Антон Владимирович Пухов
Валерий Баулин
Леонид Витальевич Лямин
Дмитрий Леонидович Волков
Николай Пятиизбянцев
Максим Кузин
Павел Владимирович Ревенков
Ирина Лобанова
И. Н. Сачков

Мошенничество в платежной сфере. Бизнес-энциклопедия

Серия «Библиотека Центра исследований платежных систем и расчетов»

Текст предоставлен правообладателем
http://www.litres.ru/pages/biblio_book/?art=16898898
Мошенничество в платежной сфере: Бизнес-энциклопедия / Центр исследований платежных систем и расчетов: Интеллектуальная Литература; Москва; 2016
ISBN 978-5-9614-2389-1

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.

Содержание

Предисловие 5
1. Мошенничество в системах дистанционного банковского обслуживания (ДБО) и электронных денег 6
1.1. Практика мошенничества в системах ДБО 6
1.2. Российский рынок электронных денег 24
1.3. Портрет пользователя электронных денег, потребительское поведение 26
1.4. Схемы мошенничества, способы информирования пользователей и методы профилактики 27
1.4.1. Вредоносное ПО 27
1.4.2. Фишинг 27
1.4.3. Методы, рассчитанные на доверие пользователей 28
1.5. Распространенные виды мошенничества в сфере электронных денег 29
2. Электронные платежи: риск возможного использования для легализации преступных доходов 31
2.1. Общая модель отмывания денег 32
2.2. Электронные платежи 37
2.3. Использование систем электронных платежей для отмывания денег 40
2.4. Уроки Liberty Reserve 43
Конец ознакомительного фрагмента. 46

Мошенничество в платежной сфере. Бизнес-энциклопедия

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*
Корректор *И. Астапкина*
Арт-директор *Л. Беншуша*
Компьютерная верстка *М. Поташкин*

* * *

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)

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 организованные 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 обозначение 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 несанкционированного 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 специализированных 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 выбирать 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.

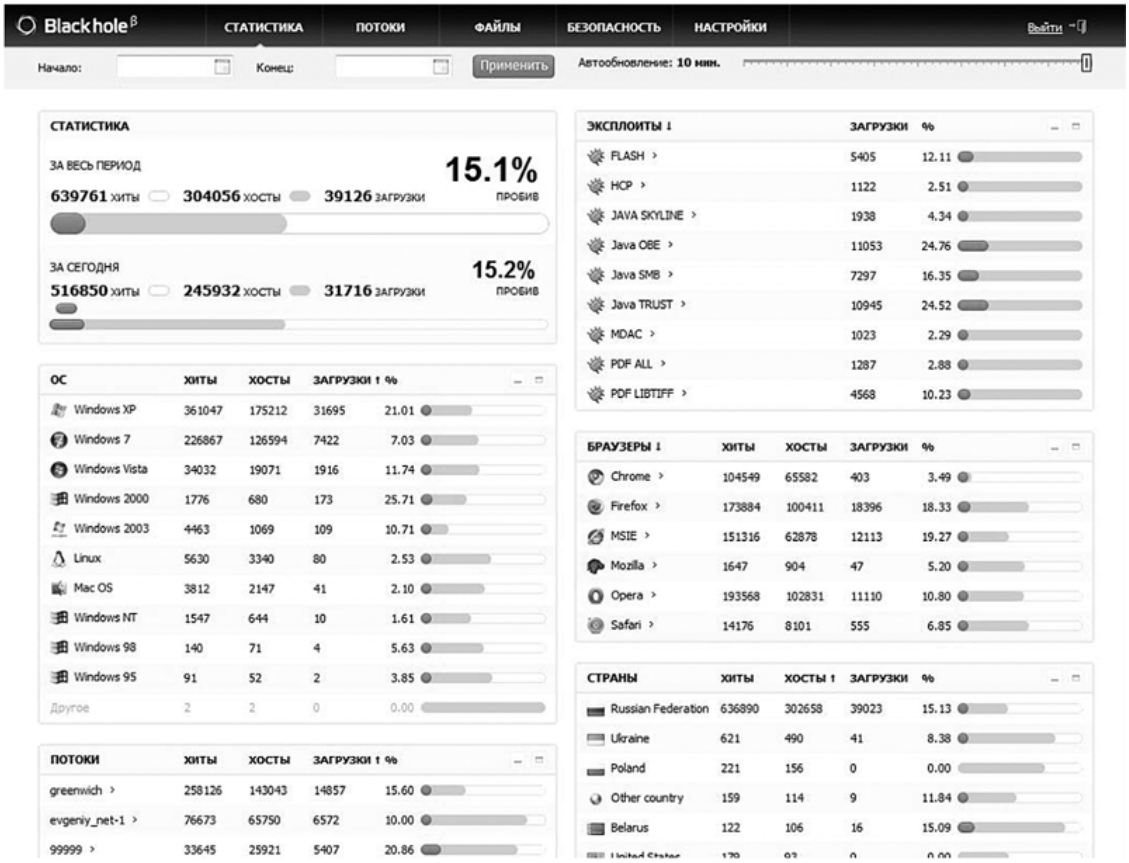

Рис. 1.2. *Панели управления связки эксплойтов Black Hole*

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.

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 развернуто 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.

