазины краденых кредиток, сканов паспортов и т. п.

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

Напомним, что ранее аналогичный случай произошел с

[18] По данным А. Комарова, аттестат вместе с SIM-картой (у WebMoney транзакция подтверждается SMS) и сканом паспорта стоит обычно $150–400.

[19] HYIP (High Yield Investment Program) – мошеннические проекты, похожие на инвестиционные фонды с высокой доходностью. В основном online-проекты, которые работают с электронными валютами.

платежной системой компании E-gold. В отличие от современных электронных платежных систем E-gold была построена не на денежных единицах, привязанных к доллару или другой валюте. Вместо этого пользователям предлагалось покупать золото или другие драгоценные металлы (серебро, платину и палладий), находящиеся на хранении у компании E-gold Ltd. На пике существования система проводила транзакции на $2 млрд в год[20].

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

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

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

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

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

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

– статья 18 Свода законов США, раздел 2 (Пособниче-

[20] См. подробнее: «Криптовалютчики под колпаком» // Коммерсант-Деньги. № 27. 15 июля 2013 г.

ство, подстрекательство и соучастие в преступлении);

– статья 18 Свода законов США, раздел 982 (a) (1) (Конфискация в уголовном порядке)[21].

Спустя год генеральный директор компании Дуглас Л. Джексон признался в совершении финансовых операций без лицензии и отмывании денег. Приговор был вынесен в 2008 г. Дуглас Л. Джексон мог получить тюремный срок до 20 лет и штраф $500 000 только за участие в операциях по отмыванию, а также пять лет тюрьмы и штраф $25 000 за работу без лицензии. Однако ему присудили всего три года условного срока (включая шесть месяцев домашнего ареста), 300 часов общественных работ и штраф $200[22].

Достаточно показательны были слова начальника отдела уголовных расследований Налоговой службы США (1RS) Ричарда Вебера, который сказал, что «мы входим в виртуальную эпоху отмывания денег – если бы Аль Капоне был жив, он бы прятал деньги именно так»[23].

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

---

[21] Достов В.Л., Шуст П.М., Валинурова А. А., Пухов А. В. Электронные финансы. Мифы и реальность. – М.: КНОРУС: ЦИПСиР, 2012. – С. 133.

[22] Другие фигуранты дела отделались аналогичными наказаниями.

[23] См. подробнее: Бочкарева Т. Виртуальная прачечная // Ведомости. № 093. 30 мая 2013 г.

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

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

Отметим еще одну особенность сегодняшнего времени – значительное ослабление режима сохранения банковской тайны в рамках решения задач по противодействию отмыванию денег, финансированию терроризма и финансированию распространения оружия массового уничтожения. Согласиться с таким подходом пришлось многим странам, включая Швейцарию, где традиционно действовал порядок мак-

симального сохранения конфиденциальных сведений, составляющих банковскую тайну. Законодательство Швейцарии не содержит определения банковской тайны и перечня информации, подлежащей охране банком. Банковская тайна охватывается статьей 13 Конституции Швейцарии, защищающей право всех лиц на уважение тайны частной и семейной жизни. Эта категория включает в себя и охрану тайны источников доходов и происхождения активов, за исключением случаев, которым предшествовало совершение преступления[24].

В банковской и судебной практике банковская тайна понимается как профессиональная обязанность банкира поддерживать строжайший режим конфиденциальности в отношении любой информации о личных и финансовых обстоятельствах клиента и некоторых третьих лиц, если она была получена в ходе осуществления им профессиональной деятельности. В статье 47 Закона Швейцарии от 8 ноября 1934 г. «О банках и сберегательных кассах» (с изменениями) для лица, раскрывшего банковскую тайну, доверенную ему или полученную им как чиновником, работником, поверенным, арбитражным управляющим, должностным лицом банка, представителем Комитета по банкам, работником аудиторской компании или лица, пытающегося вовлечь третьих

[24] К таковым преступлениям относятся: уклонение от уплаты налогов (но не налоговая оптимизация), незаконное обогащение с использованием инсайдерской информации, отмывание денег и пр.

лиц в нарушение банковской тайны, предусмотрена уголовная ответственность в виде лишения свободы на срок до шести месяцев или штрафа на сумму не более 50 000 швейцарских франков. Носителям банковской тайны запрещается даже раскрывать информацию о том, что они обладают банковской тайной. Закон также устанавливает обязанность хранить банковскую тайну даже после прекращения трудового или иного договора, при этом срок действия такой обязанности не устанавливается, из чего можно сделать вывод о ее действии в течение всей жизни ее носителя[25].

На федеральном уровне в Швейцарии действует Закон от 10 декабря 1997 г. «О борьбе с отмыванием денег и финансированием терроризма в финансовом секторе» (далее – Закон о борьбе с отмыванием денег), который в 2009 г. был приведен в соответствии с Рекомендациями ФАТФ. Учитывая Рекомендацию № 4 (банковская тайна не должна влиять на применение Рекомендаций ФАТФ), Рекомендацию № 13 (обязанность банка сообщать уполномоченному органу о совершении соответствующих правонарушений), Рекомендацию № 36 (взаимная правовая помощь, не зависящая от ограничений, связанных с банковской тайной) федеральный закон налагает на финансового посредника ряд обязанностей. Так, в частности, он должен незамедлительно напра-

[25] Однако банковская тайна может быть раскрыта ее носителем в судебном порядке.

вить уведомление в уполномоченный орган[26], если знает или имеет разумные основания полагать, что финансовая операция связана с совершением преступлений, предусмотренных статьями 260ter[27] и 305bis[28] Уголовного кодекса Швейцарии[29]. Также в случае, если активы получены в результате совершения felonии[30], находятся в распоряжении организованной преступной группировки или используются для финансирования терроризма (статья 260 quinquies Уголовного кодекса Швейцарии).

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

---

[26] В соответствии со статьей 23 он подчиняется Федеральной полиции.

[27] Организованная преступная группировка – участие лица в организации, структура и состав участников которой содержатся в тайне и целью деятельности которой является совершение преступлений с применением насилия или охраны преступно нажитого имущества.

[28] Отмывание денег – совершение лицом действий по сокрытию источников приобретения, способов отчуждения и иных сделок с имуществом, полученным в результате совершения felonии, о чем он знал или должен был знать.

[29] Уведомление также необходимо направлять и в случае прекращения деловых переговоров в связи с подозрениями в совершении клиентом вышеуказанных действий.

[30] Felония (англ, felony) – понятие в праве, означающее преступление.

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

После скандала со швейцарским банком USB (банк заплатил штраф € 780 млн и выдал информацию о 300 гражданах США, скрывавших свои доходы для целей неуплаты налогов на родине, Службе внутренних доходов США[31]) Швейцария взяла курс на имплементацию статьи 26 Модельной конвенции ОЭСР о налогообложении дохода и капитала[32]. 13 марта 2009 г. Федеральный совет заявил, что эта норма будет воспринята Швейцарией и станет основанием представления информации при условии подачи конкретного и обоснованного заявления. Однако существует точка зрения, что

---

[31] См. подробнее, например, статьи: Пономарев А. Цюрих, откройся! // Национальный банковский журнал. № 9. Сентябрь 2009 г.; Саркисянц А. Европейские банки: перспективы развития на фоне кризиса // Бухгалтерия и банки. № 4. Апрель 2009 г. и др.

[32] Типовая модель конвенции Организации экономического сотрудничества и развития (ОЭСР) представляет собой проект двустороннего налогового соглашения из 30 статей, который в большинстве случаев используется как базовый документ для подготовки и начала переговоров между заинтересованными государствами и не является для них строго обязательным.

Швейцария всегда умела грамотно защищать свои интересы и балансировать между требованиями, в частности, банкиров и зарубежных политиков, поэтому процесс пересмотра двухсторонних договоров об избежании двойного налогообложения может затянуться. Хотя соответствующие поправки уже были внесены 24 сентября 2011 г. в двусторонний договор между Швейцарией и Россией, а также еще ранее с Германией и Великобританией[33].

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

---

[33] Международное и зарубежное финансовое регулирование: институты, сделки, инфраструктура: Монография / Под ред. А.В. Шамраева: в 2 ч. Ч. 2. – М.: КНОРУС; ЦИПСиР, 2014. – С. 287–292.

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

2.5. Выводы

В заключение приведем некоторые выводы:

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

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

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

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

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

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

Глава 3
Использование современных форм платежей для легализации преступных доходов и организация противодействия

Современные условия конкуренции в сфере оказания финансовых, в частности банковских, услуг обусловливают интенсивное внедрение технологий дистанционного банковского обслуживания (ДБО) или, используя более общее понятие, – технологий электронного банкинга (ТЭБ). Практически все кредитные организации внедряют все новые варианты ДБО, причем ни одна из организаций, внедривших какую-либо технологию такого рода, не останавливается на достигнутом. По данным, получаемым Банком России в результате проведения сплошных анкетирований кредитных организаций по тематике электронного банкинга, если пять лет назад большинство этих организаций использовали в среднем одну-две системы ДБО, то впоследствии пик распределения количества различных систем электронного банкинга (СЭБ) пришелся на две-четыре одновременно используемые системы, а последнее по времени анкетирование (в 2013 г.) показало, что наиболее часто встречаются кредит-

ные организации, задействующие от трех до пяти каналов ДБО. Лидеры же в данной области, то есть наиболее высокотехнологичные из них умудряются одновременно применять восемь-десять СЭБ, таких как интернет-банкинг для юридических и физических лиц (с вариантами), интернет-трейдинг и дилинг, виды мобильного банкинга, традиционные системы типа «Клиент-банк», обслуживая также площадки интернет-торговли, биржи и т. д.

Приведенные данные свидетельствуют о том, что имеет место однонаправленный процесс перехода банковской деятельности в так называемое виртуальное пространство (или, иначе, киберпространство), а значит, тем самым подтверждается справедливость слогана «Не будет банкинга, кроме электронного банкинга, а мобильный банкинг – предел его»[34]. Этому, кстати, способствует и ориентация Министерства финансов России на перевод крупных платежей в упомянутое киберпространство безналичных карточных операций. Вместе с тем в этом пространстве наряду с легитимными клиентами высокотехнологичных кредитных организаций стали активно действовать и преступные группировки, в том числе межрегиональные и международные, равно как и отдельные лица, характеризуемые «криминальным мышлением». Вследствие этого негативного явления практически каждая СЭБ, формирующая своего рода «виртуальные воро-

[34] Лямин Л.В. Применение технологий электронного банкинга: рискориентированный подход. – М., КНОРУС; ЦИПСиР, 2011.

