УДК: 343.721

Юрочкин Н. С.
магистрант, Кемеровский государственный университет

КИБЕРМОШЕННИЧЕСТВО: ХАРАКТЕРИСТИКА, ПРИЕМЫ И МЕТОДЫ ЕГО СОВЕРШЕНИЯ

В работе рассмотрены наиболее популярные способы совершения мошенничества в сфере информационных технологий. Рассмотрены понятия объект, субъект, объективная сторона и субъективная сторона мошенничества.

***Ключевые слова**: мошенничество, обман, злоупотребление доверием, фишинг, интернет-банкинг, пластиковые карты.*

Мошенники — элита криминального мира, цель которых завладеть чужим имуществом обманным путем не прибегая к использованию насилия, угроз и оружия против жертвы. Обманутая жертва сама передает свое имущество или права на него мошенникам, при этом не подозревая о совершении противоправных деяний против нее. Данную категорию преступников можно условно назвать «гуманными» по отношению к потерпевшему, так как кроме своей хитрости, находчивости и изобретательности они не применяют каких-либо жестоких приемов к доверчивой жертве.

Уголовный кодекс Российской Федерации дает данному противоправному деянию следующее определение: мошенничество, то есть хищение чужого имущества или приобретения права на чужое имущество путем обмана или злоупотребления доверием [1].

Мошенничество можно по праву отнести к категории сложных по замыслу и исполнению преступлений, предметом которого является чужое имущество или право на него, а объектом — отношения определенной формы собственности. Хищение чужого имущества или приобретение права на чужое имущества путем обмана или злоупотреблением доверием будет являться объективной стороной мошенничества. К объективным признакам мошенничества относится: 1) изъятие и (или) обращение чужого имущества в пользу виновного или других лиц; 2) причинение этим действием реального материального ущерба собственнику или иному владельцу этого имущества; 3) противоправность совершения этих действий; 4) безвозмездность их совершения. Обязательным признаком объективной стороны мошенничества является наступление преступного результата, так как оно относится к преступлениям с «материальным» составом. Мошенничество отличается от других составов хищения чужого имущества специфическими способами его совершения — обманом и злоупотреблением доверия [2].

Первый способ совершения мошенничества: обман — это сознательное введение жертвы в заблуждение путем сообщения каких-либо ложных сведений в различных формах устной, письменной и т. д.

Обман в мошенничестве делится на активный и пассивный. Активный обман — это намеренное сообщение злоумышленником заведомо ложных сведений потерпевшему. Пассивный обман заключается в преднамеренном утаивании злоумышленником сведений об обстоятельствах, которые необходимо было сообщить потерпевшему [3].

Второй способ: злоупотребление доверием. При совершении мошенничества путем злоупотребления доверием мошенник для совершения хищения использует доверительные отношения с потерпевшим, в результате чего потерпевший сам добровольно передает мошеннику имущество либо право на него, полагая, что тот имеет на него законное основание. Доверительные отношения складываются на почве служебных, договорных и иных юридических отношений, а также родства, дружбы, знакомства. Как правило, злоупотребление доверием редко выступает способом мошенничества самостоятельно, чаще всего оно сопряжено с обманом потерпевшего.

Мошенничество признается оконченным с момента поступления в незаконное владение имущества или права на него злоумышленникам, и они получили реальную возможность распоряжаться им по своему усмотрению.

Все вышеописанное присуще классической форме мошенничества, когда злоумышленник вступает в прямой контакт с потерпевшим, но современные реалии таковы, что с развитием информационных технологий мошенничество плавно перетекло в сеть интернет, где прямого контакта не требуется. Законотворцам даже пришлось Федеральным законом от 29.11.2012 года №207-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» внести дополнения в уголовный кодекс РФ, а именно в статью 159 УК РФ. Теперь в уголовном кодексе появилась новая статья 159.3 «Мошенничество с использованием платежных карт» состав преступления данной статьи я хочу рассмотреть подробнее, потому что платежными картами сейчас пользуются огромное количество человек по всей планете, и теоретически каждый из них может стать жертвой мошенников.

С появлением пластиковых карт появились и специальные устройства, с помощью которых стало возможным получение наличных денег без траты времени на очереди в кассу банка — это банкоматы. Стоит отметить, что большинство платёжных карт имеют, определённый стандартом ISO 7810, ID-1 формат — 85,6 × 53,98 мм — и используют в качестве носителя данных магнитную полосу и чип. На лицевой стороне карты может быть любое изображение (граффити, картина, фотография) или просто фон. Кроме того, присутствуют логотип платёжной системы, номер карты, имя держателя и срок действия карты. На обратной стороне карты находится магнитная полоса, бумажная полоса с подписью владельца, трёхзначный код проверки подлинности карты (CVV2-код, CVC2-код) или его аналог. При помощи этих данных идентифицируется ее держатель и при совершении покупок или снятия денег в банкомате деньги списываются со счета держателя карты. И чтобы мошенникам получить доступ к банковскому счету потерпевшего и завладеть его денежными средствами, необходимо получить реквизиты его банковской карты.

С целью получения доступа к вышеупомянутой информации были придуманы специальные считывающие устройства «скиммеры», которые устанавливаются на банкоматы, а способ совершения кражи денег при их помощи получил название «скимминг». Эти устройства устанавливаются перед гнездом, куда вставляется банковская карта, и считывают информацию с магнитной полосы, а также защитного кода на оборотной стороне карты. Также злоумышленникам необходимо завладеть и пин-кодом который держатель карты вводит перед осуществлением банковских операций с целью идентификации своей личности как держателя карты. Для кражи пин-кода обычно используется маленькая видео камера, которая крепится к банкомату и снимает, как ничего не подозревающие люди, вводя пин-код, дают злоумышленникам ключ от своего счета в банке. После получение всех необходимых данных карты изготавливается ее дубликат, и злоумышленники снимают деньги жертвы в банкомате.