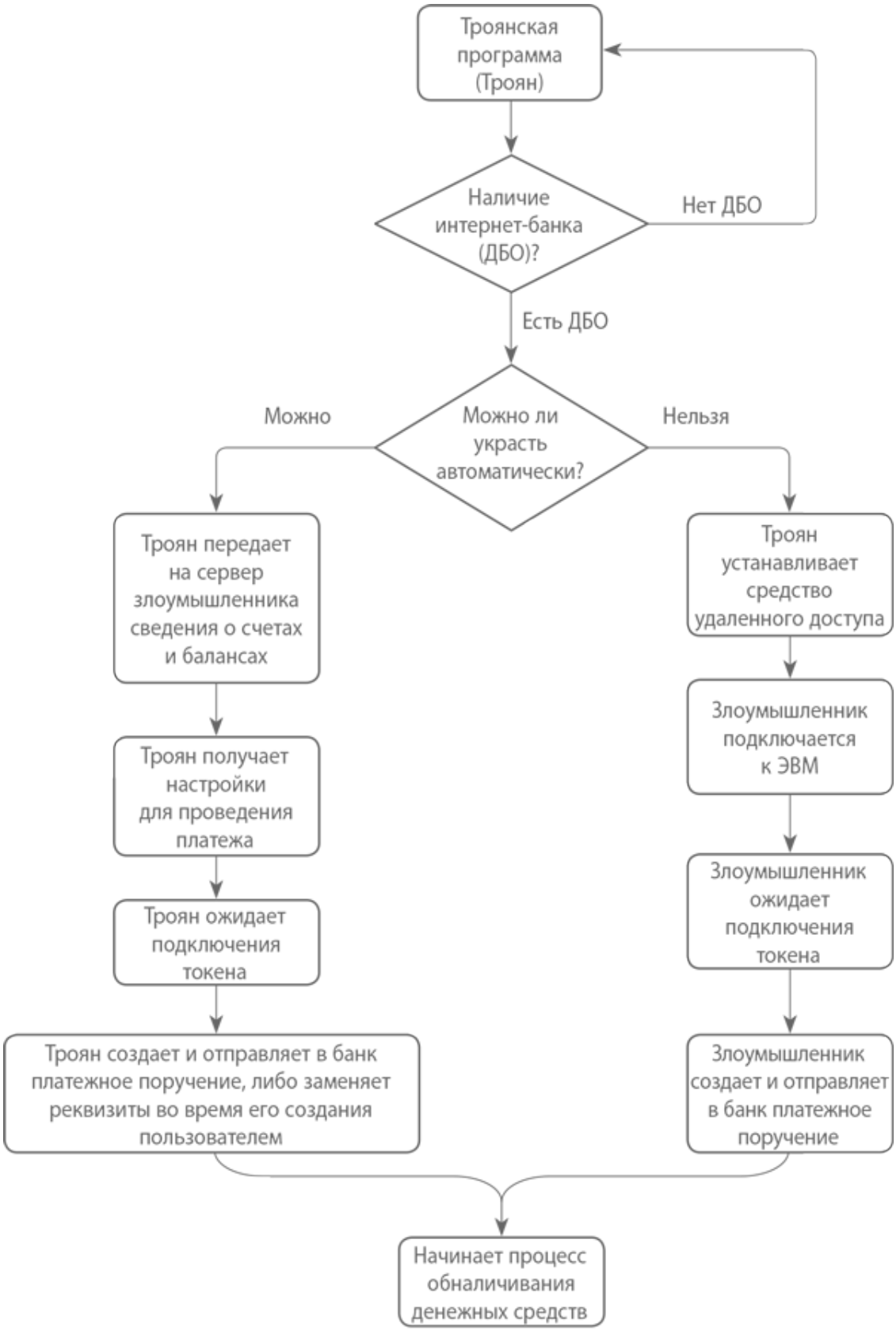

Рис. 1.4. *Блок-схема хищения денежных средств с помощью троянской программы*

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.

