УДК 343.98

О.П. Бердникова
кандидат юридических наук
доцент кафедры криминалистики
Уральский юридический институт МВД России
г. Екатеринбург, Российская Федерация
E-mail: berdnikovs@inbox.ru

О.П. Виноградова
кандидат юридических наук
старший преподаватель кафедры криминалистики
Уральский юридического института МВД России
г. Екатеринбург, Российская Федерация
E-mail: olga10vin@mail.ru

СПОСОБ СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЯ КАК ЭЛЕМЕНТ КРИМИНАЛИСТИЧЕСКОЙ ХАРАКТЕРИСТИКИ ПРЕСТУПЛЕНИЙ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Аннотация: в статье, на конкретных примерах, рассмотрены современные тенденции в сфере совершения преступлений с использованием информационных технологий. Сформулированы отдельные предложения по повышению эффективности их расследования и раскрытия.

Ключевые слова: преступление, информационные технологии, способ совершения преступления, мобильный банкинг, электронное платежное средство.

Одной из ключевых особенностей современного периода развития общества является повсеместное практическое использование компьютерной техники во всех значимых сферах человеческой жизнедеятельности, создание целой индустрии производства и обработки информации. Все более востребованными специальными знаниями при выявлении и расследовании дел данной категории становятся знания в области компьютерной информации. В правоприменительной практике умение получить необходимую значимую информацию, выделив ее из информационного шума, имеет большое значение, поскольку пользователи цифровых сетей хранят целые массивы информации о личной жизни и трудовой деятельности, совершают различного рода операции с денежными средствами. Одновременно с этими процессами преступники находят способы совершения и сокрытия преступлений в сфере информационных технологий, получения незаконного доступа к различного рода компьютерной информации, разрабатывается вредоносное программное обеспечение, которое в последствии становится орудием совершения хищений денежных средств, хранящихся на счетах в банках, сервисах онлайн-платежей. Также компьютерная информация всё чаще становится не только объектом преступного посягательства, но и используется в качестве орудия

совершения преступлений, например, связанных с несанкционированным снятием денежных средств с расчетных счетов граждан посредством средств мобильной связи и сети Интернет.

Для хищения денежных средств при помощи мобильных средств связи путем перевода денежных средств с банковских карт потерпевших на банковские счета третьих лиц характерны все основные признаки мошенничества, предусмотренного статьей 159 УК РФ. Вместе с тем их отличительной чертой являются способы завладения чужим имуществом, поскольку преступниками используются мобильные системы связи, а также возможности интернет-банкинга (т.е. способом дистанционного банковского обслуживания клиентов, осуществляемого кредитными организациями в сети Интернет (в том числе через WEB-сайт(ы) в сети Интернет и включающего информационное и операционное взаимодействие с ними).

Анализ правоприменительной практики свидетельствует о росте количества мошенничеств, совершаемых таким способом. Значительная часть указанных преступлений совершается лицами, содержащимися в местах лишения свободы.

Одним из наиболее распространенных видов электронных платежных средств являются платежные (кредитные, расчетные и предоплаченные) карты и мобильный банкинг, т.е. система управления банковским счетом с помощью планшетного компьютера, смартфона или мобильного телефона, обладающих собственным программным обеспечением, интегрированным в локальные или глобальные информационные сети, в том числе информационно-телекоммуникационную сеть «Интернет». Указанная система позволяет

переводить денежные средства абонента с его банковского счета (счета банковской карты) на счет другого лица, а также совершать некоторые платежи за услуги и товары прямо со счета с помощью мобильного телефона. Технология данного инструментария предполагает, что абонент совершает оплату в безналичном порядке. Расчеты осуществляются, как правило, с помощью сервиса коротких текстовых сообщений (SMS) оператора мобильной связи. Механизм совершения платежа носит трехсторонний характер и включает плательщика, получателя, кредитную организацию. Мобильные платежи подразделяются на обычные и микроплатежи (по сумме платежа) либо по способу реализации, когда телефон используется клиентом банка как средство для управления своим счетом или своим счетом у сотового оператора. Операторы сотовой связи кроме классического мобильного банкинга предоставляют возможность передавать средства на счет от одного абонента к другому, оплачивать некоторые виды услуг деньгами, находящимися на счете телефонного номера (мобильный платеж). Услуги, которые можно оплатить непосредственно с телефона включают коммунальные платежи, услуги связи, Интернет и др. Большая их часть, оказывается через SMS-сервис или с помощью звонка в центры поддержки оператора сотовой связи.