та» в банк, превратилась в объект виртуальных атак на банки и их клиентов, приводящих к вполне реальным финансовым потерям, в совокупности исчисляемыми миллиардами рублей. Следствием этого стала дополнительная и весьма серьезная нагрузка как на Банк России (в форме многочисленных жалоб клиентов), так и на правоохранительные органы и, соответственно, судебную систему.

Безусловно, банки всегда подвергались рискам, связанным с ошибками или мошенничеством, однако вместе с внедрением современных компьютерных технологий уровень таких рисков и масштаб их влияния существенно выросли ввиду того, что количество причин и состав возможностей реализации угроз, лежащих в основе новых компонентов рисков такого рода, значительно увеличились. Подтверждением этому является постоянный рост числа финансовых преступлений разного рода как против юридических и физических лиц, пользующихся банковскими услугами, так и против самих банков, анализу которых посвящен настоящий раздел книги. При этом акцент делается на существенно более широкой по сравнению с традиционной (ограниченной рамками Федерального закона от 07.08.2001 № ФЗ-115 «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма») интерпретацией понятия и содержания процесса финансового мониторинга (ФМ). В связи с указанной позицией можно отметить также, что расширенная трактовка по-

нятия ФМ стала встречаться и в мировой практике анализа противоправной финансовой деятельности и организации противодействия ей. Например, в материалах таких организаций, деятельность которых направлена против отмывания денег (ОД) и финансирования терроризма (ФТ), как ФАТФ и FinCEN[35], встречаются указания на то, что финансовым организациям необходимо усилить борьбу с компьютерными мошенничествами, поскольку успехи в борьбе международного сообщества с ФТ и перекрытие различных каналов, используемых для этого, привели к тому, что для финансирования деятельности таких чрезвычайно опасных организаций стали широко задействоваться команды хакеров и применяться способы осуществления крупномасштабных финансовых мошенничеств. Из этого делается вывод о том, что собственно осуществление противодействия совершению компьютерных мошенничеств в отношении этих организаций и их клиентов следует рассматривать в том числе и как непосредственно связанное с борьбой с международным терроризмом.

Ввиду этого в современных банках неизбежно внедрение специальных процедур для адекватного реагирования на возможную противоправную деятельность (ППД), осуществляемую с помощью ТЭБ. Поэтому и необходим анализ и практический учет новых потенциальных угроз, связанных

[35] Financial Crimes Enforcement Network (Сеть для противодействия финансовым преступлениям – специальное бюро в Казначействе США).

с этими технологиями, а также сценариев их возможной реализации с оценкой последствий. Следует отметить, что в силу неразвитости отечественного законодательства в области так называемых электронных финансов[36] последующее изложение ведется с позиций организации противодействия на основе риск-ориентированного подхода.

Начать такой анализ уместно с рассмотрения общей картины усложнения структуры типичных банковских рисков[37].

[36] Насколько известно автору, проект соответствующего федерального закона был разработан еще в 2000 г. и «хранится» в Государственной думе, однако дальше дело, похоже, так и не пошло, тогда как во многих цивилизованных странах законодательные акты такого рода работают давно и успешно.

[37] В терминологии Письма Банка России от 23.06.2004 № 70-Т «О типичных банковских рисках».

3.1. Новые факторы риска для кредитных организаций и их клиентов в условиях применения технологий электронного банкинга

Не подлежит сомнению тот факт, что применение кредитными организациями (далее для краткости называемыми банками) технологий ДБО или, иначе, «электронного банкинга» **радикально изменяет способы и условия** осуществления банковской деятельности. Эти изменения необходимо учитывать в организации и содержании целого ряда внутрибанковских процессов, что будет детально описано в предпоследнем подразделе настоящего раздела. В цитировавшейся выше книге описывалось принципиально новое явление в сфере банковской деятельности, «вызванное к жизни» применением самих ТЭБ, а именно так называемый информационный контур банковской деятельности (ИКБД), приводилась его обобщенная схема, а также рассматривались три основных, «системных» фактора риска, обусловливающие возникновение новых источников компонентов банковских рисков[38]. До наступления эры ДБО данное явле-

[38] В данном случае используется терминология, отличающаяся от общепринятой в соответствующей отечественной литературе, поскольку речь далее идет о возникновении новых угроз надежности банковской деятельности с точки зре-

ние отсутствовало как таковое, хотя, строго говоря, элементы этого контура стали появляться в банках вместе с внедрением первых же структур локальных вычислительных сетей (изначально строившихся на основе сетевых систем типа «клиент – сервер» по простым схемам типа «звезда», которую составляли центральный универсальный компьютер и рабочие станции, используемые операционным банковским персоналом). Для того чтобы обеспечить ясность последующего анализа усложнившейся структуры банковских рисков, упомянутая схема в несколько измененном вариант приводится и здесь (рис. 3.1).

ния анализа возможного вмешательства в нее преступных элементов, о чем необходимо иметь отчетливое представление руководителям и персоналу высокотехнологичных кредитных организаций, а также их клиентам. Как следствие, возникают новые составляющие типичных банковских рисков, связанные с противоправной деятельностью, из-за которых смещаются их профили и повышаются уровни.

Рис. 3.1. *Информационный контур банковской деятельности, формирующийся при дистанционном банковском обслуживании*

На приведенной схеме условно показаны два входящих в ИКБД банка (Банк-1 и Банк-2), укрупненная структура их локальных вычислительных сетей (ЛВС) и банковских автоматизированных систем (БАС)[39] с функциями управления,

[39] Здесь, к слову, можно отметить, что использование понятия «банковская автоматизированная система» в отличие от часто встречающейся в литературе аббревиатуры АБС (автоматизированная банковская система) представляется предпочтительным, имея в виду именно назначение автоматизированных систем в банках, с учетом того, что понятие «банковская система» определено в Федеральном законе «О банках и банковской деятельности», но представлять ее автоматизированной до настоящего времени затруднительно.

обработки и хранения данных (обозначенных как СУБД – система управления базой данных), элементы сетевой защиты, представленные (только для примера) брандмауэрами (сетевыми экранами), виртуальное пространство, образованное системами, каналами и линиями связи провайдеров банков и клиентов, собственно варианты клиентской части ДБО и два неприятных типа: хакер (хронически занятый попытками несанкционированного доступа (НСД) к банковским информационным ресурсам) и крэкер (ориентированный на нанесение ущерба организациям любым доступным через сетевое пространство способом за счет «взлома» и уничтожения их программно-информационного обеспечения). Как отмечалось, в условиях ИКБД возникают **три основных** новых фактора риска, о которых необходимо знать руководству банков и на которые следует правильно реагировать посредством адекватной модернизации процесса управления банковскими рисками (УБР):

1) возникновение клиента нового типа, который во многих случаях, не приходя в банк, сам «играет роль» операциониста, при этом, как следствие, для банка и клиента возникает **взаимная анонимность,** на эффектах которой основаны все схемы организации финансовых преступлений и так называемого фишинга при ДБО;

2) возникновение **зависимости надежности** банковской деятельности от сторонних организаций – провайдеров разного рода, автоматизированные системы и каналы связи

которых могут использоваться для реализации противоправной деятельности в отношении банков и их клиентов с нанесением ущерба их интересам;

3) возникновение разнообразных **возможностей для НСД** к сетевым структурам и БАС банков за счет особенностей функционирования так называемых открытых систем со стороны как внешних преступных элементов, так и инсайдеров в самих банках, обладающих специальными знаниями в части организации и функционирования БАС.

В случае действия первого из приведенных факторов могут иметь место два главных негативных эффекта. Первый из них заключается в том, что банк не всегда может быть уверен в том, что к нему обращается легитимный, официально зарегистрированный, то есть априори известный ему клиент. Это происходит из-за так называемого хищения личности (identity theft), то есть имитации злоумышленником действий упомянутого клиента за счет использования данных его удаленной идентификации. Поэтому персоналу банков следует информировать клиентов ДБО о приемах, с помощью которых может быть совершена подмена такого рода, и о тех мерах, которые им следует оперативно принимать в случаях противоправных попыток имитации их действий, а также о новых способах и попытках компрометации схем подтверждения идентичности удаленных клиентов. Кроме того, в договорах с клиентами целесообразно указывать, ка-

кие способы банк будет использовать для связи с клиентами и на какие «подвохи» клиент обязан не реагировать. Второй эффект связан с тем, что клиент не всегда может быть уверен в том, что взаимодействует со «своим» банком из-за «успешных» действий фишеров, которым он невольно выдает данные своей персональной удаленной идентификации. Это происходит преимущественно за счет применения методов так называемой социальной инженерии и хакерских приемов. Данные вопросы будут рассмотрены в одном из последующих подразделов.

Действие второго фактора (в части противоправной деятельности, технические проблемы здесь не рассматриваются) может проявляться в том, что атаки на банки (и, как следствие, на их клиентов) осуществляются через системы провайдеров, включая предоставляемые ими общедоступные каналы (линии) связи. При такого рода намерениях разрабатываются и применяются специальные программные средства, которые должны нарушать работу аппаратно-программного обеспечения взаимодействующих при ДБО сторон (то есть переводить его в нештатные режимы работы (в широком смысле, включая создание возможностей для НСД) или выводить из строя). При этом сами системы провайдеров могут превращаться в источники угроз для банков, если входящие в них вычислительные сети заражаются вредоносным кодом (в том числе программами-вирусами), с помощью чего формируются, в частности, так называемые бот-

неты («роботизированные» вычислительные сети), используемые для нарушения функционирования вычислительных сетей и серверов организаций, которые оказываются объектами сетевых атак[40]. Под прикрытием таких атак стали все чаще совершаться финансовые преступления против банков и их клиентов, в том числе с проникновением и «усилением» атак через посредство автоматизированных систем провайдеров кредитных организаций.

Третий фактор может реализоваться в форме различных угроз: специально организуемые или случайно возникающие схемы для осуществления НСД (в том числе через информационные сечения, образуемые при стыковке различных автоматизированных систем или подсистем), сетевые, вирусные, хакерские атаки и т. п. В этих случаях речь идет, как правило, о нелегитимном завладении теми или иными информационными активами (учитывая, что современная банковская деятельность превратилась преимущественно в информационную дисциплину) или о прикрытии таких действий. Вследствие того что при ДБО формируются новые информационные потоки, число которых при массовом обслуживании может исчисляться десятками, сотнями тысяч и миллионами и которые выходят далеко за пределы офисов банка, а это – неотъемлемое свойство любого ИКБД, существенно

[40] Этой проблематике Банк России посвятил письмо от 24.03.2014 № 49-Т «О рекомендациях по организации применения средств защиты от вредоносного кода при осуществлении банковской деятельности».