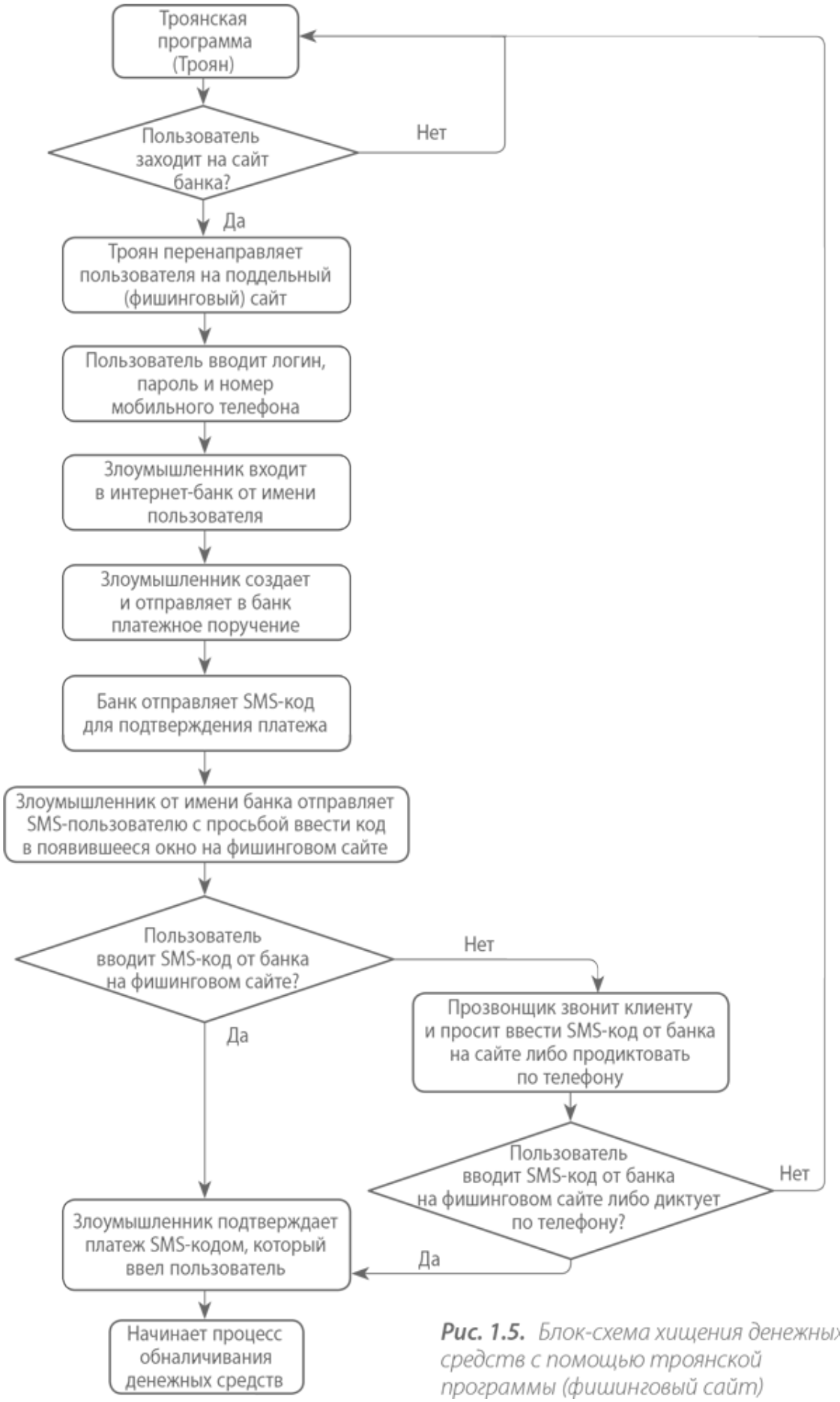

Рис. 1.5. *Блок-схема хищения денежных средств с помощью троянской программы (фишинговый сайт)*

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.

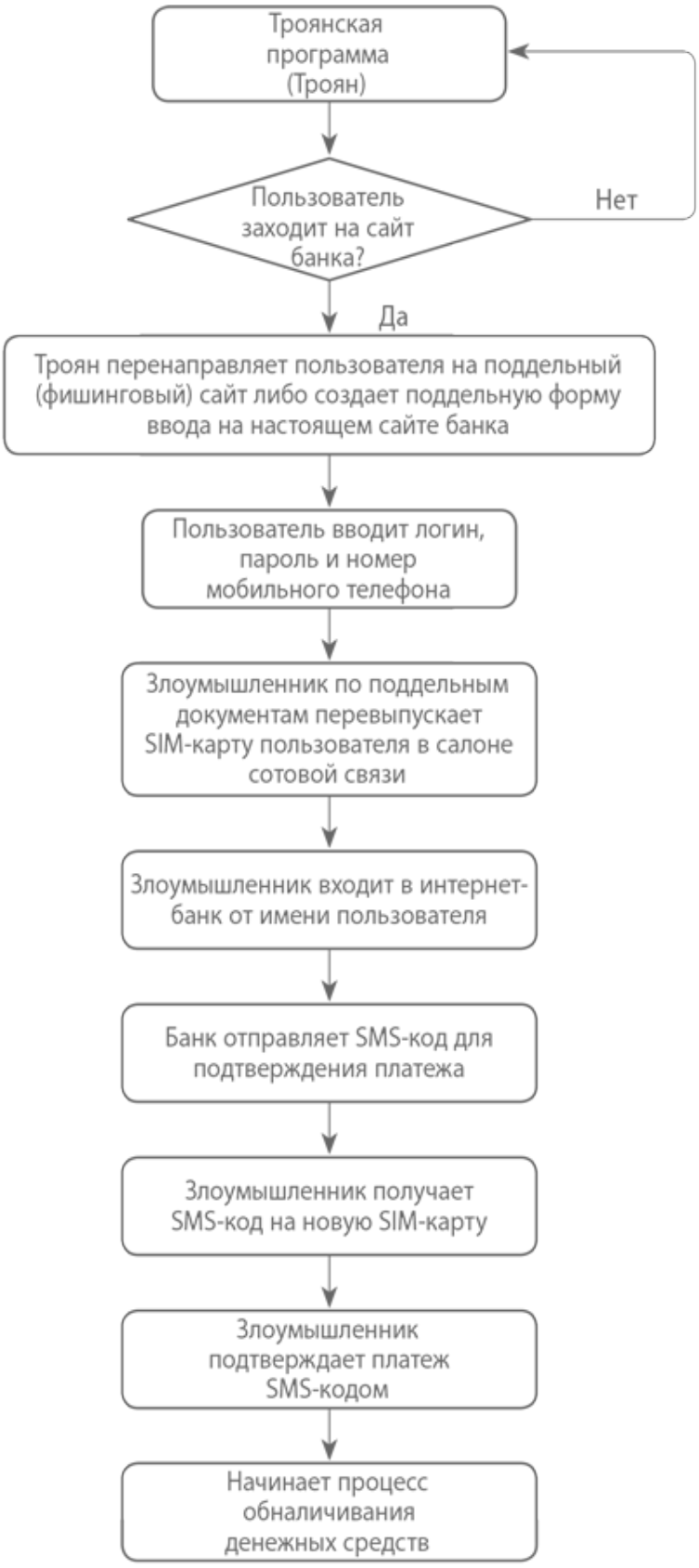

Рис. 1.6. *Блок-схема хищения денежных средств с помощью троянской программы, перевыпуск SIM-карты*

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.

