# Мошенничество в системах электронных платежей

*А.В. Пименов, генеральный директор*
*ООО «Агентство экономической безопасности "Защита бизнеса"»,*
*А.Е. Изотов, эксперт-криминалист ОАО «БИНБАНК»*

**Мошенничество в современном мире отличается исключительной многоликостью, динамизмом и способностью к модернизации. Важнейшее значение приобретают информационные технологии, особенно в сфере бизнеса и финансов, все чаще общение между людьми и организациями происходит с помощью новейших средств коммуникации: от мобильных телефонов до Интернета.**

Развитие систем электронных платежей и взаиморасчетов повлекло за собой и совершенствование методов преступных посягательств на расчетные счета физических и юридических лиц. Основной целью мошенников попрежнему остаются карточные и расчетные счета физических лиц.

Мошеннические и другие противоправные действия в электронных системах обычно разделяют на две основные группы:

– действия, связанные с завладением идентифицирующей информации о расчетных и карточных счетах, о данных пластиковых карт их владельцев, а также с созданием различных возможностей доступа к ним;
– действия, позволяющие обманным путем получить денежные средства физических лиц.

Что касается второй группы, то, по мнению специалистов, их не совсем корректно относить к видам электронных мошенничеств, поскольку электронные системы в данном случае используются только как средство обмана и очень редко включены в механизм получения незаконной прибыли.

Методы мошенников достаточно хорошо известны. Чаще всего они используют в первую очередь человеческие недостатки и неинформированность людей. И напомнить о некоторых существующих способах обмана лишний раз не помешает.

## Внимание: обычное мошенничество

Вот несколько схем, рассчитанных на доверчивость жертвы. Довольно распространенной является схема, имеющая название «6 кошельков».

В тексте спамерского сообщения предлагается отправить некую не очень большую сумму (обычно несколько долларов или десятков рублей) на несколько предложенных кошельков, потом удалить первый или последний (по-разному пишут) и вписать в конец или начало свой адрес, после чего массово рассылать то же электронное письмо дальше.

Дескать, со временем на следующих этапах те, кому придет от вас сообщение, отправят на ваш адрес деньги, а потом будут пересылать письма от вашего имени и еще другим адресатам, получившим от вас сообщение.

В общем, банальная схема финансовой пирамиды. Хотя в советские времена жители одной шестой части суши достаточно интенсивно играли в эту игру. Необходимо было отправлять 10 рублей в конверте на первый адрес пришедшего вам письма, при этом вписав себя восьмым.

Теоретически выигрыш мог быть огромным, если бы не разного рода обстоятельства, то конверта нет под рукой, то лишнего червонца, а то и вообще хочется вписать себя первым. Цепочка нарушалась, пирамида рассыпалась, и ОБХСС не дремлет...

Вторая распространенная схема так и называется – **«Волшебный кошелек»**. В тексте спамерского сообщения рассказывается о том, что, дескать, есть такой замечательный кошелек, отправив деньги на который можно в ответ получить в 2 раза (или другое количество раз) больше.

Для правдоподобности могут также написать, что нужно посылать только определенные суммы, не больше какого-либо количества раз и так далее. Также для правдоподобности стали писать, что якобы нашли кошельки мошенников, которые воруют деньги таким образом, но при отправке незначительных сумм они умножатся. Естественно, что это все – мошенники.

Сумма денег, по их заверениям, при отправке на такой кошелек автоматически увеличивается и затем возвращается обратно адресатам.

Для правдоподобности нередко появление таких кошельков обосновывается увольнением из платежной системы озлобленного программиста, который решил наказать обидевших его начальников, забытыми тестовыми кошельками или другими причинами. Естественно, деньги просто уходят в кошелек мошенника, и ничего назад уже никому не возвращается.

Схема эта очень похожа на схему «6 кошельков», только здесь предлагается покупать некую программу или специальные электронные ключи.

Причем процесс «активизации» происходит поэтапно: есть либо 6 (или иное количество) программ/ключей, или уровней программы, или что-либо подобное. И каждый последующий этап дороже предыдущего.

Банальная схема финансовой пирамиды: сначала человек покупает первый уровень «программы», продает его какому-то количеству людей, затем покупает второй уровень и продает его тем, у кого купят первый уровень те, кому он сам продал первый уровень

или же тем же, кому он сам продал первый уровень. В общем, вариантов этой схемы множество, но их объединяет одно – это все мошенничество.

