СОДЕРЖАНИЕ

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.

Изображение панели управления связки эксплойтов Black Hole показано на рисунке 1.2. Основным параметром, характеризующим связку эксплойтов, является коэффициент «пробива» — это

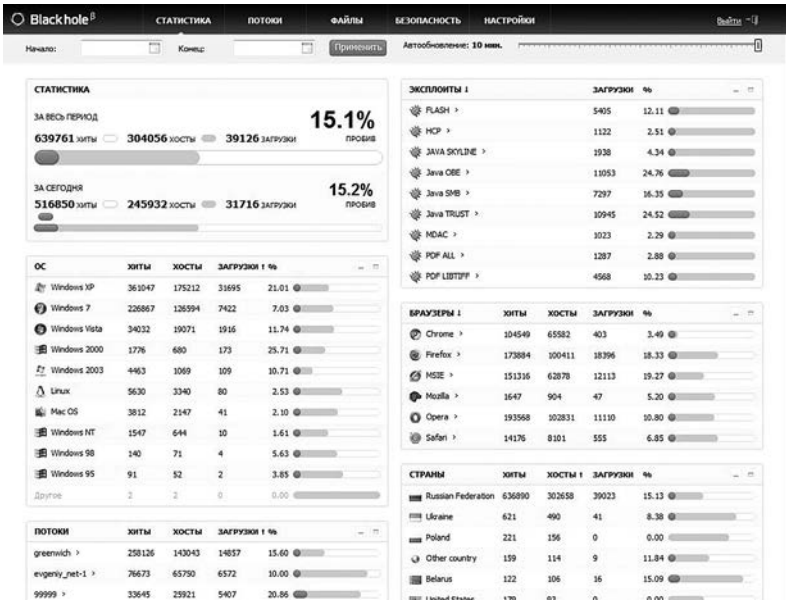

Рис. 1.2. *Панели управления связки эксплойтов Black Hole*

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.

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.

