УДК 343.72:004

Е.С. Щербаков[*]

ПОНЯТИЕ КАРДИНГА В СОВРЕМЕННОЙ КОМПЬЮТЕРНОЙ ПРАКТИКЕ

Слово «кардинг» уже прочно вошло в лексикон наших правоохранительных органов. С развитием в экономики в нашей стране в обиход граждан прочно попала банковская пластиковая карточка, дающая неоспоримые преимущества перед обычными деньгами. Сейчас большая часть населения использует пластиковые карты для начисления и хранения заработной платы, пенсии; при оплате покупок как в реальных, так и в интернет-магазинах. Конечно, криминальный мир не мог обойти эту новую для него систему, связанную с деньгами.

Так что же такое кардинг? Кардинг (от английского carding) – род мошенничества, при котором производится операция с использованием банковской карты или ее реквизитов, не инициированная или не подтвержденная ее держателем. Проще говоря, кардинг – это незаконное получение реквизитов банковской карты различными способами для дальнейшего ее использования. Для лучшего понимания масштабов этого мошенничества приведем некоторые цитаты из доклада испанского производителя средств безопасности Panda Security «Черный рынок киберпреступлений».

«Когда я исследовал эту область в 2007 году, было только несколько мест, где можно совершить такого рода операции, и большая часть мест были расположена в России. Но теперь они везде. Так просто делать это, и мы, как индустрия, не можем их остановить», – говорит технический директор Panda Labs Луис Корронс.

И хотя электронные платежные средства пришли в нашу страну далеко не так быстро, как в страны западного мира, специалисты, ставшие впоследствии мошенниками-кардерами, начали формироваться именно в России. Хотя, конечно, полем их деятельности служат страны, где пластиковые карты используются на порядок чаще, чем в нашей стране, и соответственно, суммы находящиеся в оборотах, – выше.

Мошенничество в этой сфере приносит мошенникам очень большие деньги.

Ущерб почти в 25 млн. долларов причинили американским банкам два хакера из России. В ноябре 2000 года в США ФБР поймало хакеров из Челябинска: 20-летнего Алексея Иванова и 25-летнего Ва-

[*] Работа выполнена под руководством д-ра техн. наук, проф. ГОУ ВПО ТГТУ В.Н. Чернышова.

силия Горшкова. Россиянам удалось взломать компьютерные системы нескольких компаний и украсть номера кредитных карт, в частности они похитили 15,7 тыс. номеров кредитных карт из Western Union.

Несколько миллионов долларов сумел украсть из иностранных банков одессит Дмитрий Голубов. С помощью созданного им сайта Carderplanet.com примерно 7 тыс. мошенников-кардеров продавали друг другу краденые данные о банковских счетах по всему миру. Преступник был задержан 7 июля 2005 года и провел в тюрьме шесть месяцев.

Одним из самых масштабных преступлений в области кардинга считается взлом глобального оператора кредитных карт Worldpay и кража с помощью его данных более 9 миллионов долларов США. В ноябре 2009 года по этому делу были предъявлены обвинения преступной группе, состоящей из граждан СНГ. Взлом компьютерной сети филиала платежной системы RBS WorldPay в Атланте был осуществлен в 2008 году. Хакеры тогда скопировали сведения о владельцах платежных карт и их пин-коды. С использованием украденных данных были изготовлены поддельные банковские карты, и в течение 12 часов деньги были сняты в двух тысячах банкоматах по всему миру.

Благодаря высокому развитию Интернета кардинг стал одним из самых распространенных преступлений в сети. Одной из особенностей кардинга стало то, что потерпевшая сторона может находиться за тысячи километров от преступника. Также собираются преступные группы, члены которых могут находиться в разных странах, но с помощью современных информационных технологий действуют четко и организованно. Из-за различия законодательных систем в разных странах, по-разному характеризующих виды новых компьютерных преступлений и ответственности за них, преступники могут находиться в благоприятном месте для совершения компьютерного мошенничества и почти или вовсе безнаказанно совершать свои злодеяния. Все более совершенствующийся инструментарий и программные средства позволяют злоумышленникам выходить на новый уровень эффективности совершения преступлений, сокрытия улик и избежания наказания. Все это приносит правоохранительным органам большие трудности в расследовании таких преступлений, как кардинг.

В Российском законодательстве данный вид преступления проходит по статье 187 УК РФ.

Статья 187. Изготовление или сбыт поддельных кредитных либо расчетных карт и иных платежных документов.