изменяются характеристики так называемого периметра безопасности банка. Следствием же этого становится необходимость внедрения таких средств защиты архитектур вычислительных сетей (основными из которых являются маршрутизаторы и брандмауэры или их аппаратно-программные комбинации, а также прокси-сервера, – хотя это не единственные средства сетевой защиты), которые позволяют изолировать чувствительные к НСД информационные сечения в таких архитектурах[41]. Ключевым фактором надежности функционирования любого банка при этом становится осведомленность его высшего руководства о новых потенциальных угрозах при ДБО.

Необходимо отметить, что в условиях ДБО проблематика точной локализации сечений указанного рода реально «выходит на передний план», поскольку в таких местах возможно прежде всего несанкционированное вмешательство в информационные потоки, в особенности при нелегитимном использовании прав и полномочий доступа к ним и к аппаратно-программному обеспечению (АПО) банков и провайдеров, через которое они проходят. Как показывают исследования, наиболее серьезные угрозы при этом могут возникать со стороны инсайдеров кредитных организаций. Информационные сечения, через которые возможно какое-ли-

[41] Под информационными сечениями в данном случае понимаются те места в компьютерных системах (в том числе сетевых, распределенных), через которые потоки данных передаются из одной системы или подсистемы в другую, либо претерпевают какие-либо преобразования.

бо вмешательство в информационные потоки, генерируемые, поддерживаемые и обрабатываемые банками, следует, по возможности, исключать из ИКБД, а если это оказывается невозможным, то их необходимо наиболее строго контролировать в соответствии с так называемым принципом четырех глаз[42]. Предотвращение возникновения подобных сечений в любом ИКБД или, в случае их неизбежного появления, обеспечение возможностей их полноценного контроля руководству банков целесообразно предусматривать, начиная еще с этапа принятия решения о внедрении той или иной ТЭБ и проектирования/разработки реализующей ее СЭБ. Очевидно, что для этого требуется наличие в банке соответствующих распорядительных документов и осуществление «проактивного» анализа сопутствующих внедрению ТЭБ изменений в структуре банковских рисков.

При реализации любого из упомянутых выше факторов или какой-либо одной связанной с ними угрозы денежные средства, хранящиеся в банке в форме записей об их суммах в его базах данных, могут быть нелегитимно и оперативно переведены на сторонние счета в электронной форме, что обычно и происходит в процессе совершении мошенничеств. При этом современные возможности использования сетевых технологий, а также зонального и даже глобального сетевого информационного взаимодействия позволяют осуществлять подобные трансферы на счета, расположенные

[42] Речь в данном случае идет о двойном независимом параллельном контроле.

практически в любой юрисдикции (городе, регионе, стране). Поэтому, в частности, руководству банков следует помнить о необходимости четкого и полного определения состава так называемой сеансовой информации (СИ), о чем будет сказано в последнем подразделе, накапливаемой и сохраняемой в течение каждого отдельного сеанса информационного взаимодействия удаленного клиента с банком, и обеспечения гарантий ее сохранения в течение установленных сроков (которые следует указывать также и в правоустанавливающих документах на пользование ДБО). При этом необходимо гарантировать и возможность оперативного доступа к ней как минимум при инициации претензионной работы. В основу такого определения целесообразно закладывать механизмы моделирования угроз надежности банковской деятельности в части противодействия возможной ППД, сценарии их возможного развития, состав угрожаемых активов банка, возможные последствия реализации таких сценариев и тому подобные соображения, относящиеся к процессу УБР[43].

Эта информация может впоследствии составить основу для принятия решений при разрешении конфликтных (спорных) ситуаций, возникающих в процессе осуществления ДБО между банком и клиентами, или при проведении расследований случаев ППД. Таким образом, речь идет, по сути, о постоянном формировании и поддержании **доказа-**

[43] К сожалению, нельзя сказать, что описанный подход до настоящего времени является общепринятым в российском банковском секторе.

тельной базы ДБО и обеспечении ее **юридической силы** – в этом заключаются две главные задачи, которые подлежат решению при организации и реализации с помощью информационных технологий (ИТ) в составе ФМ как внутрибанковского процесса и определения видов и содержания составляющих его процедур. При этом, как отмечалось выше, ФМ целесообразно организовывать как внутрибанковский процесс с заведомо более широким содержанием, нежели обычно принято определять, которое заведомо не ограничивалось бы требованиями традиционного противодействия ОД и ФТ (ПОД/ФТ), но охватывало бы всю возможную ППД, с которой в перспективе могут столкнуться банки и их клиенты ДБО. Тем самым можно будет устранить и неоднородности в распределении соответствующих функциональных ролей между такими структурными подразделениями банков, как службы ИТ, внутреннего контроля (ВК), ФМ, безопасности (информационной или экономической), подразделениями, ответственными за работу с клиентами и т. д.

Со времени первой публикации по рассматриваемой тематике банковских рисков, связанных с ДБО[44], прошло уже немало времени, и количество публикаций по данной тематике постоянно увеличивается (что свидетельствует одновременно о «разрастании» рассматриваемой проблемной об-

---

[44] Лямин Л.В. Анализ факторов риска, связанных с интернет-банкингом // Расчеты и операционная работа в коммерческом банке. 2006. № 5. С. 52–63; № 6. С. 43–54; № 7–8. С. 37–54.

ласти). Однако угроз надежности банковской деятельности не только не стало меньше, но они стали, так сказать, еще более изощренными, а их реализация даже только в плане ППД в киберпространстве ИКБД по-прежнему обусловливается прежде всего такими факторами, как:

– новизна технологических и технических достижений в области ДБО (которые могут оказаться связаны с новыми компонентами таких банковских рисков, как операционный, правовой, репутационный[45], ликвидности (неплатежеспособности), стратегический, а в некоторых случаях и страновой);

– сложность анализа связанных с разновидностями ДБО потенциальных угроз, преобразующихся в компоненты банковских рисков (в том числе комплексного анализа, охватывающего все «виртуальные ворота», которые неизбежно «открывает» банк, переходящий к ДБО);

– недостаточная компьютерная (как, впрочем, и финансовая, и правовая) грамотность подавляющего количества клиентов, которые охотно переходят от традиционного банковского обслуживания на ТЭБ и пользуются соответствующими СЭБ, которые реализуют такие технологии.

Эти и другие, менее очевидные, причины для существен-

[45] Этот риск в отечественной литературе известен также как риск потери деловой репутации, но в данном контексте используется международная терминология.

ного расширения возможностей осуществления в банках противодействия возможной ППД в условиях применения ТЭБ будут более детально рассмотрены ниже.

Можно отметить также, что на фоне все большего усложнения компьютерных технологий, ориентированных на внеофисное обслуживание клиентов банков, и, соответственно, необходимого для этого банковского АПО, то же самое происходит и с криминальной деятельностью, поскольку преступные сообщества охотно и быстро «осваивают» новые электронные банковские технологии и используют их для создания новых вариантов ППД в киберпространстве. Одним из наиболее типичных примеров в последние годы стало использование в противоправных целях вариантов мобильного банкинга, которые приходят на смену традиционному «телефонному» банковскому обслуживанию. Вследствие этого вместе с новыми достижениями в направлениях применения этих технологий развивается и существенно усложняется сопутствующая рассматриваемой проблематике область расследования компьютерных преступлений (о чем еще будет говориться в подразделе 3.3). В современном мире эти факты целесообразно учитывать руководству высокотехнологичных банков в рамках организации противодействия возможной ППД, а теперь, в первую очередь, при внедрении и развитии ДБО.

Основной акцент при этом целесообразно делать на тех новых специализированных процедурах, которые позволяли

бы эффективно учитывать во внутрибанковских процессах управления и контроля, во-первых, факт удаленности клиентов при ДБО, во-вторых, специфику виртуального пространства, через которое оно осуществляется, в-третьих, особенности функционирования так называемых открытых систем. Здесь, прежде всего, целесообразно рассмотреть организацию ПОД/ФТ, осуществляемого в связи с реализацией процессов ВК и ФМ, поскольку эти задачи имеют достаточно проработанную правовую основу (имея в виду такие основополагающие акты, как Федеральные законы «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» (далее – 115-ФЗ) и «О Центральном банке Российской Федерации (Банке России)») и сопутствующие подзаконные акты[46].

Как свидетельствуют материалы финансовых разведок, в том числе России, различных международных организаций, в частности ФАТФ, практически все финансовые преступления совершаются посредством проведения операций в платежных системах, в том числе трансграничных. При этом чем лучше их параметры (скорость, надежность функциони-

[46] Например, Положения Банка России от 29.08.2008 № 321-П «О порядке представления кредитными организациями в уполномоченный орган сведений, предусмотренных Федеральным законом "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма"», от 02.03.2012 № 375-П «О требованиях к правилам внутреннего контроля кредитной организации в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» и др.

рования), тем выше, при недостаточных мерах противодействия ППД, их уязвимость с точки зрения возможностей ОД и ФТ. В связи со сказанным из числа известных 40 рекомендаций ФАТФ две непосредственно связаны с использованием технологических нововведений (таких как ТЭБ), а именно Рекомендации 15 и 16[47]:

15. Новые технологии

Странам и финансовым учреждениям необходимо определять и оценивать риски отмывания денег или финансирования терроризма, которые могут возникнуть в связи с а) разработкой новых продуктов и новой деловой практики, включая механизмы передачи, и б) использованием новых или развивающихся технологий как для новых, так и для уже существующих продуктов. В случае финансовых учреждений такая оценка риска должна проводиться до запуска новых продуктов, деловой практики или использования новых или развивающихся технологий. Им также следует принимать соответствующие меры для контроля и снижения этих рисков.

16. Электронные переводы средств

Странам необходимо обеспечить включение

[47] Международные стандарты по противодействию отмыванию денег, финансированию терроризма и финансированию распространения оружия массового уничтожения / Пер. с англ. – М.: Вече, 2012.

финансовыми учреждениями требуемой и точной информации об отправителе и требуемой информации о получателе в электронный перевод и сопровождающие сообщения и то, чтобы эта информация сопровождала электронный перевод или передаваемое сообщение по всей цепочке платежа.

Странам необходимо обеспечить, чтобы финансовые учреждения осуществляли мониторинг электронных переводов в целях выявления тех из них, по которым отсутствует требуемая информация об отправителе и (или) получателе, и принимали соответствующие меры.