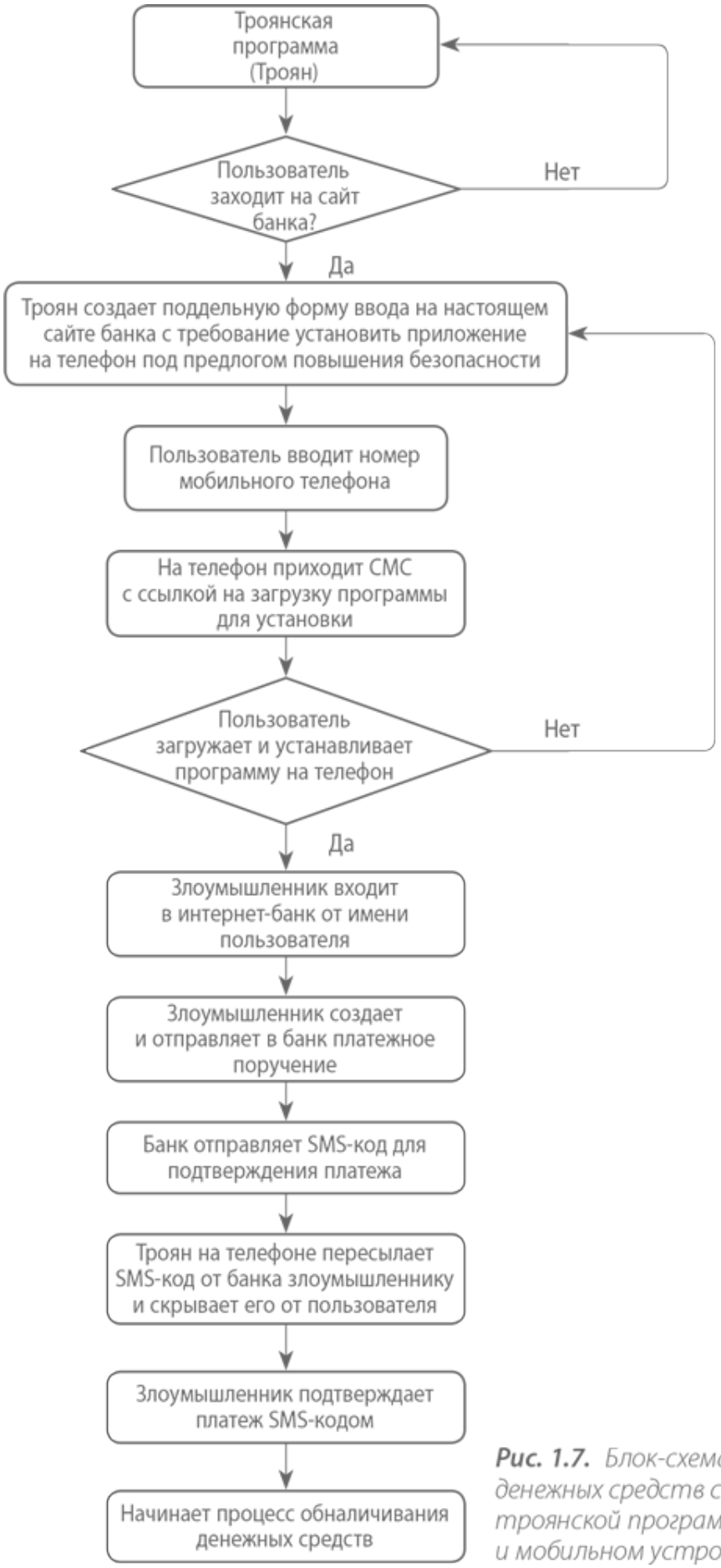

Рис. 1.7. *Блок-схема хищения денежных средств с помощью троянской программы на компьютере и мобильном устройстве*

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.

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

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.