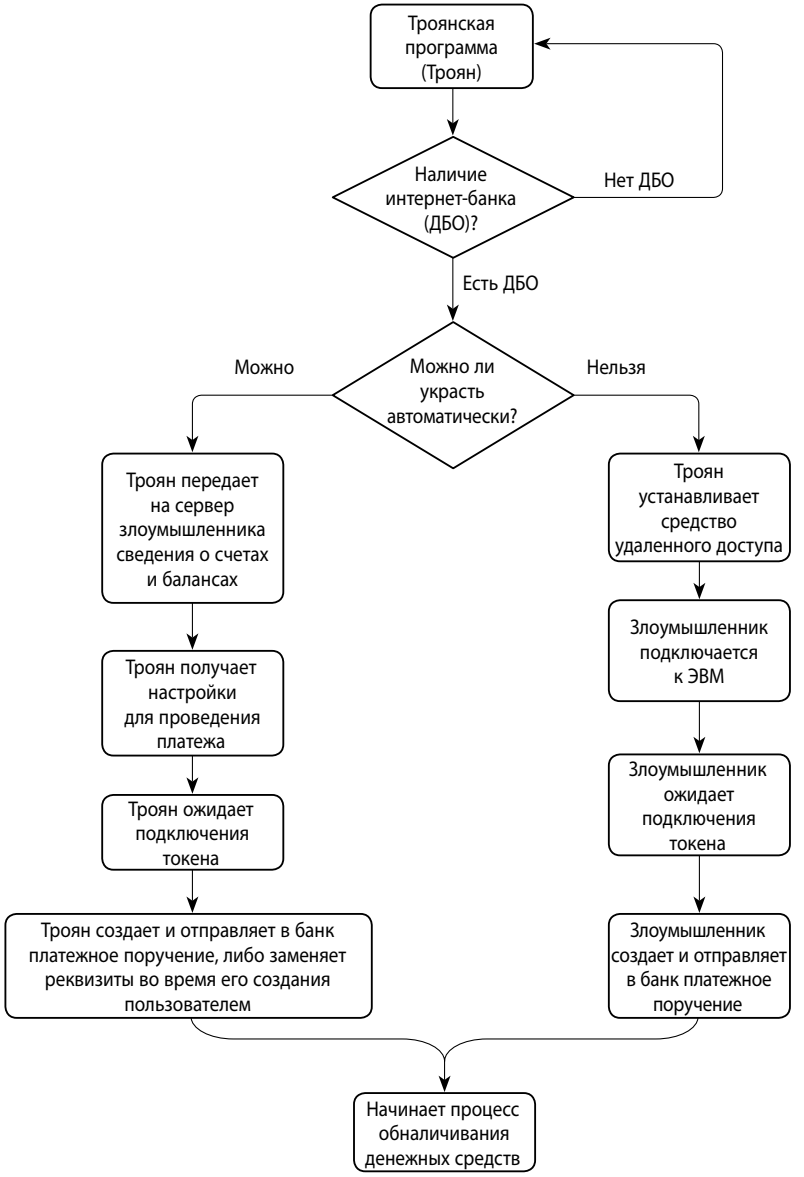

Рис. 1.4. *Блок-схема хищения денежных средств с помощью троянской программы*

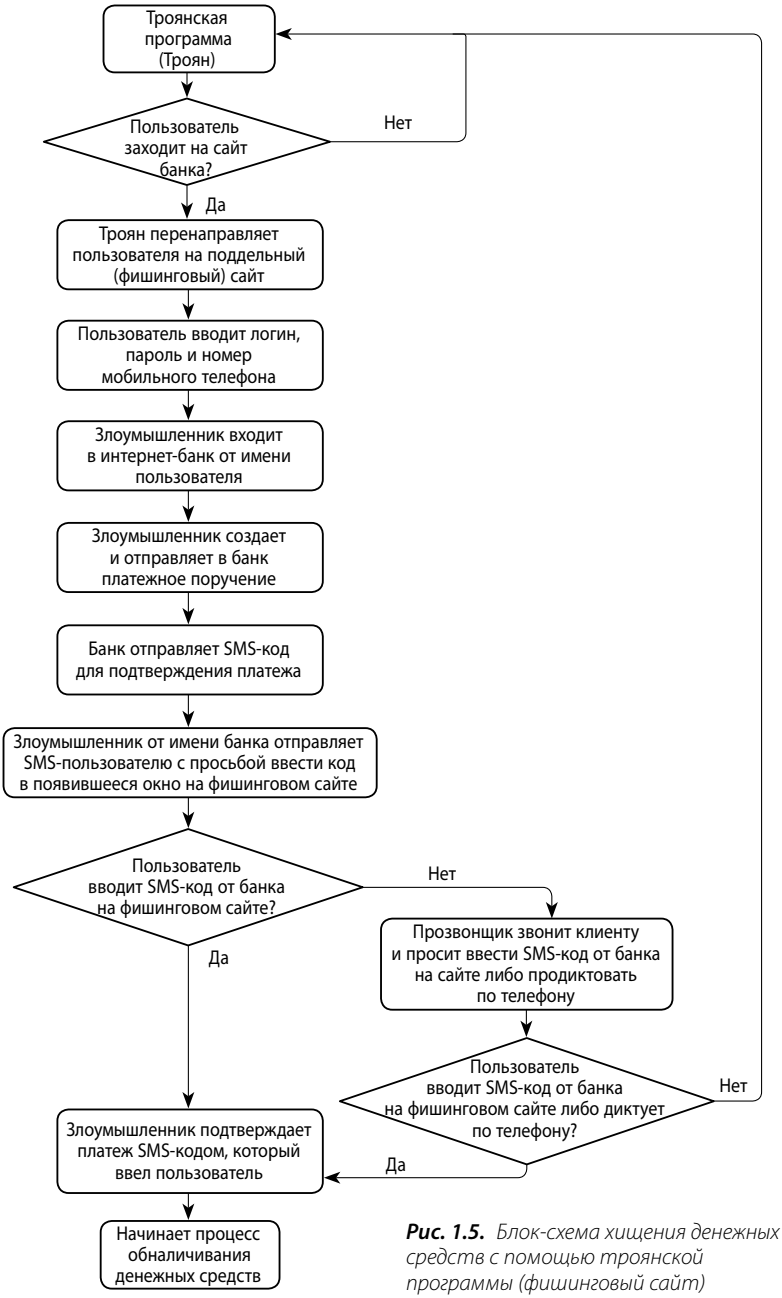

Рис. 1.5. *Блок-схема хищения денежных средств с помощью троянской программы (фишинговый сайт)*