Странам необходимо обеспечить, чтобы при обработке электронных переводов финансовые учреждения предпринимали действия по замораживанию. Они должны также запрещать проведение операций с установленными лицами и организациями в соответствии с обязательствами, которые определены в соответствующих резолюциях Совета безопасности ООН…

При этом ФАТФ акцентирует внимание на том, что при осуществлении ФМ и реализации процедур ПОД/ФТ следует переходить от анализа отдельных финансовых операций клиентов банков к анализу их хозяйственно-экономической деятельности. Однако, это, конечно, гораздо проще сказать, чем сделать.

Аналогичной позиции придерживается и Базельский комитет по банковскому надзору (БКБН), который в одной из своих публикаций, посвященных так называемому электронному трансферу денежных средств в части «скрытых» или «прикрытых» платежей[48], отмечает:

> **При выполнении трансграничных банковских операций помимо банка источника ордера (originator) и банка бенефициара в процесс передачи и обработки банковских данных могут вовлекаться другие банки, выполняющие функции посредников…**
>
> **…Кредитным организациям, играющим роль таких посредников, независимо от их юрисдикции, следует соблюдать требования, предъявляемые к основным участникам трансграничных банковских операций (источнику и бенефициару), включая определения, содержащиеся в «Специальных Рекомендациях VII» ФАТФ (SR VII), особенно в условиях, снижающих прозрачность (transparency) выполняемых операций (например, через S. W. I. F. T.)».**

Также подчеркивается:

> **Недостаток информации об источниках**

[48] «Due diligence and transparency regarding cover payment messages related to cross-border wire transfers», Basel Committee on Banking Supervision, Bank of International Settlements (BIS), Basel, May 2009.

и бенефициарах переводов денежных средств может препятствовать банку-посреднику точно оценить риски, ассоциируемые с корреспондентскими и клиринговыми операциями. Такой банк не сможет сопоставить данные с признаками, требующими блокировать или задержать операции либо «заморозить» активы ее участников. <…>

…Повышение прозрачности платежных операций зависит не только от стандартов передачи данных, но и от рабочих процедур банков, вовлекаемых в их обработку, от чего зависит надежность и качество функционирования платежной системы.

Одной из наиболее неприятных для банков особенностью реализации двух связанных с ДБО эффектов взаимной анонимности является то, что банки могут оказаться незаметно для себя вовлечены в ту или иную ППД, что может негативно сказаться на их отношениях и с государством, и со своими клиентами (тем самым повышаются уровни правового и репутационного рисков). Руководству этих учреждений целесообразно помнить о последствиях такого рода, поскольку, как будет показано далее, развитие ситуации при проведении расследований ППД может негативно сказаться на их имидже, а если банки действительно окажутся обоснованно обвиненными в незаконной деятельности, то это может повлечь за собой отзыв лицензии на осуществление банков-

ских операций (что, к сожалению, давно уже не редкость).

При совершении трансферов денежных средств в электронной форме виртуальное пространство позволяет скрывать как их инициаторов, так и бенефициаров уже при самом незначительном числе агентов сетевого «финансово-информационного» взаимодействия. При типовых трехэтапных схемах ОД («размещение – расслоение – интеграция») с участием множества промежуточных (подставных) агентов, «перекачивающих» денежные средства между своими банковскими счетами, для выявления этого взаимодействия требуется наличие достаточно сложных аналитических алгоритмов, как и для обнаружения любых сомнительных операций. А поскольку схемы ОД модернизируются, то и алгоритмы ФМ должны становиться все более сложными, точно так же, как и его информационная основа и критериальная база.

В простейшем и типичном варианте на первом этапе ОД денежные средства, полученные нелегитимным путем, «вбрасываются» в финансовую систему, как правило, через специально создаваемые подставные фирмы, которые характеризуются как минимальным капиталом, так и тем, что существуют весьма непродолжительное время, после чего выполняется совокупность проводок, «не имеющих явного экономического смысла». Это переводы со счетов юридических лиц крупных денежных сумм, «распыляемых» по карточным счетам физических лиц (так называемых дропперов), с оперативным их получением или снятием через банкома-

ты. От банков, не желающих подпасть под подозрение в соучастии или в организации преступных финансовых схем, при этом требуется возможно более тщательное следование принципу, постоянно пропагандируемому БКБН, – «знай своего клиента» (ЗСК, за рубежом: КУС – Know Your Client). В то же время при использовании современных схем ОД и массовом ДБО это становится затруднительно, а поэтому безоглядное стремление какого-либо банка захватить значительную часть рынка ДБО вполне может оказаться необоснованным с точки зрения достаточности ресурсной базы такого банка в плане реализации необходимых (довольно сложных) процедур в составе процесса ФМ и контроля над хозяйственно-экономической деятельностью большого числа клиентов в целом (что специально отмечалось ФАТФ).

На втором этапе денежные средства, как правило, разделяемые на части, проводятся через ряд банков с использованием дистанционного управления счетами, что позволяет серьезно затруднить отслеживание транзакций и придать анонимность процедурам перевода денежных средств (в том числе за счет подставных промежуточных агентов финансовых операций). При этом нередко задействуются офшорные зоны и варианты технологии интернет-банкинга, в которых могут быть сконцентрированы сотни банков (включая так называемые бумажные или пустые банки, фигурирующие исключительно в электронном трансфере), а также сторонние анонимные прокси-сервера, не позволяющие опре-

делить местоположение участников информационного взаимодействия.

Для выявления таких ситуаций и придания операциям статуса сомнительных или для отказа от выполнения соответствующих операций банкам необходимо разрабатывать и внедрять соответствующие аналитические процедуры (об этом еще будет говориться ниже).

На третьем этапе денежные средства, которые могут с помощью удаленного управления пройти много циклов перемещений между юрисдикциями, банками и счетами большого количества фирм, в завершение процесса ОД концентрируются на счетах вполне легитимно существующих и действующих юридических или физических лиц. При этом обоснования для транзакций могут оказаться произвольными и никак не связанными с предыдущими транзакциями (БКБН, кстати, делает особый акцент на полноте информации, сопровождающей переводы денежных средств, когда рассматривает цепочечные операции). Поэтому возникает потребность в совершенствовании аналитических методов, применяемых в процессе ФМ, особенно в целях выявления банками связанных клиентов и транзакций на базе так называемого эффективного группового подхода[49] (имея в виду в том числе, что отдельные клиенты или связанные общими интересами группы клиентов могут осуществлять финансо-

[49] "Consolidated KYC Risk Management", Basel Committee on Banking Supervision, Basel, BIS, Oct. 2004.

вые операции через разные подразделения – филиалы, дополнительные офисы и пр. – одних и тех же банков). Вследствие этого пропагандируется требование наличия единой политики работы с клиентами в групповой структуре.

Как указывает БКБН, банкам следует руководствоваться основными положениями, способствующими эффективной реализации ФМ:

> **Необходимо разработать политику и процедуры идентификации, мониторинга и снижения репутационного, операционного, правового рисков и риска концентрации**[50].
>
> **Политика и процедуры на уровне филиалов и дочерних организаций должны быть согласованы с групповыми стандартами «знай своего клиента» и обеспечивать их поддержку.**
>
> **Подходы к идентификации клиента должны быть сформированы на основе возможных сопутствующих рисков.**
>
> **Между головным офисом и филиалами должно быть налажено такое информационное взаимодействие, чтобы была возможность получать информацию о рискованных клиентах для управления правовым и репутационным рисками.**

---

[50] Данный вид риска в цитируемой работе не поясняется, но из контекста можно понять, что речь идет о связанных операциях, совершаемых либо одним клиентом через разные филиалы банка, либо группой связанных какими-либо отношениями лиц.

Неизбежность усложнения алгоритмов ФМ видна также из содержания нормативных и других документов Банка России, которые продолжают разрабатываться и приниматься со времени принятия Закона № 115-ФЗ. По состоянию на последнее время банкам при организации и определении содержания внутрибанковского процесса ФМ (и ВК в соответствующей части) удобнее всего ориентироваться на письмо Банка России от 04.09.2013 № 172-Т «О приоритетных мерах при осуществлении банковского надзора», в котором описываются так называемые критерии определения признаков высокой вовлеченности кредитной организации в проведение сомнительных безналичных и (или) наличных операций (там же приведен и перечень документов Банка России для целей квалификации операций в качестве сомнительных). Поэтому банкам требуется разработка все более специализированных и детальных аналитических процедур ФМ (в интересах ПОД/ФТ) для идентификации указанных лиц, контроля и сопоставления данных, осуществляемых в соответствии с их ордерами. То же самое относится и к специализированному программно-информационному обеспечению (ПИО) процесса ФМ, функции которого должны соответствовать требованиям, установленным законодательными и подзаконными актами.

Если доказательство участия банка в каких-либо операциях, связанных с отмыванием денег или финансированием терроризма, карается в соответствии с федеральными зако-

нами и подзаконными актами, то наказание за другие виды ПДД далеко не всегда «находит своих героев». Расследование и доказательство преступлений, совершаемых в киберпространстве, стало в последние три десятилетия настолько актуальным, что за рубежом давно уже организована подготовка сотрудников финансовых организаций по специальности «сертифицированный инспектор по мошенничествам»[51]. В задачи специалистов, проходящих подготовку такого рода, входят прежде всего: предотвращение и (или) предупреждение мошенничеств, особенно корпоративных, проведение расследований преступлений (начиная с обеспечения сохранения улик, включая компьютерные устройства и данные, хранимые в электронной форме), взаимодействие с правоохранительными органами и участие в судебных разбирательствах и процессах в качестве экспертов; кроме того, они могут участвовать также в реализации отдельных функций в составе процессов обеспечения информационной безопасности (ОИБ), ФМ и ВК в своих организациях (постоянно или на основе привлечения).

Как отмечается в одной из популярных книг по противодействию мошенничествам, «совершение корпоративного мошенничества всегда связано с посягательством на активы корпорации и их хищением»[52]. При этом необходимо учиты-

---

[51] Certified Fraud Examiner.

[52] Ковасич Дж. Л. Противодействие мошенничеству. Как разработать и реализовать программу мероприятий. – М.: Маросейка, 2010.

вать тот принципиально важный факт, что упомянутые активы теперь – преимущественно «информационные», а следовательно, методы и средства их защиты оказываются прямо связаны с процессами ОИБ, ФМ и ВК в банках. Без сомнения, банковское дело также превратилось во многом в «информационную дисциплину».