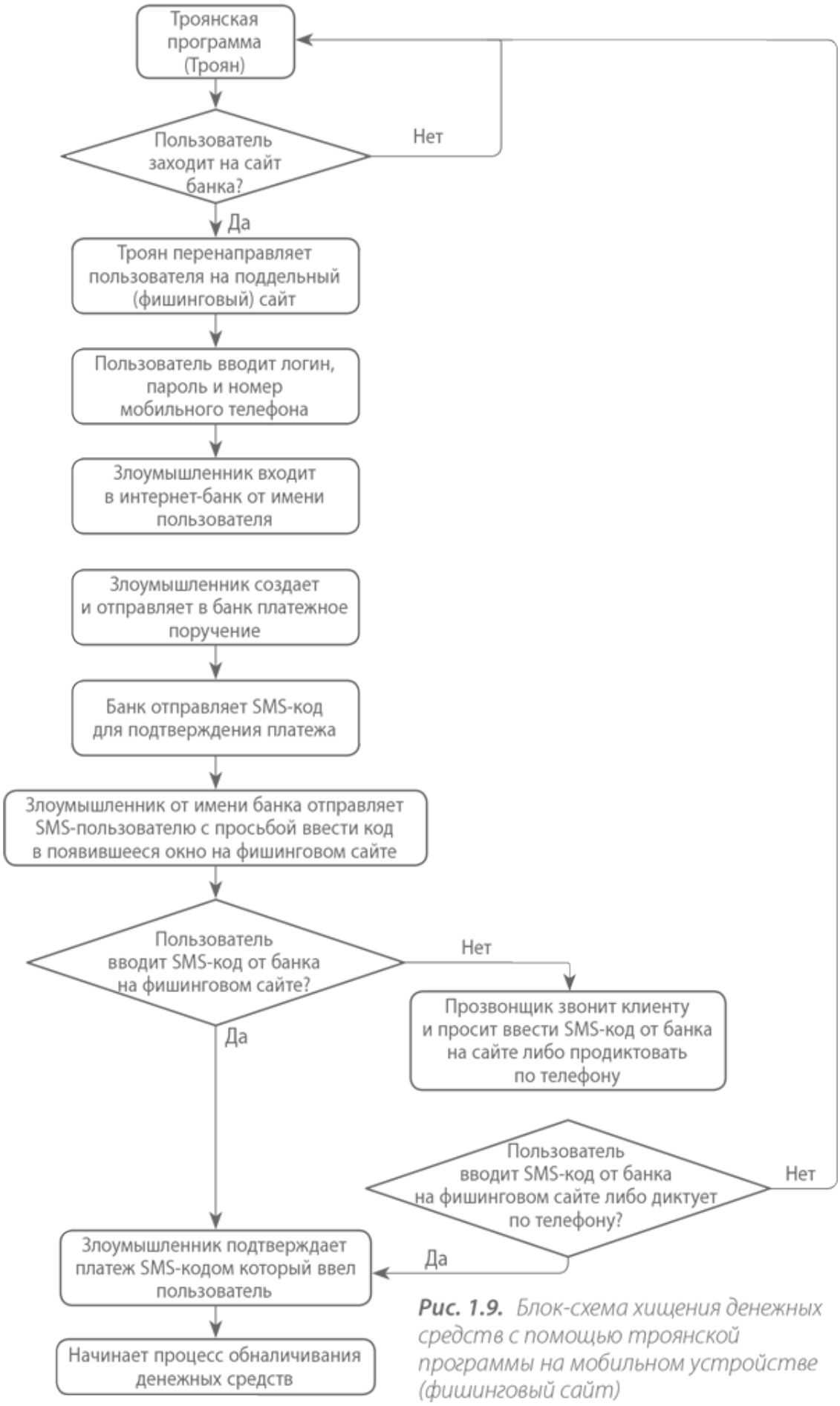

Рис. 1.9. *Блок-схема хищения денежных средств с помощью троянской программы на мобильном устройстве (фишинговый сайт)*

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.

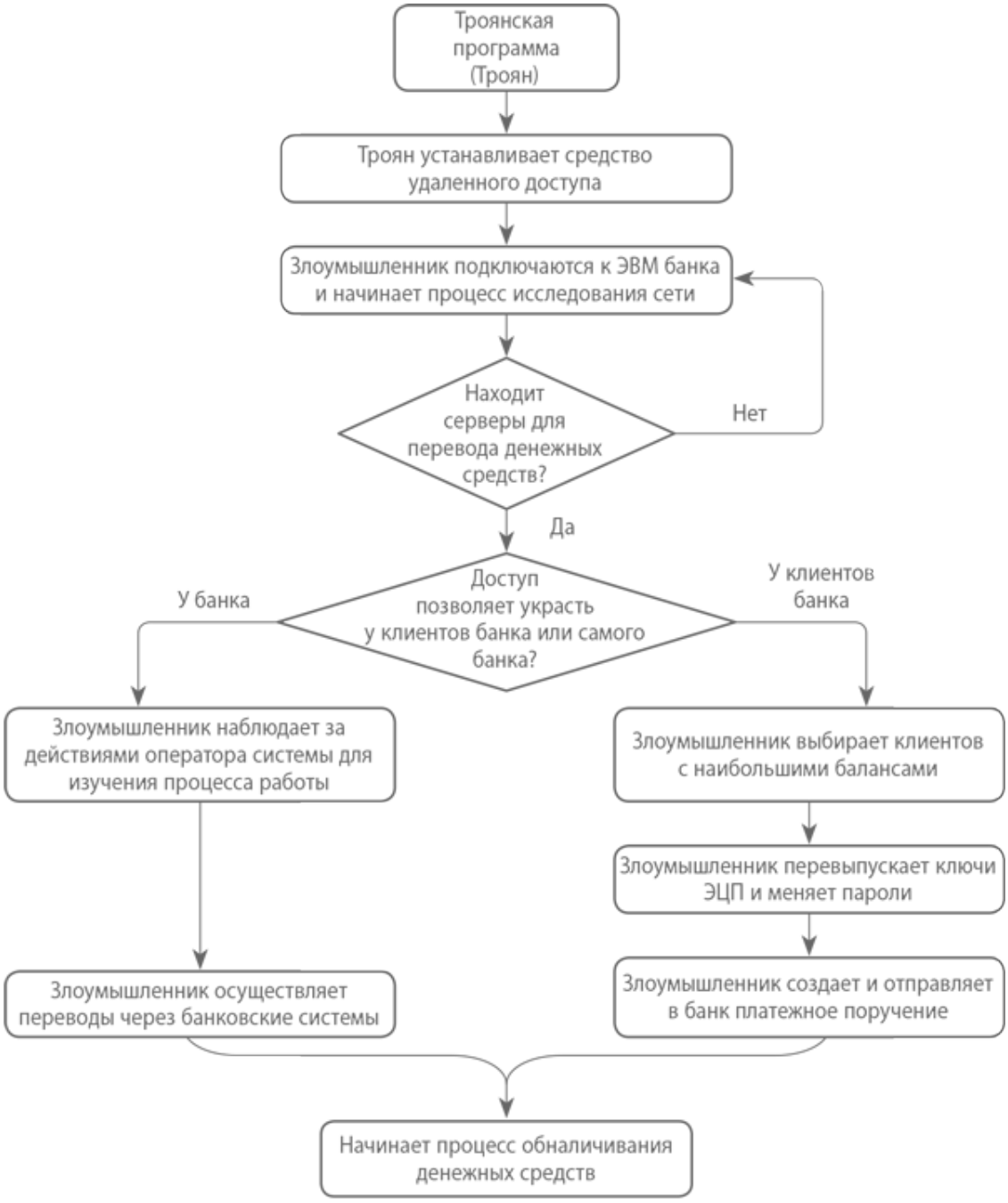

Рис. 1.10. *Блок-схема хищения денежных средств через компрометацию системы банка*

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. Процент зависит от условий работы и оговаривается в начале взаимодействия.