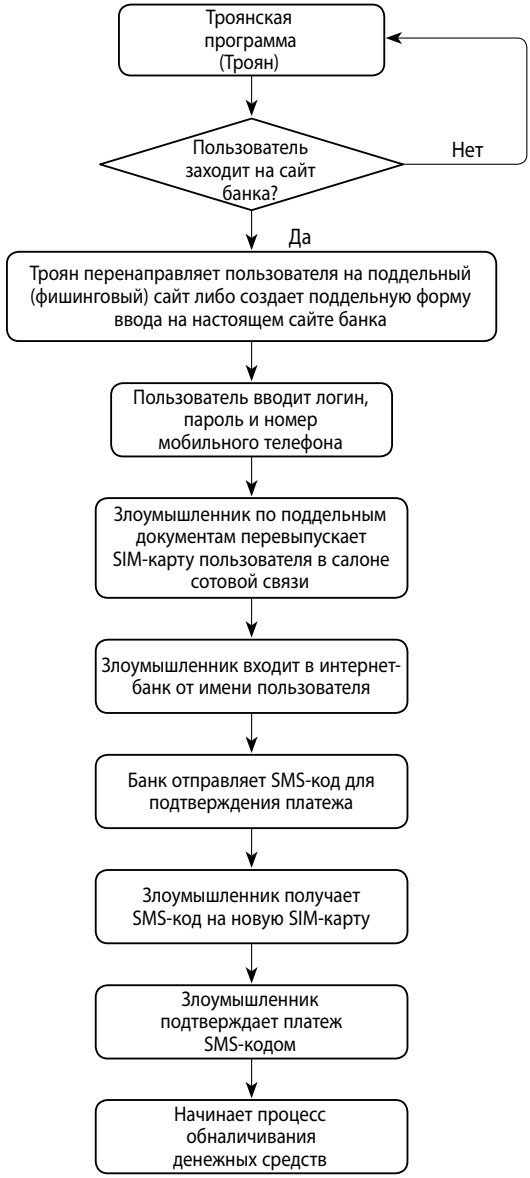

Рис. 1.6. *Блок-схема хищения денежных средств с помощью троянской программы, перевыпуск SIM-карты*

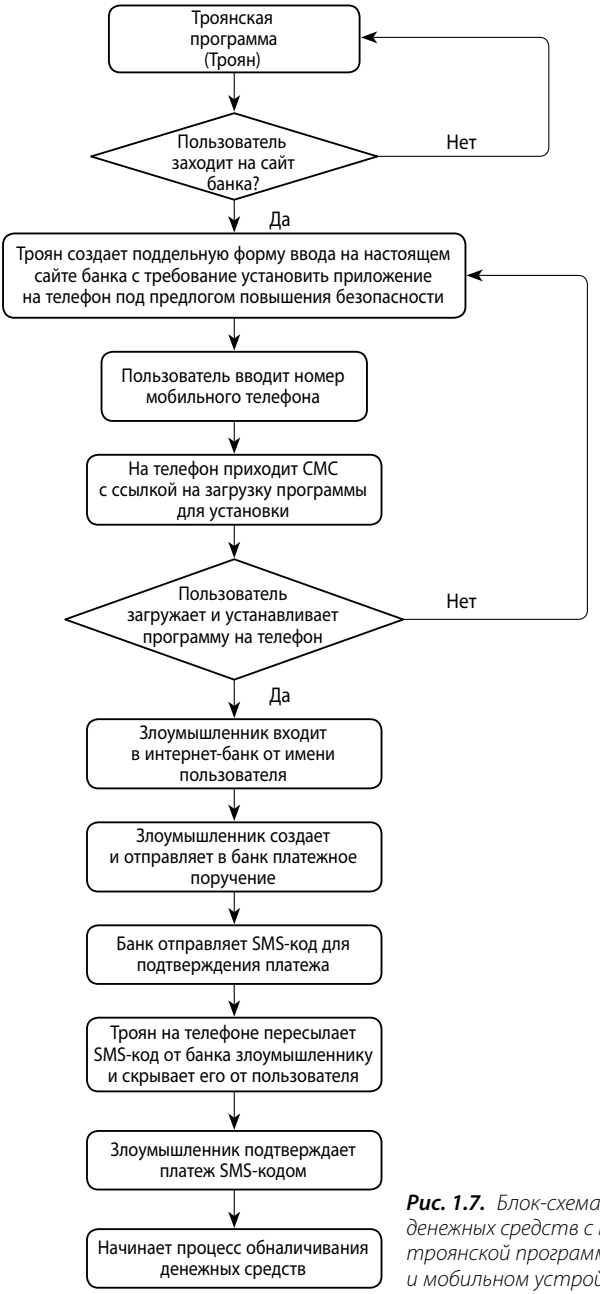

Рис. 1.7. *Блок-схема хищения денежных средств с помощью троянской программы на компьютере и мобильном устройстве*