Как отмечается в одной из популярных книг по так называемому киберправосудию (или, иначе, киберследствию) [53]:

> **Риски, с которыми сталкивается руководство кредитных организаций, по мере усложнения технологий только повышаются. Лица, склонные к злоупотреблениям технологиями, обнаруживают, что их возможности в этом плане расширяются, тогда как возможности руководства по удержанию их от этого становятся экспоненциально более проблематичными и ограниченными…**
>
> **В XXI веке ни одна организация не может забывать о возможности возникновения потребности в высококвалифицированном специалисте в области киберправосудия, независимо от включения его в персонал или приглашения со стороны. При этом актуальным является вопрос не «если» потребуется, а «когда»…**
>
> **Необходимость наличия актуальной**

[53] По материалам книги A.J. Marcella, Jr., D. Menendez "Cyber Forensics", 2nd ed., Auerbach Publications, Taylor & Francis Group, Boca Raton, FL, USA, 2008.

программы киберправосудия, обеспеченной подготовленным персоналом с квалификацией сертифицированного инспектора по мошенничеству и требуемыми рабочими процедурами для проведения служебных расследований, должна полностью осознаваться.

В формируемых новыми информационными технологиями условиях «электронной» финансовой и, в частности, банковской деятельности кибермошенничества становятся все более привлекательными, так как преступник «может скрываться» за киберпространством и использовать для совершения преступления специфические технологии: сетевые, хакерские, шпионские, троянские и т. п., а также прикрытия в форме сетевых атак, фальсификации маршрутной информации (к примеру, IP-адресов при ДБО в варианте интернет-банкинга и др.), равно как и разнообразные приемы, которые позволяют скрывать инициатора мошенничества, его бенефициаров или же сами факты мошенничества (когда прикрытие срабатывает). Практически все подходы такого рода базируются на одной основе – сочетании тех или иных способов НСД к атакуемым ресурсам и БАС кредитных организаций, а также аппаратно-программным средствам их удаленных клиентов (в том числе через автоматизированные системы провайдеров).

Надо отметить, что любое мошенничество, реализуемое через тот или иной способ НСД, связано с упоминавшим-

ся выше «хищением личности», то есть с приданием видимости легитимности обращения к каким-либо информационным активам и операциям с ними. Из этого следует, что основное внимание при использовании любых современных форм платежей и расчетов следует уделять способам и средствам подтверждения **идентичности** пользователя конкретных информационно-процессинговых ресурсов и правомерности использования тех или иных полномочий доступа к информационно-процессинговым ресурсам[54]. В свою очередь, само возникновение возможностей НСД всегда обусловлено недостатками в установлении ограничений на физический и логический доступ к АПО и информационным ресурсам организаций, что, в свою очередь, свидетельствует, как правило, о неполноте проведения приемо-сдаточных испытаний конкретных автоматизированных системы (БАС или СЭБ). Такая неполнота при построении логики рассуждений в обратном порядке свидетельствует о наличии недостатков в программах, методиках, актах и протоколах проведения этих испытаний, а значит, о недопонимании руководством банка значимости полного подтверждения заявленных свойств БАС и (или) СЭБ. Логическая последовательность обеспечения легитимности прав и полномочий доступа к чувствительным информационно-процессинговым

[54] При наиболее общем подходе понятие «пользователь» охватывает всех участников ИКБД как в банке, так и вне его, то есть и операционистов, и операторов, и администраторов (системных, сетевых, баз данных, информационной безопасности и т. п.), а также клиентов ДБО.

ресурсам, с известной долей условности показана на рисунке 3.2, скомпонованном на основе карикатуры, хорошо отражающей суть данной проблематики. Тем самым отражается также тесная и неразрывная связь процедур управления распределением прав и полномочий доступа к информационно-процессинговым ресурсам банка (включая филиалы, дополнительные офисы и пр.) и контроля над ними.

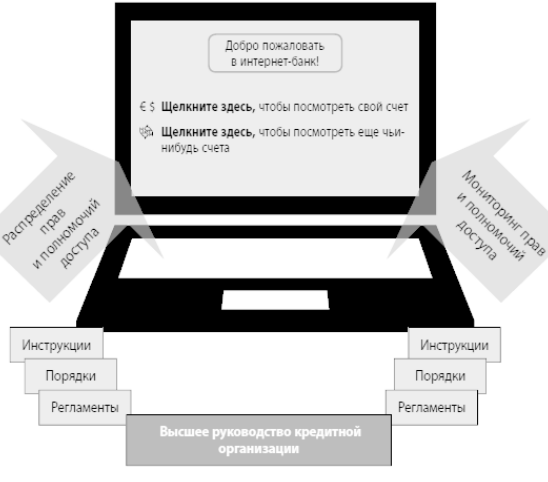

Рис. 3.2. *Пример проблематики разграничения прав и полномочий доступа в условиях применения технологий электронного банкинга*

Следует отметить, что нередко наблюдаемое в кредитных организациях, прежде всего банках, желание руковод-

ства «сэкономить» на так называемых незарабатывающих подразделениях, к числу которых, как исторически сложилось, относятся подразделения ИТ, ОИБ, ВК, ФМ, УБР и ряд других, гарантированно приводит к недостаткам в обеспечении надежности банковской деятельности. Следствиями такой «экономии» часто оказывается нехватка высококвалифицированного персонала, необходимого для правильной и надежной организации автоматизированной банковской деятельности, или недопустимая концентрация полномочий, в особенности это касается совмещения в одних руках функций администрирования: системного, сетевого, баз данных, информационной безопасности и т. п. Ситуация, в которой один человек совмещает несколько функций, которые в соответствии с правилами здравого смысла (в отсутствие соответствующих нормативных правовых актов) должны быть разделены, как это считается необходимым с точки зрения обеспечения гарантий невозможности НСД высокого уровня, может оказаться связанной с угрозами для безопасности информационных активов организации, так как при этом заведомо не выполняется упоминавшийся принцип «четырех глаз». В этом *случае* те или иные сотрудники, с одной стороны, получают наиболее полные права и полномочия доступа к таким ресурсам, а с другой стороны, оказываются фактически неподконтрольными.

Как отмечает в своей оригинальной книге один известный в прошлом в США мошенник: «Важно помнить: если для

людей невольно создаются условия, чтобы они воровали, они будут это делать!», вследствие чего постулируется, что «Доверие – хорошо, но контроль – лучше!»[55]. Данный автор знает, что говорит, когда заявляет в этой книге, что «Абсолютной надежности не существует» и что «Обман не прекращается никогда», – проведя за решеткой несколько лет за махинации с чеками, банкоматные мошенничества и прочую противоправную деятельность, он по освобождении открыл консультационную фирму по организации противодействию корпоративным и другим мошенничествам и написал упомянутую в ссылке книгу. В ней, помимо прочего, он приводит такие данные социологического опроса, которым были охвачены сотрудники нескольких сотен североамериканских компаний, которым задавались вопросы об их отношении к воровству:

> **Результаты исследований показали, что 10 % работников воровали бы все время, еще 10 % никогда не украли бы, а 80 % воровали бы, если бы у них была для этого причина. Это свидетельствует о том, что руководство компаний должно проявлять обеспокоенность о 90 % своего персонала…**

По данным указанного автора:

> **Банки теряют в пять раз больше денег от**

[55] Абигнейл Ф.У. Поймай его, если сможешь, или он поймает тебя. – М.: Поколение, 2007.

хищения денежных средств, чем от вооруженных ограблений. Кража на рабочем месте может быть настолько пагубной для компании, ставшей ее жертвой, что почти одна треть всех банкротств приписываются присвоению чужих средств.

Остается надеяться, что столь безрадостная картина является типичной только для США…

Ситуация усугубляется тем, что в виртуальном пространстве мошенничества совершаются мгновенно и практически незаметно. При виртуальном мошенничестве обычно неизвестно наверняка, кем является злоумышленник. Его нельзя увидеть, потому что это – аноним, скрытый технологиями и автоматизированными системами. Кроме того, как отмечает тот же автор, «Для подавляющего большинства клиентов банков электронные банковские операции все еще остаются загадочными». Практика изучения жалоб клиентов российских банков подтверждает этот неутешительный вывод, поэтому помимо широко обсуждаемой потребности в повышении финансовой грамотности населения логично было бы говорить и о повышении его «технологической грамотности». Сказанное относится и к качеству соглашений о ДБО в том смысле, что в соответствующих договорах, как правило, не оговариваются упоминавшиеся выше его доказательная база и ее юридическая сила.

В настоящее время специфика условий функционирования российского банковского сектора предполагает, как от-

мечалось, возникновение новых источников компонентов только для следующих банковских рисков: стратегического, операционного, правового, репутационного (потери деловой репутации), ликвидности (неплатежеспособности) и, в некоторых специфических случаях, странового[56]. Чтобы правильно определить состав источников компонентов рисков, способных негативно повлиять на процесс и результаты банковской деятельности кредитных организаций, удобно разбить ИКБД, образуемый той или иной системой электронного банкинга (СЭБ), на своего рода «зоны концентрации источников риска» и проанализировать особенности каждой из них. Затем, в соответствии с принятой в том или ином банке методологией УБР, можно сгруппировать отдельные факторы или источники компонентов рисков по их возможному проявлению в тех или иных типичных банковских рисках, которые описываются, как правило, во внутрибанковских документах типа «Положения об управлении банковскими рискам». Это может оказаться полезным, например, при организации управления рисками по их типам, перечисленным выше, при переходе к применению ТЭБ.

---

[56] В зарубежной практике риск-ориентированного банковского надзора в области ДБО рассматриваются все банковские риски (хотя их полный состав варьируется в зависимости от идеологии надзора, принятой конкретным федеральным ведомством), поскольку в некоторых странах допускается более «демократичный» подход к регламентации банковской деятельности, обеспечивающей организационно-финансовые потребности бизнеса: в ряде случаев можно дистанционно открывать банковские счета, оформлять кредиты и т. п.

Ниже проводится краткий анализ структуры этих банковских рисков[57] в части свойственных применению ТЭБ и реализующих их СЭБ причинно-следственных связей их компонентов наряду с теми угрозами надежности банковской деятельности, которые привносит ДБО само по себе. Если говорить конкретно о ППД, то, трактуя понятие указанной надежности с точки зрения выполнения кредитными организациями (в широком смысле) своих обязательств перед клиентами и контролирующими органами, можно определить те компоненты типичных банковских рисков, которые непосредственно связаны с опасностью осуществления ППД[58]:

• для операционного риска – это потенциальные финансовые потери, обусловленные мошенническими действиями в отношении кредитной организации и (или) ее клиентов за счет перевода автоматизированных систем, применяемых ею для осуществления банковской деятельности, в нештатные (в широком смысле) режимы функционирования, из-за чего могут осуществляться противоправные действия, включая проведение несанкционированных транзакций или прямые хищения финансовых средств в электронной форме либо конфиденциальной («чувствительной») информации и пр.,

---

[57] В данном случае используется нетипичная терминология, обусловленная акцентом на возникновении новых угроз надежности банковской деятельности, проявляющихся в уровнях и профилях типичных банковских рисков.