Еще один замечательный пример. И опять впереди планеты всей — Африка. На адрес вашей электронной почты приходит сообщение следующего содержания:

*«Здравствуйте! Я сын бывшего премьер-министра маленькой, но очень гордой черной страны Сааваты Мумба Кошачий Остров. Мой отец в течение 10 лет возглавлял Правительство нашей очень независимой республики. Он имел счета в Американском банке Нью-Йорк Клинтон-Буш Банк на сумму порядка 10 миллионов долларов. От Вас требуется помощь в обналичке этих средств. Ведь, как многие знают, после прихода очередного дерьмократического правительства счет моего отца был заблокирован. Сейчас моя мать сидит в тюрьме Кашатии, а брат болтается на виселице. Мне удалось чудом получить убежище в соседней Фейхоа-Авокадии, но я абсолютно не имею средств. Я нашел людей для разблокирования счета в американском банке, но для этого требуется 1 миллион долларов (или 100 тысяч). Если вы окажете мне помощь в разблокировании счета, то вы получите премию в 3 (5) миллиона. От Вас требуется...»*

К счастью, такие письма жителям России практически не приходят, а вот европейские небольшие финансовые, благотворительные организации и частные лица в свое время были завалены такого рода спамом.

А вот примеры мошенничеств, рассчитанных на жалость, а точнее, на глупость и излишнюю доверчивость человека.

*«Здравствуйте! Доход нашей семьи невелик, и я по мере возможностей стараюсь помочь. Так как я бедный школьник (студент), то я занимался нелегальным копированием и распространением пиратских дисков. Однажды мне поступил заказ на 10 дисков с Windows и Office. Я пришел на встречу, а меня скрутили спецагенты ФСБ (ЦРУ, ФБР, Моссад). Меня так избили, проломили череп и завели дело. Я месяц лежал в больнице, а когда вышел, то получил повестку. И когда я пришел в милицию, мне там сказали, что посадят где-то на пять лет. Но генерал сказал, что дело можно уладить за 200 (300, 500) долларов (евро). Помогите, пожалуйста, а то из-за зажиревших буржуев моя жизнь будет поломана. Деньги перечислите на WMZ(R)XXXXXXX или E-голд YYYYY.»*.

*«Доброго здоровья! Месяц назад к нам приблудился кот. Он был поранен злыми собаками. Кровь сочилась фонтаном из его лапок. Я выходил его, и он выздоровел. Мне мама давала денег на завтрак, но я покупал еду для больного котика. За это время он стал мне единственным другом, который не предаст и не продаст. Но беда в том, что у меня брат просто живодер какой-то. Он сказал, что сдаст его на шапку. Он бил моего друга ногой, обутой в кирзовый сапог! Впрочем, он сказал, что не тронет кота, если я ему дам 100 долларов. Люди добрые, помогите! Он такой чудный и ласковый! Он пушистый, белый, с серыми подпалинами. Не будьте черствыми, я хочу верить, что справедливость на свете существует. Деньги перечислите на WMZ(R)XXXXXXX.»*.

Во всех вышеперечисленных случаях электронные системы являются только способом передачи информации – спамерские рассылки, форумы и электронные платежные системы, доступ к которым никто не получал. Жертвы сами отправляли свои деньги мошенникам, поддаваясь на глупые рассылки. Это еще более прискорбно, что, когда жертву обманывают «лохотронщики», где угодно навязчиво предлагая свой ненужный товар или лотерею, на нее идет массированная психологическая атака, и жертва не всегда адекватна. Но если человек сидит дома в спокойной обстановке за своим компьютером, то на него очень сложно повлиять. К сожалению, это так, и мошенники, а также всякого рода аферисты получают свою долю преступного пирога.

## Банковские мошенники

Следует рассмотреть и поучительные примеры противоправных действий, направленных на получение доступа к электронным платежным системам. Чаще всего мошенники используют различные методы получения паролей и электронных ключей доступа к счетам, реже – прямые атаки на платежные системы.

В отношении юридических лиц мошенниками, как правило, используются тривиально простые методы завладения идентифицирующей информацией. Хотя в современной ситуации банки используют в системах «клиент-банк» достаточно сложные алгоритмы шифрования и электронной идентификации клиентов. Зачастую хищения денежных средств с расчетных счетов юридических лиц происходят по вине сотрудников фирм-клиентов.

Самой распространенной причиной является невнимательное отношение к хранению электронных съемных носителей информации (дискеты и флэшки), на которых записаны ключи к электронно-цифровой подписи (ЭЦП) клиента. Достаточно часто небольшие фирмы для оптимизации своих налогов нелегально и незаконно используют некоторое количество фирм-посредников.