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. Процент 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*

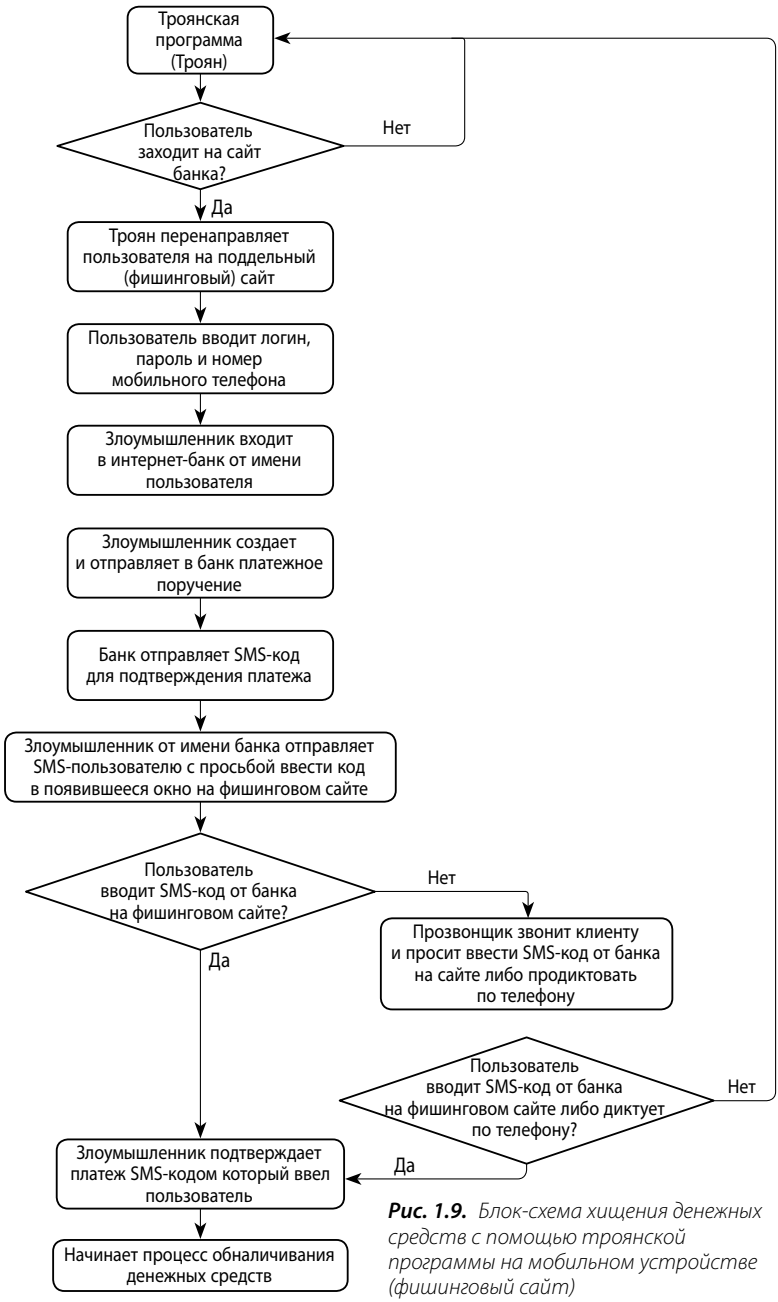

Рис. 1.9. *Блок-схема хищения денежных средств с помощью троянской программы на мобильном устройстве (фишинговый сайт)*