[58] В последующих определениях используется понятие «кредитная организация» более широкое, чем «банк», поскольку они касаются и небанковских организаций.

происходить нарушения доступности автоматизированных систем и (или) непрерывности их функционирования (включая как причины «удачные» сетевые и хакерские атаки, отказы и сбои аппаратно-программного обеспечения для прикрытия мошенничеств как самой кредитной организации, так и ее провайдеров), следствием чего окажется невыполнение кредитной организацией обязательств перед клиентами;

• для правового риска – это потенциальные финансовые потери, обусловленные невыполнением кредитной организацией требований нормативных правовых актов, регулирующих банковскую деятельность, и (или) законодательной неопределенностью дистанционного предоставления банковских услуг, а также судебными издержками/санкциями из-за невыполнения обязательств перед клиентами (включая потерю значимых данных и утечку «чувствительной» информации, нарушение банковской тайны, противоправную деятельность, которая оказывается возможной из-за недостатков аппаратно-программного или программно-информационного обеспечения банковской деятельности как самой кредитной организации, так и ее провайдеров, хищения денежных средств клиентов и т. д.), включая ситуации, в которых клиенты оказываются не способны выполнять свои обязательства перед третьими сторонами по вине кредитной организации и (или) ее провайдеров;

• для риска ликвидности (неплатежеспособности)[59] – это

[59] В данном случае имеется в виду то, что традиционное понятие «ликвид-

потенциальные финансовые потери кредитной организации из-за хищений ее информационных активов и (или) в форме ее неспособности полностью и своевременно выполнять свои финансовые обязательства в отношении конкретных клиентов в случаях несанкционированных переводов их финансовых средств, изменений в характеристиках управления ликвидностью в условиях открытого сетевого взаимодействия (блокировка автоматизированных систем или каналов/линий связи, непредвиденный отток финансовых средств, крупномасштабные финансовые хищения, другие потери высоколиквидных активов, сбои и отказы в работе аппаратно-программного обеспечения, применяемого для осуществления банковского обслуживания как кредитной организации, так и ее провайдеров), а также недостатки организационного характера, из-за которых финансовые обязательства перед клиентами не выполняются (таким образом возникает своего рода «персональная» неплатежеспособность, то есть в отношении конкретного клиента);

• для репутационного риска – это потенциальные финансовые потери, обусловленные формирующимся негативным общественным мнением в отношении кредитной организации из-за невыполнения ею обязательств перед клиентами (включая недоступность/неработоспособность/неполную функциональность/ненадежность/небезопасность ее автома-

---

ность» обретает новое смысловое содержание с точки зрения выполнения банками своих финансовых обязательств.

тизированных систем, потерю (утечку, хищение)/искажение/чувствительных данных из-за недостатков/отказов аппаратно-программного обеспечения кредитной организации и (или) ее провайдеров (в том числе саботажа, компьютерных преступлений (мошенничеств), сетевых, хакерских, вирусных атак, несанкционированного доступа к упомянутым данным, ставших известными судебных исков или сведений о нарушениях конфиденциальности информации (банковской тайны), веб-сайтов-муляжей и т. п.), воздействия на используемые этой организацией веб-сайты (блокировка, искажение контента и пр.);

• для стратегического риска – это потенциальные текущие и перспективные финансовые потери, обусловленные ошибочными бизнес-решениями относительно состава и (или) схемы дистанционного предоставления банковских услуг или неправильной реализацией основных решений такого рода в кредитной организации, которые приводят к возникновению возможностей использования банковских автоматизированных систем для осуществления и (или) прикрытия мошенничеств, нарушения целостности и (или) конфиденциальности клиентских или банковских данных, отмывания денег и финансирования терроризма (включая неправильное распределение функций, в том числе в рамках аутсорсинга, ошибки в способах предоставления и контроля оказания банковских услуг клиентам, в технологических и (или) организационно-технических решениях, приводящие

к неадекватности бизнес-моделям, недостаточную отладку, защищенность, управляемость и контролируемость банковских автоматизированных систем и т. п.).

Не исключено, что здесь можно было бы упомянуть и страновой риск (хотя это, скорее, перспектива), поскольку в современной банковской деятельности широко используется международное разделение труда, при котором банки открывают свои филиалы в разных странах, банковский процессинг концентрируется в специальных процессинговых центрах или на вычислительных мощностях крупных кредитных организаций, компаний-интеграторов, то есть в разнообразных формах аутсорсинга. В таких случаях возникают новые виды зависимости надежности банковской деятельности от сторонних для конкретного банка организаций, а вместе с ними – и новые проблемы обеспечения ее надежности, включая гарантии ОИБ как для самого банка, так и для его клиентов, однако в этих условиях полноценный контроль со стороны банка над обеспечивающими организациями становится более проблематичным.

Главными негативными последствиями мошенничеств являются прежде всего финансовые потери. Но это общее понятие целесообразно детализировать, поскольку эти потери могут быть разнородными. Так называемые прямые потери имеют наглядное денежное выражение как для клиента банка, так и для самого банка, поскольку при таких по-

терях речь идет о реализации компонента риска неплатежеспособности в отношении конкретных пострадавших клиентов. Помимо этих потерь часто приходится говорить о «косвенных» потерях – это расходы на расследование, ущерб от совершенной атаки, приведший к дополнительному расходу ресурсов банка (персонал, время, превентивные меры на будущее и т. д.), компенсационные выплаты и судебные издержки. Здесь проявляются преимущественно компоненты правового риска. Наконец, следует помнить и о, если можно так выразиться, «наведенных» потерях, то есть реализации компонентов репутационного риска: это потенциальная упущенная выгода, связанная с оттоком клиентов, понижением курса акций, негативным общественным мнением (даже просто отсутствие роста клиентской базы) и другие негативные последствия. Ну и, наконец, могут возникнуть компоненты стратегического риска как следствие явления взаимного влияния рисков – нерентабельность скомпрометированной СЭБ и напрасные затраты на ее внедрение.

Говоря об источниках компонентов банковских рисков, нельзя не сказать о тех, которые прямо связаны с понятием новых информационных технологий и автоматизированных систем. Известно, что если раньше внедрение этих технологий и освоение соответствующих автоматизированных систем могло растягиваться на годы, то в последнее время в условиях обостряющейся конкуренции на это уходят всего лишь месяцы. Поэтому помимо таких негативных явлений,

как недостаточная отладка и неполноценные приемо-сдаточные испытания новых СЭБ или БАС (что, бывает, выясняется уже в процессе их эксплуатации), может возникать и серьезная зависимость от компаний-разработчиков таких систем. Известны случаи, когда из-за сложности найма или переподготовки собственных специалистов банки «перекупают» специалистов из этих компаний, которые и становятся «автоматически» ответственными за работу новых автоматизированных систем. С одной стороны, это весьма эффективное решение проблемы с обеспечением необходимой квалификации и требуемой в ряде случаев узкой специализации персонала, однако, с другой стороны, неизбежно возникает вопрос: кто в кредитной организации сможет проконтролировать работу таких специалистов и насколько можно быть уверенными в них (то есть в их честности и добросовестности)?

Кроме того, практика свидетельствует о том, что наблюдается нехватка специалистов, способных оценить истинные масштабы новых угроз, связанных с киберпространством, в том числе со стороны вредоносных программ разного рода[60], с которыми может столкнуться кредитная организация и ее клиенты, разработать и внедрить эффективную политику ОИБ, грамотно построить защиту корпоративных вычислительных сетей, включая защиту от действий инсайдеров,

[60] Так называемого в общем случае класса вредоносного кода malicious ware или, сокращенно, malware.

внедрить технологию «виртуальных частных сетей» [61], позволяющую защищать чувствительную информацию, передаваемую по сетям связи общего пользования и т. п. При этом чаще всего четкие требования к ОИБ не входят в содержание политики развития ИТ кредитных организаций и не становятся составной частью соответствующей стратегии. Из-за этого появляются компоненты банковских рисков, связанные с недостаточно проработанными планами развития технологического и технического обеспечения банковского обслуживания, выполнения банковских операций и их обеспечением, то есть соответствующим АПО и высококвалифицированным персоналом (основной ресурсной базой).

Общая «беда», сопутствующая внедрению и применению в банках новых информационных технологий, состоит в том, что нередко такие немаловажные внутрибанковские процессы, какУБР, информатизация банковской деятельности, ОИБ, ВК, ФМ и работа других, как считается, «не зарабатывающих» подразделений кредитной организации, вообще финансируются по «остаточному принципу». При этом наблюдаются и такие нежелательные варианты «экономии» на дорогостоящих специалистах, что, как отмечалось, ведет к образованию чрезмерной концентрации полномочий в руках отдельных должностных лиц или к невозможности надежного выполнения довольно «тонких» функций в части ОИБ, таких как настройка брандмауэров, прокси-серверов

[61] Virtual Private Network – VPN.

и т. п. в том смысле, что специалисты, обладающие необходимой для этого достаточно узкой специализацией и высокой квалификацией, во-первых, становятся «штучным товаром», во-вторых, их действия оказывается некому контролировать. Кроме этого, средства сетевой защиты стоят, как правило, недешево, а не в каждом банке руководство имеет полное представление о тех мерах и средствах защиты, которые необходимо приобретать, внедрять, настраивать и сопровождать в связи с каждым новым ИКБД, формируемым той или иной новой ТЭБ. Вследствие этого надежно защитить все «виртуальные ворота» такого рода окажется весьма проблематично, то есть опять-таки может формироваться почва для использования служебных полномочий в личных целях (на исполнительском уровне) с последующим нанесением крупного финансового ущерба банку и его клиентам – это тот же проблемный вопрос о контролируемости информационных сечений, возникающих в ИКБД, между БАС и СЭБ и т. п.