Использование данного способа хищения денег сильно усложнилось, когда банковские карты стали оснащаться защитным чипом; теперь, не имея на дубликате карты чипа, снять деньги со счета потерпевшего через банкомат не получится, но получится осуществить покупки в интернет-магазинах.

С развитием сети интернет и для удобства предоставления банковских услуг клиентам стал широко применяться интрнет-банкинг. Интернет-банкинг — это общее название технологий дистанционного банковского обслуживания, а также доступ к счетам и операциям (по ним), предоставляющийся в любое время и с любого компьютера, имеющего доступ в интернет. Для того чтобы получить доступ к дистанционному банковскому обслуживанию посредством интернет-банкинга, пользователю необходимо идентифицировать себя при помощи логина и пароля. Для завладения конфиденциальными данными пользователя мошенниками был придуман способ, получивший название «фишинг»,

который подразумевает создание сайта, внешне неотличимого от настоящего сайта банка. При попадании на фальшивый сайт ничего не подразумевающий пользователь вводит свой логин и пароль в предусмотренные для этого поля, после чего мошенники получают доступ к конфиденциальной информации пользователя и, соответственно, — к его счетам. Этот способ также широко распространен для кражи логинов и паролей от аккаунтов страниц в социальных сетях, аккаунтов электронной почты и т. д.

Современную жизнь уже невозможно представить без смартфонов со встроенными камерами, музыкальными плеерами и даже компасами. Они очень прочно закрепились в нашей жизни и не только упростили ее, но и добавили рад проблем. Сейчас на смартфонах в большинстве случаев используется две операционные системы: Android и iOS, есть также еще и третья Windows Phone, но она менее распространена. Операционная система Android является программным обеспечением с открытым исходным кодом. Ее исходный код доступен для просмотра, изучения и изменения, это позволяет пользователям данной операционной системы принимать участие в ее доработке. Также пользователи могут использовать код для создания новых программ, исправления в них ошибок — это возможно через заимствование исходного кода, если это позволяет совместимость лицензий, или через изучение использованных алгоритмов, структур данных, технологий, методик и интерфейсов (поскольку исходный код может существенно дополнять документацию, а при отсутствии таковой сам служит документацией).

Основным же конкурентом Android является операционная система — iOS. iOS является закрытым программным обеспечением. Закрытое программное обеспечение — это модель, при которой автор (или иной правообладатель) удерживает за собой ряд прав. В частности, повторное распространение или изменение программы запрещено или требует особого разрешения, или очень жестко ограничено. Для большинства программ исходный код недоступен, что делает невозможной или, по крайней мере, нетривиальной задачу модификации программ под определенные нужды [4].

Современные банки разрабатывают приложения доступные на обеих операционных системах, которые позволяют их клиентам получать доступ к банковским услугам со своих смартфонов. Мошенники и здесь придумали, как заполучить конфиденциальную информацию для доступа к интернет-банкингу. Так как iOS — является закрытым программным обеспечением, пользователи данной системы не являются жертвами приложений, разработанными мошенниками для кражи персональных данных их пользователей. Это невозможно, потому что каждое приложение, которое становится доступным в магазине приложений App Store, проходит тщательную проверку корпорацией Apple, в том числе на предмет содержание вредоносных программ. В операционной системе Android есть аналог App Store, который называется Google PLAY, но Android является открытым программным обеспечением и любой желающий может разработать приложение для смартфона и распространять его через магазин приложений без каких-либо проверок, чем и пользуются мошенники.

При установке такого приложения на смартфон жертвы устанавливается вредоносное программное обеспечение, которое отслеживает действия и отправляет всю необходимую информацию мошенникам.

Но эти способы довольно сложны, так как требуют приличных навыков программирования для создания приложения или фальшивого сайта банка при вводе в которые логина и пароля, эта информация бы считывалась, и отправлялась мошенникам. Гораздо проще получить необходимую конфиденциальную информацию при помощи хитрости и доверчивости жертвы. Злоумышленники отправляют смс-сообщение от имени банка о блокировки карты с указанием номера телефона, по которому необходимо будет позвонить для ее разблокировки. Жертва звонит по указанному номеру телефона, на другом конце берет трубку мошенник, и просит назвать необходимую ему информацию для разблокировки карты, ничего не подразумевающая жертва с легкостью сообщает

конфиденциальную информацию, после чего мошенник получает полный доступ к ее счетам. Также могут совершаться звонки самими мошенниками от имени банка, как непосредственно человеком, представляющимся сотрудником банка, так и автоинформатором, сообщающим о блокировке карты и необходимостью идентификации личности ее владельца сообщить необходимые данные.

Мошенничество — как и технический прогресс — не стоит на месте, а идет в ногу со временем. Изобретаются все новые способы хищения чужого имущества. Мошенники по праву считаются элитой криминального мира: они изобретательны и находчивы. В большинстве случаем это умные образованные люди, которые решили применить свои умения и навыки в криминальной сфере. Соответственно, методы борьбы с ними должны быть такими же, или даже гораздо более профессиональными.

Литература

1. Уголовный кодекс РФ;

2. Аванесян С. Р. Мошенничество как форма хищения // Право: теория и практика. — М.: Тезарус, 2007, № 4 (93). — С. 65–67;

3. Постановление Пленума Верховного Суда РФ от 27 декабря 2007 г. № 51 «О судебной практике по делам о мошенничестве, присвоении и растрате»;

4. Черненко С. В., Авраменко Н. А. Автомобильно-Дорожный Институт ГВУЗ «ДонНТУ»; «Закрытое, открытое и свободное программное обеспечение — основные различия и тенденции развития».