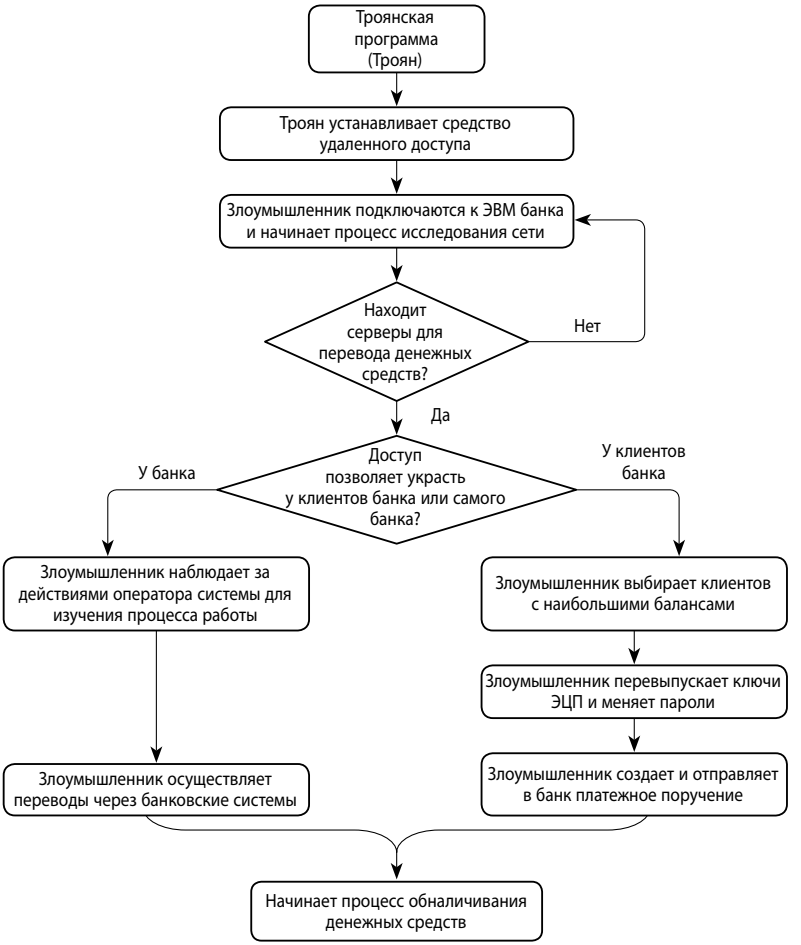

Рис. 1.10. *Блок-схема хищения денежных средств через компрометацию системы банка*

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 транзакций. Это обусловлено целым рядом причин.

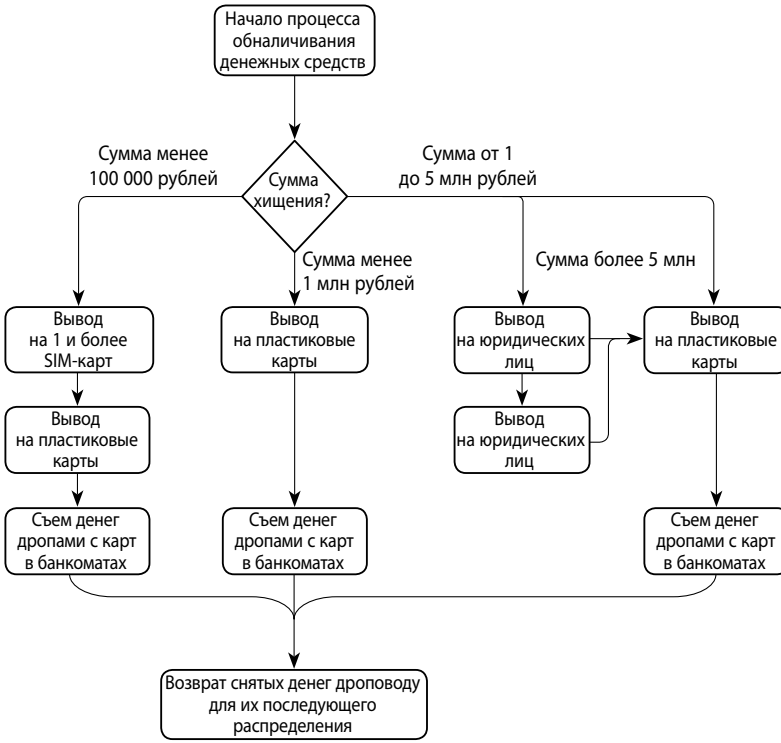

Рис. 1.11. *Процесс обналичивания похищенных денежных средств*

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 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).