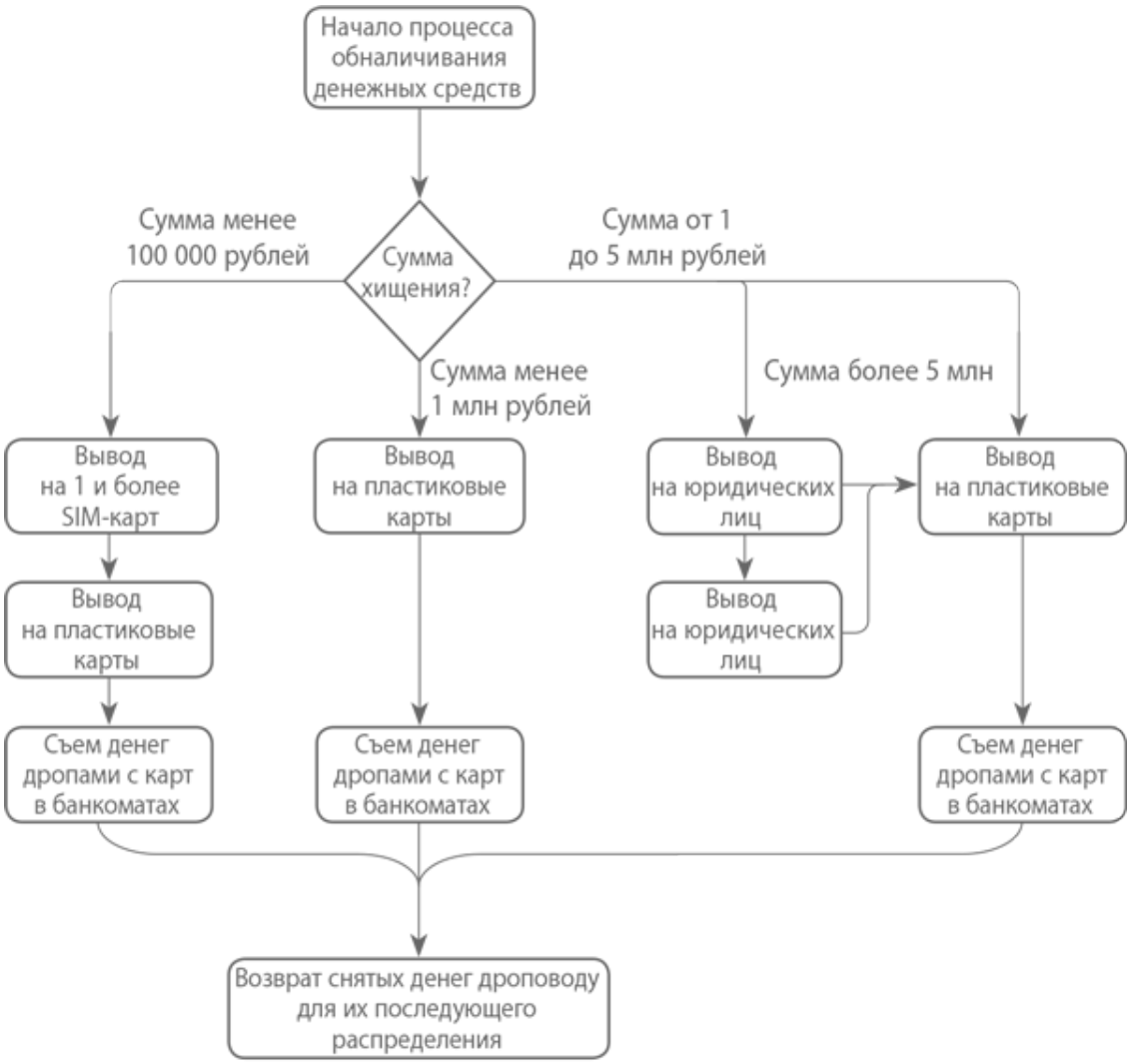

Рис. 1.11. *Процесс обналичивания похищенных денежных средств*

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.

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 транзакций. Это обусловлено целым рядом причин.

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 ситуация 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 перечисленных 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 кошелька 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 пользователя.

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. Такие 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 мошенники 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.

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 международными 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 созда-

[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.

ются 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).

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.).

[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.