1. Изготовление в целях сбыта или сбыт поддельных кредитных либо расчетных карт, а также иных платежных документов, не являющихся ценными бумагами, – наказываются лишением свободы на срок от двух до шести лет со штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет.

2. Те же деяния, совершенные организованной группой, наказываются лишением свободы на срок от четырех до семи лет со штрафом в размере до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период до пяти лет либо без такового.

Сразу видно, что понятие кардинга выходит за рамки данной статьи Уголовного Кодекса, так как при кардинге преступнику не нужна сама пластиковая карточка, а требуется только ее номер, проверочный CVV/CVV2 код (трехзначный или четырехзначный код проверки подлинности карты платежной системы), имя собственника карты и данные, связанные с собственником (адрес, телефон и т.д.). На основании этих данных преступник и совершает хищение денежных средств с карточки. По сути он не подделывает карточку, как материальный объект она ему не нужна, а просто незаконно использует секретные данные. Соответственно в его деяниях не присутствует сбыт (продажа) карточек, преступник продает лишь информацию о ней, т.е. состав преступления выходит на новый, виртуальный уровень, так как физические составляющие, а именно – платежные документы, отходят на второй план, а основополагающее место занимает информация об этих документах, а именно конфиденциальные сведения, хранящиеся в базах данных на компьютерных носителях.

Интересно, что если рассматривать кардинг поэтапно и разбить его на несколько последовательных стадий, то получится, что одним из первых этапов совершения преступления будет неправомерный доступ к информации, позволяющий использовать нужную банковскую карту для дальнейших целей, т.е. доступ к компьютерной информации. Данный вид преступления классифицируется статьей 272 УК РФ и подходит под вид компьютерных преступлений. Здесь же существует несколько оспариваемых нюансов, связанных с копированием информации, но в данном случае это является не столь принципиальным.

Неправомерный доступ к личным данным может быть осуществлен несколькими путями: с помощью программно-аппаратных средств и методов, таких как взлом системы (например, системы безопасности банка), проникновение в исходные коды приложений с целью завладения администраторскими правами и возможностями, а также внедрение вредоносных программ, с помощью которых также возможно получение конфиденциальной информации. Все это подходит к статье 272 УК РФ.

Но также имеются случаи, когда преступники получают данные банковских карт, вводя в заблуждение их собственников или злоупотребляя их доверием. Примерами являются случаи, когда люди получали ссылки на подставные веб-сайты несуществующих интернет-магазинов, где пытались купить какой-либо товар, формировали заказ и затем вво-

дили данные своих банковских карт. Соответственно никаких торгово-финансовых операций не происходило, а данные карт уже были получены мошенниками, а это уже классифицируется Уголовным Законодательством как мошенничество и проходит по статье 159 УК.

Далее злоумышленники занимаются изготовлением поддельных банковских карт с реквизитами жертв и дальнейшим их распространением – уже упоминаемая статья 187, относящаяся больше к «реальному кардингу».

Виртуальный же кардинг заключается в доступе к финансовым сбережениям, находящимся на банковской карте, и использовании их в виртуальном компьютерном пространстве – интернет-магазинах, электронных платежных системах и так далее.

Таким образом, очевидно, что кардинг при данном рассмотрении является многосоставным преступлением и, значит, должен регулироваться еще и статьей 69 УК РФ.

Таким образом, основываясь на развитии современных технологий, необходимо внести более четкие понятия, связанные с кардингом, обозначить новые нормы ответственности за преступления, для того, чтобы своевременно реагировать и противостоять им.

Рядовому же собственнику стоит принять меры безопасности своего имущества, а именно:

– открывать карточку в крупном банке, имеющем свой процессинговый центр и позволяющем оперативно контролировать остаток средств на счете;

– по возможности хранить деньги на нескольких картах;

– установить предел суммы, возможной для снятия с карты за один раз или за один день;

– использовать для финансовых операций только проверенные интернет-порталы, имеющие свои системы безопасности, избегать интернет-сайты сомнительного типа;

– при возникновении подозрений относительно банковских операций со своей картой сразу же взять выписку с банка со списком транзакций, реквизитами торговых точек, с которыми производились операции; попытаться опознать свои транзакции. При взломе банковской карты транзакции с нее идут небольшими суммами, но в течение нескольких дней наносят значительный урон.

СПИСОК ЛИТЕРАТУРЫ

1. The cyber-crime black market: uncovered // Panda security, 2011. – http://press.pandasecurity.com/press-room/reports/

Кафедра «Информатизация правовой деятельности» ГОУ ВПО ТГТУ