Известно, что «рыба ищет, где глубже, а человек – где лучше», и такого рода поиски неудовлетворенных своим положением специалистов с высокой и достаточной специфичной узкой квалификацией могут приводить к тому, что отдельные банки будут терять определенных специалистов уровня, например, системных администраторов и других, которые при уходе в другую организацию будут уносить с собой всю информацию о составе и архитектуре БАС и СЭБ поки-

даемого ими банка, порядках, правилах, правах и полномочиях доступа к чувствительным программно-информационным ресурсам ит.п., то есть представлять в итоге совершенно конкретные угрозы для этого банка. Такие угрозы, будучи «сдобрены» плохими взаимоотношениями с прежними работодателями (причины которых – в недостаточной по мнению того или иного лица финансовой оценке его квалификации, трудозатрат, ответственности, функциональной и технологической зависимости и т. п.), могут оказаться причинами последующих инцидентов ППД, причем по своему характеру наиболее серьезных для банка и его клиентов (точнее, принадлежащих им финансовых средств и конфиденциальной информации, что в условиях известной «криминализации» российской экономики может обернуться для участников финансовых отношений непредсказуемыми последствиями). Известны случаи «закладывания» увольняющимися специалистами своего рода «программных бомб», которые через какой-то интервал времени наносят физический ущерб ПИО банков, организации ими скрытых каналов доступа к разным компонентам ПИО, сговора с отдельными сотрудниками подразделения, отвечающего за ИТ или ОИБ с целью совершения впоследствии хищений финансовых средств или конфиденциальной информации и т. д.

В общем случае руководству насыщенных информационными технологиями банков (да и любых кредитных организаций) необходимо учитывать все источники угроз, связан-

ных прежде всего с проявлениями так называемого человеческого фактора, которые показаны на рисунке 3.3 [62].

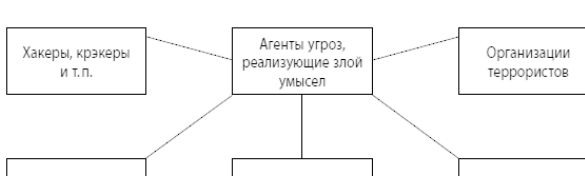

Рис. 3.3. *Взаимодействие структурных подразделений кредитной организации в целях обеспечения осуществления В К*

Совокупность рассмотренных в настоящем подразделе проблемных вопросов свидетельствует о том, что в области таких наиболее современных электронных банковских технологий, как ДБО, присутствуют серьезные компоненты стратегического риска, чему нередко просто не уделяется внимание (чтобы убедиться в этом, достаточно прочитать те же «Положения об управлении банковскими рисками» в высокотехнологичных кредитных организациях). Очевидно, что если в отношении новых угроз надежности банковской деятельности не принимаются должные меры, препятствующие их реализации, – хотя для этого достаточно начать с

[62] Ковасич Дж. Л. Противодействие мошенничеству. Как разработать и реализовать программу мероприятий. – М.: Маросейка, 2010.

полноценного анализа зон концентрации источников компонентов банковских рисков и зон ответственности банка, то и сам бизнес в рамках ДБО может оказаться скомпрометированным. Следствием этого станут финансовые потери банков и их клиентов, а итоговыми последствиями – отказ от использования той или иной СЭБ, то есть в результате, как уже отмечалось, к ее нерентабельности и вообще неокупаемости, возможно, многомиллионных внедренческих и эксплуатационных расходов (чему в российском банковском секторе также имеются примеры). А в обществе возникнут и сомнения в квалификации персонала банка. Порочный круг!

В качестве только одного такого варианта можно привести многогранный и интенсивно развивающийся карточный бизнес. Главная беда здесь заключается в том, что само наличие возможностей осуществления карточных мошенничеств и наблюдаемое интенсивное использование их преступными элементами при негарантированном обеспечении возврата утраченных финансовых средств могут подорвать доверие клиентов кредитных организаций к карточному обслуживанию как разновидности электронного банкинга. Отсутствие полного доверия со стороны клиентов банков к данному виду услуг ДБО проявляется в первую очередь в том, что в подавляющем большинстве случаев пластиковые карты используются для получения наличных денег в банкоматах.

К сожалению, недостатки российского законодательства в части обеспечения предоставления финансовых услуг в

электронной форме не удается до настоящего времени компенсировать и с помощью законодательных актов, например принятием Федерального закона «О национальной платежной системе» (имеется в виду прежде всего многострадальная статья 9). На фоне отсутствия полноценного законодательства о предоставлении финансовых услуг «в электронной форме» это также свидетельствует о недостаточности паллиативных мер для обеспечения гарантий надежности вне офисной банковской деятельности. Сказанное относится и к другим видам ДБО. Поэтому кредитные организации фактически вынуждены самостоятельно находить эффективные и полноценные способы предотвращения ППД в киберпространстве, что не у всех из них хорошо получается.

Наиболее очевидные недостатки в организации ДБО российскими банками проявляются в организации договорных отношений с его клиентами и контрактных отношений с провайдерами, возникающими в ИКБД вместе с каждой новой ТЭБ. Эти недостатки очень серьезно затрудняют ведение соответствующей претензионной работы и крайне негативно сказываются на интересах указанных клиентов, в том числе в ходе судебных разбирательств (об этом еще будет говориться в подразделах 3.3 и 3.4).

3.2. Организация финансовых преступлений с помощью технологий электронного банкинга и воздействие на удаленных клиентов кредитных организаций

Как уже отмечалось, преступные сообщества и отдельные криминальные элементы во всем мире охотно применяют «высокие технологии» в своей противоправной деятельности. При этом в России они пользуются, с одной стороны, недостатками российского законодательства (включая Уголовный кодекс РФ), с другой стороны – отсутствием закрепленных в нормативных правовых документах «канонов» ДБО, и, в-третьих, недостаточной финансовой и компьютерной грамотностью клиентуры кредитных организаций. В случае ДБО речь всегда идет об использовании для организации инцидентов ППД маскировки злоумышленника той или иной средой информационного взаимодействия (тем же киберпространством). Руководству кредитных организаций никогда не следует забывать о том, что ППД – это непрерывный процесс, характеризуемый тем, что преступные сообщества постоянно изыскивают все новые способы ОД, совершения мошенничеств, а также хищения кон-

фиденциальной информации. Недостаточное осознание специфики электронного банкинга может привести к появлению серьезных проблем с управлением банковской деятельностью и контролем над ней в плане обеспечения ее надежности и соответствия установленным требованиям (то есть к потере полноценного управления и контроля). Поэтому руководству и персоналу высокотехнологичных банков необходимо отчетливо понимать, кто конкретно может являться агентами угроз, знать их образ действия и применяемые способы маскировки как ППД, так и самих этих агентов.

Для осуществления финансовых преступлений, в особенности ОД, чаще всего используется эффект анонимности пользователя, скрытого киберпространством, что позволяет реализовать многочисленные проводки (трансферы, транзакции) без личной явки в банк. При этом может имитироваться деятельность сколь угодно большого количества клиентов: главное – разжиться достаточным числом средств и полномочий удаленного доступа, для чего преступными сообществами обычно специально и тщательно формируется своя «клиентская база». Можно привести некоторые примеры из материалов реальных расследований.

Наиболее простой способ осуществления одновременно хищений и ОД может основываться, к примеру, на контракте на выполнение неких строительных работ, который заключается между фирмой-посредником и государственной организацией и который никогда не будет выполнен. Эта

фирма, в свою очередь, заключает договор с подставными компаниями, которые якобы должны выполнять строительные работы, и эти работы действительно как бы начинаются. Компания-»исполнитель» нанимает за некоторое денежное вознаграждение некое лицо, которое должно сыграть роль ее генерального директора. Такой «директор» является в небольшой банк, расположенный обычно в другом городе, предоставляющий услуги интернет-банкинга, открывает необходимый для осуществления финансовых операций счет, после получения первой фирмой (якобы исполнителем по контракту) бюджетных средств в крупном размере возникают невесть откуда взявшиеся компании со счетами в других банках, и начинается финансовая чехарда, причем, естественно, управление счетами осуществляется дистанционно, так что банк-посредник первый и единственный раз видит упомянутого директора, а поскольку компания иногородняя, то не возникает и мысли проверить ее местонахождение. После того как казенные деньги будут распылены по счетам подставных фирм и «выведены» из оборота, имитация бурной деятельности на объекте прекращается, затраты преступной группировки ограничиваются стоимостью возведения забора и кратковременной арендой технических средств и оказываются существенно меньше выделенных на производство заявленных работ, к примеру десятков миллионов рублей. Через некоторое время за дело берутся следователи, которые выясняют, что по своему юридиче-

скому адресу строительная компания никогда не находилась, ее генеральный директор в силу очень преклонного возраста успел своевременно скончаться, отправившись на свою традиционную прогулку, выяснить, кому он передавал средства и права доступа, невозможно, задействованные фирмы-однодневки исчезли, а установить с помощью функций и баз данных той же системы интернет-банкинга, откуда именно и кем осуществлялось управление счетами, невозможно, потому что необходимые для этого данные в составе СИ почему-то не фиксировались (а никто, собственно, и не обязывал банк это делать). В итоге следствие заходит в тупик, а виновных не найти, потому что в схеме были задействованы утерянные и фальшивые документы, бомжи и пр., однако сам банк уже вовлечен в преступную схему, а значит, с большой вероятностью попадает под подозрение в соучастии.