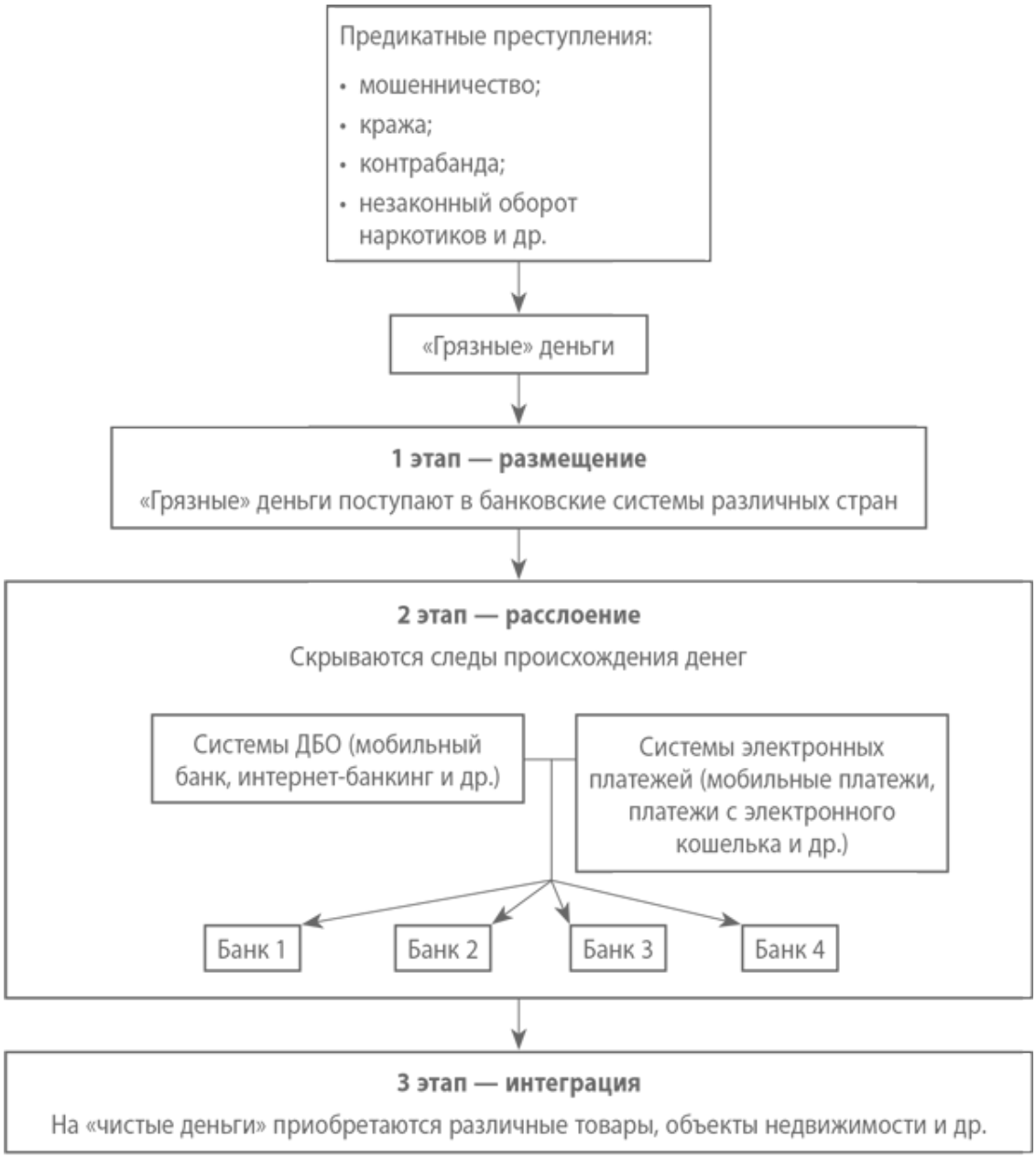

Рис. 2.1. *Обобщенная схема отмывания денег с использованием технологии ДБО и систем, осуществляющих электронные платежи*

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 **под-**

рыв 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 нерыночные 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 серьезных 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

[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.

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.

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, позволяющих 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 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 уни-

---

[7] По данным Российского отделения IDC, во II квартале текущего года было поставлено около 1 960 000 планшетов, что, по оценкам IDC, 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.).

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

чтожения. 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 организации 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 посредничестве 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 предложил 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].

---

[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).

[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.

[13] В 2001 г. Европарламент ввел требование обязательной идентификации клиентов, которое распространяется на операции, превышающие €150 000.

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 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.

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

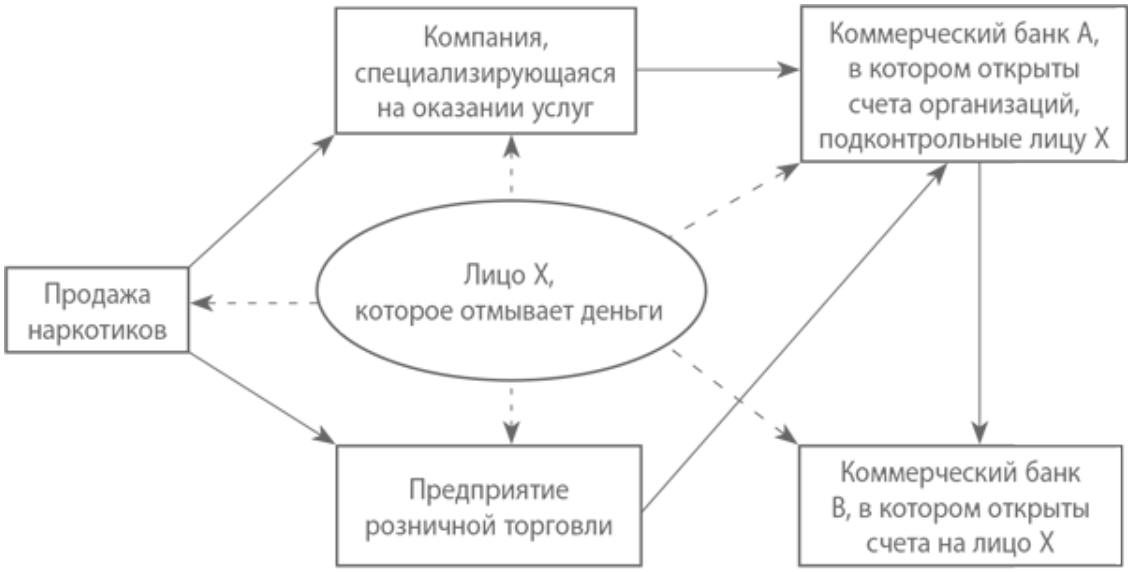

Рис. 2.2. *Схема легализации денежных средств от продажи наркотиков, с использованием одноразовых карт номиналом до $100*

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).