Для обеспечения расчетов с клиентами в бухгалтериях таких организаций выделяется отдельный сотрудник для работы в системе «клиент-банк» с различными счетами в одном или нескольких банках.

Зачастую съемные носители с ключами ЭЦП в лучшем случае находятся в ящике стола у операциониста, а то и вообще разбросаны хаотично на столе. При этом все дискеты и флэшки, как правило, подписаны и указаны перечень и названия организаций, которым принадлежит ключ ЭЦП. Любой маломальски знакомый с системами «клиент-банк» специалист в IT-области легко может скопировать ключи ЭЦП и впоследствии воспользоваться нужной информацией для несанкционированного списания денежных средств со счета организации.

Ключами ЭЦП завладевают чаще всего либо сотрудники IT-подразделений компании, либо приглашенные специалисты, к примеру, для настройки неисправного системного блока.

После кражи денежных средств с использованием копии ЭЦП владелец денежных средств обращается в банк для их возврата. Но обычно бывает уже поздно, деньги уже прошли через несколько счетов и сняты наличными в другом городе. При поведении расследования совместно со службой безопасности банка выявляется такая же самая халатность с хранением ключей ЭЦП.

В отношении физических лиц методы завладения идентификационной или контактной информацией могут быть различными. От тривиальной кражи пластиковой карты, до установки дополнительного оборудования на банкоматы.

Достаточно распространенным методом получения необходимых для доступа к счетам клиента данным является так называемый метод «фишинг» (от английского слова fish – «ловить рыбу»).

Клиенту банка направляется сообщение с информацией о некотором техническом сбое в системе электронных платежей и просьбой перейти на указанную в сообщении ссылку.

Эта ссылка переводит клиента на страничку, практически полностью повторяющую страницу электронной системы банка, но при этом не имеющую к банку-эмитенту никакого отношения.

Клиенту предлагается ввести идентифицирующую информацию – ID клиента и пароль доступа.

Через некоторое время клиенту по электронной почте приходит сообщение о восстановлении работоспособности системы или клиенту перезванивает «сотрудник» банка с той же «информацией».

Этого времени мошенникам хватает на то, чтобы войти в систему и перевести деньги клиента по необходимым им реквизитам.

Хочется отметить, что ни один банк НИКОГДА не рассылал и не рассылает клиентам предложений о сообщении своих идентификационных данных.

В связи с повсеместным распространением банкоматов участились случаи противоправных действий с такими электронными устройствами.

При этом потерпевшей стороной может являться как клиент банка, так и сам банк.

Не так давно в США произошла серия достаточно поучительных краж из банкоматов. Как правило, банкоматы поступают от производителя с нулевым кодом доступа в систему настройки.

Случается, что банк-эксплуатант не всегда меняет этот код. Компьютер, управляющий банкоматом, находится за металлической дверцей, и подобрать ключи к ней не составляет труда.

Так вот, один бывший сотрудник фирмы-поставщика банкоматов, используя форменную одежду, вполне открыто и спокойно подбирал ключи к дверце. Затем входил в систему управления банкоматом, в настройках менял местами кассеты с однодолларовыми и стодолларовыми купюрами, снимая, таким образом, не один доллар, а сто.

Другой способ связан с установкой на банкомат специального оборудования, так называемого «скиммера». Данное устройство позволяет считывать данные с магнитной полосы пластиковой карты, а также получать информацию о PIN-коде владельца. С помощью полученной информации можно изготавливать дубликат карты и снимать с нее денежные средства. Кстати, такого рода устройства недавно были установлены на банкоматы нескольких московских банков. К счастью мошенники не успели воспользоваться своими устройствами.

Отдельное внимание стоит уделить широко применяемым в последнее время платежным терминалам. Владельцами терминалов являются в основном вовсе не платежные системы, как может показаться на первый взгляд. На самом деле платежные системы широко применяют для развития дилерских сетей, которые позволяют достаточно быстро нарастить объемы присутствия терминальных точек.

Торговая организация приобретает и устанавливает свой платежный терминал на своей территории, а затем получает комиссионный доход.