Речь может идти и о крупномасштабных закупках какого-либо оборудования за рубежом, которое отсутствовало в природе, и тогда дистанционное управление счетами в банках-посредниках может вестись как из Москвы, откуда выделяются бюджетные деньги компаниям, обещавшим такие закупки осуществить, так и из-за рубежа, где также окажутся зарегистрированы некие компании-посредники. Здесь счет может идти уже на сотни миллионов и даже миллиарды рублей, поскольку масштабы операций гораздо больше, а проверять целый ряд фирм-нерезидентов (для данного города), тем более зарубежных «партнеров», существен-

но сложнее. Опять-таки для операций выбирается какой-нибудь среднерусский «банчок», в котором доверенными лицами открываются счета для фирм-посредников, отечественных и зарубежных. Выделенные из бюджета суммы дробятся на несколько или множество финансовых потоков, в выбранном банке, располагающем системой интернет-банкинга, они в рамках ДБО конвертируются и переводятся на счета зарубежных фирм в России, после чего осуществляется их трансфер за рубеж. Никаких поставок, естественно, не происходит, но банк формально ничего не нарушает – в его системе интернет-банкинга и БАС происходят какие-то вполне законные операции, за IP-адресами он следить не обязан (то есть он может даже не фиксировать их, как и другую маршрутную информацию в составе СИ, и тем более не анализировать). Через какое-то время из банка начинают направляться запросы на документы, подтверждающие поставки оборудования, но, к сожалению, отвечать на эти запросы давно уже некому, а доверенные лица растворились на бескрайних российских и мировых просторах. В итоге на счетах в зарубежных банках оседают уже сотни миллионов долларов, однако реальные бенефициары остаются неизвестными, а руководство банка недоуменно пожимает плечами и объясняет следователям и Банку России, что никто не ожидал такого эффекта от дистанционного предоставления банковских услуг, и уж теперь-то ДБО лучше и не заниматься! Однако, немалые премиальные, по-видимому, получены…

ДБО через Интернет может использоваться и для подпольной банковской деятельности, при этом организуется имитация производственной, торговой и даже банковской деятельности, то есть в электронном трансфере фигурируют как реально существующие, так и не существующие бумажные» (или «пустые») банки. Одним из примеров является организация фиктивных поставок товаров и услуг за рубеж, за которые впоследствии взимается компенсация НДС, в том числе – в страны СНГ или бывшего СССР. При этом преступным сообществом организуется управляющий центр, в котором концентрируется большое количество идентификационных данных для обслуживаемых банками лиц и подставных фирм, якобы занятых упомянутой деятельностью, которая может продолжаться годами. Результаты ее оцениваются во многие десятки и сотни миллионов долларов, при этом в управляющем центре ведется свой бухгалтерский учет, а банкам, для того чтобы оказаться замешанными в таких операциях и потом – в числе подозреваемых, достаточно просто не обращать особого внимания на то, откуда ведется управление счетами, не анализировать СИ и не проверять реальное существование участвующих в имитируемой «деятельности» банков-контрагентов, предприятий, компаний, индивидуальных предпринимателей и т. д. Правда, в итоге может возникнуть необходимость каким-то образом оправдывать впоследствии перед контролирующими и правоохранительными органами свою невнимательность к тому, что

происходит под видом ДБО, или халатность…

В большинстве известных примеров ППД, связанной с финансовыми хищениями и ОД, применяется централизованная схема управления счетами, хотя немало и вариантов с распределенным управлением ими в разных банках, которых объединяет наличие систем ДБО. Велико и количество ситуаций, в которых используются фальшивые ордера клиентов ДБО, в особенности юридических лиц, со счетов которых деньги уходят на счета физических лиц, упоминавшихся «дропперов» (или «дропов»), обналичивающих денежные средства. Несмотря на то что количество подобных случаев велико и ситуации такого рода продолжают множиться, ни у руководства, ни у персонала банков не возникает мыслей хотя бы убедиться в том, что десятки миллионов рублей со счетов тех или иных фирм совершенно законным образом перекачиваются в карманы физических лиц, якобы выполнявших некие дорогостоящие работы. Подобных своего рода «разведпризнаков» можно набрать немало, причем их целесообразно было бы не только использовать в процессе ФМ, но и «увязывать» с процессом УБР, что должно было бы отражаться и во внутрибанковских документах. В этом могла бы проявляться активность высшего руководства банков, заботящихся о своей репутации.

Для прикрытия мошенничеств в киберпространстве используются различные приемы, варьирующиеся от задействования, как отмечалось, так называемых анонимных или

слепых прокси-серверов, которые позволяют скрывать истинное местоположение в мировой паутине злоумышленников, управляющих счетами, до сетевых атак типа Denial of Service (DoS) или наиболее опасных – типа Distributed DoS (DDoS)[63], которыми блокируются вычислительные мощности кредитных организаций и (или) их провайдеров. В то же время наибольший ущерб (по совокупности похищенных средств – за последние несколько лет счет уже идет на миллиарды рублей) наносится клиентам кредитных организаций.

Подавляющее большинство мошенничеств в отношении клиентов ДБО – физических лиц основывается на различных методах так называемой социальной инженерии. Многие виды мошенничеств такого рода, широко распространявшиеся за последние 30 лет в Западной Европе и США, в российских условиях оказались непопулярными из-за исторических различий в развитии инфраструктуры и информационных технологий (скажем, атаки через центры обслуживания или внутриведомственные коммутаторы), вследствие чего здесь они не рассматриваются. Вместо этого весьма быстрое развитие получили способы реализации приемов «социального инжиниринга» на основе вариантов мобильного банкинга. В свою очередь, примерно 70–80 % из них[64]

---

[63] Атака типа «распределенный отказ в обслуживании».

[64] Оценка автора (Л. Лямина) по данным литературы и собственных исследований, хотя встречаются и оценки в 90 %.

ориентированы на обман владельцев карточных счетов. Ниже приведены отдельные примеры типичных попыток совершения мошенничеств на основе приемов такой разновидности социального инжиниринга (которые тем не менее нередко срабатывают):

• «Проверка персональных данных, перезвоните по указанному номеру телефона».

• «Ваша карта заблокирована, необходимо сообщить пин-код службе безопасности банка по телефону…»

• «Ваша карта заблокирована, необходимо связаться со службой безопасности по указанному номеру телефона».

• «Ваша карта заблокирована Центральным банком РФ, необходимо связаться со справочной службой по указанному номеру телефона»[65].

• «Отдел безопасности: ваша карта заблокирована, для разблокировки необходимо сообщить ПИН-код».

• «Ваша карта заблокирована по инициативе банка, срочно оплатите долг 1000 рублей. Телефон…»

• «Операции по вашей банковской карте временно приостановлены, справка по указанному телефону».

• «Действие вашей карты приостановлено ввиду взлома ПИН-кода, перезвоните по указанному номеру телефона».

• «Была попытка взлома ПИН-кода, ваша карта заблокирована, срочно перезвоните по указанному номеру телефо-

[65] Банк России в сообщениях такого рода упоминается часто, видимо, «для солидности».

на».

• «Ваша карта заблокирована, для разблокировки необходимо подойти к ближайшему банкомату и выполнить следующие действия…»[66]

• «Была попытка перевода денег с вашего счета, перезвоните по указанному номеру».

• «С вашей карты списано xx xxx рублей, перезвоните по указанному номеру».

• «С вашего счета произойдет списание на сумму xx xxx рублей, инфо по телефону…»

• «Ваша заявка на перевод в сумме xx xxx рублей принята, перезвоните по указанному номеру».

• «Подготовка перевода на сумму xx xxx рублей с вашего счета завершена, для справки позвоните по указанному номеру телефона».

• «Для подтверждения платежа по вашей карте в размере xx xxx рублей позвоните по указанному номеру телефона».

• «Вам звонят из банка ***, зайдите в интернет-банк и введите пароль…»[67]

• «Вам звонят из банка***, зайдите в интернет-банк, введите пароль и нажмите кнопку “Отмена”»[68].

---

[66] По командам злоумышленника клиент собственноручно переводит деньги на его счет.

[67] На дисплее клиента появляется изображение с веб-сайта-муляжа, практически идентичное настоящему диалоговому окну с веб-сайта банка, после ввода пароля происходит хищение денежных средств.

[68] На самом деле для кнопки «Отмена» в апплете запрограммирована команда

• «Введите подтверждающие данные для входа в интернет-банк…»

• «Была попытка входа в ваш интернет-банк, для предотвращения мошенничества перезвоните по указанному номеру и приготовьте данные по карте».

Любой звонок обеспокоенного клиента по предлагаемому номеру телефона влечет за собой «уговоры» сообщить данные персональной идентификации удаленного клиента или заставить его «выдать» их другими способами. Как видно, в подавляющем большинстве случаев используется достаточно примитивный подход (из-за чего многие клиенты сразу обращаются в свой банк), при этом интересно отметить, что мошенники зачастую даже не затрудняют себя сменой номеров телефонов, с которых звонят клиентам банков (а на условиях анонимности владельца номера этого и не требуется). Используются десятки вариантов социального инжиниринга такого рода и, что интересно, находятся люди, неоднократно «попадающие» под одни и те же приемы и, как следствие, теряющие деньги более одного раза. Как говорится, «для компьютерных программ могут существовать “заплатки”, но от человеческой глупости их придумать невозможно». Все перечисленные выше подходы (равно как и многие другие) банкам нужно иметь в виду и «обучать» своих кли-

---

подтверждения ввода, но клиент реагирует на само слово, полагая как раз, что ничего негативного не произойдет.

ентов противодействию таким «социальным» атакам, к чему можно добавлять и выпуск специальных памяток, информирование через Интернет и т. д.

Более «тонкие» методы используют своего рода «настройки» на клиентов конкретных сервисов и могут характеризоваться довольно специфической предварительной подготовкой, обескураживающей атакуемого клиента или завлекающего его в ловушку, например:

• Клиенту поступает телефонный звонок с сообщением якобы от сотрудника банка о блокировке карты и крупной суммы на карточном счете в связи со «взломом ПИН-кода», после чего для разблокировки предлагается сообщить реквизиты карты, что тот и делает.

• Клиенту поступает сообщение «Вы выиграли ноутбук, позвоните в банк по указанному номеру телефона»; когда клиент (любитель халявы!) звонит по указанному номеру, ему предлагают дать номер карты и ввести заданный код для перевода средств с его счета, что зачастую и происходит.

• Клиенту поступает телефонный звонок с предложением якобы от сотрудника банка о возможности льготного кредитования на крупную сумму, после чего следует запрос о его идентификационных данных, номере банковской карты и т. п.

• Клиенту поступает телефонный звонок с сообщением якобы от сотрудника банка о необходимости «войти в интернет-банк» и ввести предлагаемый в коротком сообщении,

пришедшем на его мобильный телефон, пароль в связи с тем, что надо отменить некую мошенническую операцию.

• Клиенту не удается инициировать сеанс ДБО, после чего ему поступает телефонный звонок с вопросом якобы от сотрудника банка о технических проблемах с ДБО и предложением ввода данных персональной идентификации в поля диалогового окна, которое выводится на экран его дисплея.

Можно было бы также привести десятки подобных примеров и данные о тысячах ежегодных целенаправленных атак на клиентов ДБО высокотехнологичных банков (и на сами банки с проникновениями в их сетевые структуры), при этом за счет низкой компьютерной грамотности клиентов и нередко безразличной позиции банков клиенты терпят убытки и потом предъявляют претензии тем же банкам[69]

[69] Детальный анализ карточных мошенничеств здесь не проводится, поскольку существует полноценная литература по данной проблематике, см., например: «Безопасность карточного бизнеса. Бизнес-энциклопедия» (разделы 1 и 3). – М.: МФПА; ЦИПСиР, 2012.

Конец ознакомительного фрагмента.