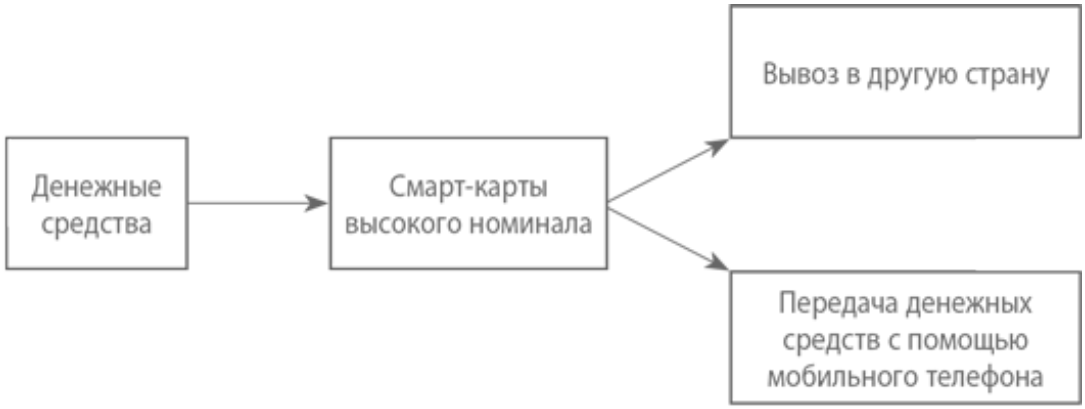

Рис. 2.3. *Схема передачи денежных средств с использованием смарт-карт высокого номинала*

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 ана-

лиз поступающих денежных переводов и дальнейшее использование фондом денежных средств может значительно облегчить процесс выявления истинных целей создания таких фондов.

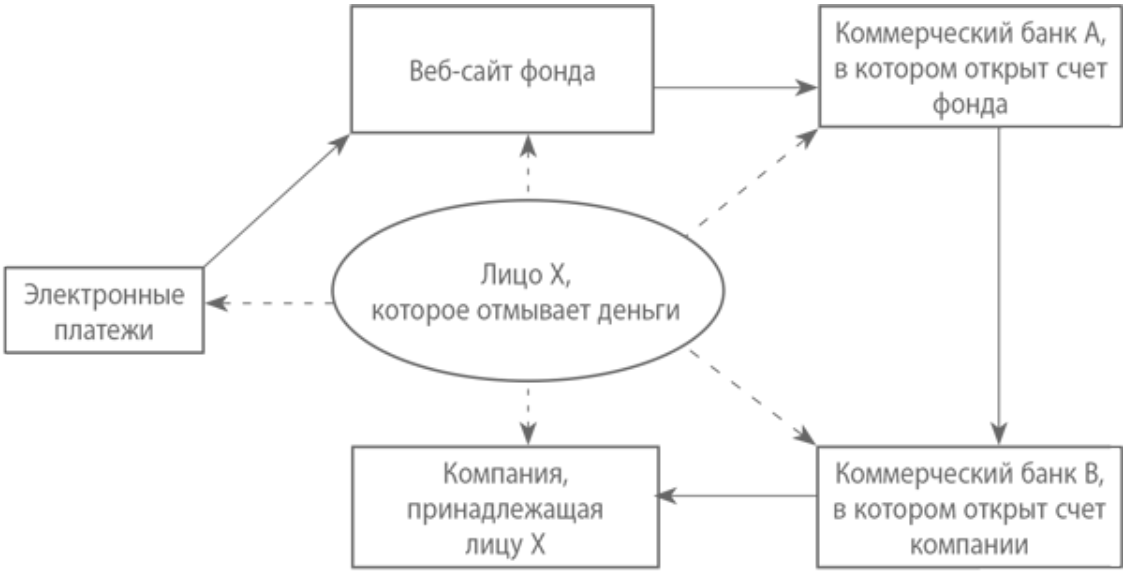

Рис. 2.4. *Схема легализации денежных средств с использованием благотворительного фонда*

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

---

[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.

[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.

[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

носных кодов, распространителей мошеннических SMS-подписок, магазины краденых кредиток, сканов паспортов и т. п.

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

Напомним, что ранее аналогичный случай произошел с платежной системой компании E-gold. В отличие от современных электронных платежных систем E-gold была построена не на денежных единицах, привязанных к доллару или другой валюте. Вместо этого пользователям предлагалось покупать золото или другие драгоценные металлы (серебро, платину и палладий), находящиеся на хранении у компании E-gold Ltd. На пике существования система проводила транзакции на $2 млрд в год[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 (Пособничество, 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 (IRS) 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 зрения противодействия отмыванию денег необходимо помнить, что деятельность по противодействию легализации доходов, полученных преступным путем, и финансированию терроризма является, скорее, вспомогательной. Необходимость в ней возникает не из-за «врожденных»

доходностью. В основном online-проекты, которые работают с электронными валютами.

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

[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.

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.

Конец ознакомительного фрагмента.