## Пример установки скиммера на банкомат

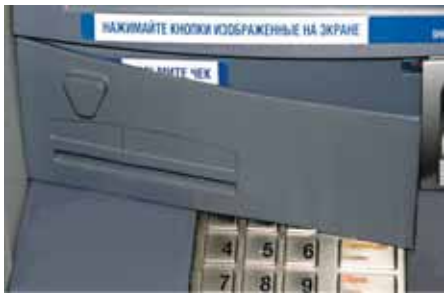
*Ил. 1. Общий вид фальшивой накладной панели и картридера*


*Ил. 2: а) общий вид банкомата;*

*б) общий вид банкомата с установленными фальшивой панелью и картридером*

*Ил. 3. Выступ со встроенной видеокамерой*

*Фальшивые панель и картридер крепятся на поверхность банкомата при помощи двухсторонней клеящей ленты.*
*После установки плоскость панели и картридера располагаются на одном уровне с корпусом экрана банкомата, в то время как конструктивно они должны располагаться ниже уровня корпуса экрана.*
*Характерная особенность: на фальшивой панели имеется выступ со встроенной миниатюрной видеокамерой, а также на панели отсутствует устройство выдачи чека.*

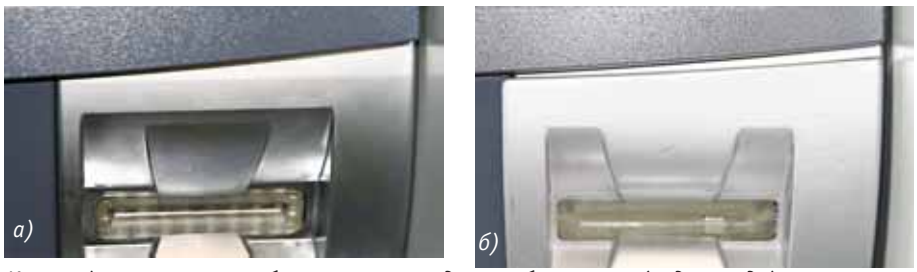



*Ил. 4. Способ установки фальшивой накладной панели*

*Ил. 5. Способ установки фальшивого картридера*


*Ил. 6. Общий вид фальшивых панелей*


*Ил. 7: а) общий вид картридера и клавиатуры банкомата;*
*б) общий вид установленной фальшивой клавиатуры и картридера на банкомат*




*Ил. 8: а) увеличенное изображение картридера на банкомате (вид спереди);*
*б) увеличенное изображение фальшивого картридера на банкомате (вид спереди)*

*Фальшивый картридер накладывается на настоящий и прикрепляется к нему при помощи двухсторонней липкой ленты. При этом появляется зазор между краем картридера и корпусом банкомата, и под ним может быть виден настоящий картридер. Красной стрелкой указан важный признак установки фальшивого картридера.*


*Ил. 9: а)увеличенное изображение клавиатуры на банкомате;*
*б) увеличенное изображение установки фальшивой клавиатуры на банкомат*

*Мошенники крепят фальшивую клавиатуру на настоящую. При этом накладываемая панель выступает над поверхностью корпуса банкомата, где может быть видна настоящая клавиатура. Красной стрелкой указан признак установки фальшивой клавиатуры.*

Но вот только, как в случае с американскими банкоматами, никто не утруждает себя обеспечением безопасности доступа к настройкам.

Некоторые сервисные службы для удобства обслуживания терминалов не отключают дополнительные возможности сенсорных мониторов, за исключением простого нажатия кнопок-картинок. Это позволяет, набирая необходимую комбинацию, входить в настройки операционной системы, получать доступ к каталогу установленных программ и совершать много интересных и неприятных в отношении платежной системы действий.

А еще мошенники, используя фишинг, направляют владельцам терминалов сообщения о необходимости переслать свои регистрационные данные в связи со сменой оборудования и так далее.

Ничего не подозревающие офисные работники владельца терминала, испугавшись отключения или выхода из строя оборудования, используемого ими для оплаты личных счетов, отправляют мошенникам все необходимые данные.

Затем на основании полученной информации создается XML-файл, который отправляется POST-запросом на сервер платежной системы. И все…

В заключение хотелось бы отметить, что чаще всего мошенничества как в обычной жизни, так и в электронных системах происходят из-за невнимательности людей.

Мошенники используют доверчивость граждан, порой их слабые знания и навыки при работе с платежными системами.

Помните: ни один банк никогда не пришлет вам сообщение с просьбой о предоставлении своих регистрационных данных. А что касается взлома самих платежных систем или доступа к точкам оплаты, то владельцы такого рода сервисов постоянно улучшают и модернизируют системы защиты. И на этом поле происходит постоянная борьба. Мошенники выискивают всё новые возможности для взлома, а платежные системы создаются с учетом всё новых средств защиты.