Таким образом, электронные платежные инструменты представляют собой безналичные денежные средства, только со значительно облегченным порядком доступа к ним.

Лица, совершающие хищения денежных средств с помощью электронных платежных инструментов, используют полученную информацию и современные технологии, вынуждая потерпевших

раскрывать информацию о своей личности, платежных картах, совершать переводы денежных средств на их счета.

К распространенным способам совершения рассматриваемого преступления относят:

направление заявителю посредством средств мобильной связи SMS (или путем телефонного звонка) информации о том, что с его родственником (или иным близким лицом) произошло какое-либо негативное событие, и за разрешение проблемы требуется перечислить денежные средства на определенный банковский счет или мобильный телефон;

направление на мобильные телефоны клиентов кредитных организаций SMS о необходимости позвонить по номерам телефонов, которые в действительности не принадлежат этим организациям;

звонки клиентам с сообщением автоинформаторов о предоставлении продуктов и услуг банка с предложением нажать определенные клавиши на телефоне для подтверждения согласия в их приобретении и т.п.

Введенные в заблуждение клиенты кредитных или расчетных организаций вступают в контакт с мошенниками, целью которых является получение конфиденциальной личной информации (например, реквизиты банковской карты и личного опознавательного номера – PIN)[1]. Например, А. отправил на абонентский номер, находящийся в пользовании у С. SMS, содержащее заведомо ложные сведения о том, что ее банковская карта заблокирована. Получив сообщение, С. перезвонила на абонентский номер, указанный в SMS. На звонок

[1] Письмо Банка России от 07.12.2007 № 197-Т «О рисках при дистанционном банковском обслуживании» // Вестник Банка России, № 68, 12.12.2007.

ответил А., представившись сотрудником Сбербанка России, подтвердил информацию о блокировке банковской карты и пояснил**,** что необходимо произвести перезагрузку банковской карты. А. под предлогом разблокировки банковской карты убедил С. подойти к терминалу и проверить остаток денежных средств на балансе ее банковской карты. С. выполнила его указание, после чего А. продиктовал ей набор цифр, обозначающий номер сотового телефона, на который необходимо перечислить денежные средства, и сумму денежных средств, снимаемых с баланса банковской карты. С. ввела указанные цифры и перечислила на лицевой счет гр-на А. денежные средства в сумме 29 754 руб.[1].

Размещение на сайте в сети Интернет предложений об услугах, товарах, работе, трудоустройстве и других, выполнение которых предполагает частичную или полную предоплату путем перечисления денежных средств потерпевшим на определенный банковский счет. Например, К. в поисках работы зашла на сайт с объявлением о работе вахтовым методом в г. Санкт-Петербурге. Ознакомившись с условиями приема, она предложила своему сожителю Б. отправить по электронной почте свою анкету. Через некоторое время ему на электронный адрес поступило письмо с просьбой позвонить по прилагаемому номеру телефона. По указанному номеру неустановленная женщина сообщила о необходимости внесения через платежный терминал предоплаты за проживание в общежитии, страховку, вызов бригадира, спецодежду. После осуществления денежного перевода неустановленная женщина сообщила, что вызова на работу можно ждать, пока не надоест и после

[1] Официальный сайт Надымского городского суда ЯНАО. Дело № 1-4/2014 (1-261/2013;)

этого дозвониться на указанный номер К. и Б. не смогли[1].

Также достаточно распространенным способом преступления является перевод денежных средств с банковских карт потерпевших на банковские счета третьих лиц путем направления SMS о поступлении на его счет денежных средств с помощью услуги «мобильный перевод». После чего лицо, совершающее преступление, звонит потерпевшему и просит вернуть указанную в SMS сумму обратно с помощью «мобильного перевода». Похожими являются и другие способы совершения такого рода мошенничеств: направление SMS с информацией о том, что потерпевший выиграл приз и предложением перевести деньги за пересылку приза; звонок потерпевшему от лица, представляющегося «знакомым», с просьбой пополнить счет мобильного телефона.

Для раскрытия неочевидных краж и мошенничеств, совершенных с использованием банковских карт, посредством средств мобильной связи и сети Интернет необходимо обратить внимание на ряд мероприятий.

1. Истребовать либо направить повторные запросы операторам сотовой связи, в финансово-кредитные учреждения по установлению принадлежности расчетных счетов.

2. По уголовным делам, возбужденным по фактам хищения денежных средств с помощью «вирусных программ», направлять представления в ПАО «Сбербанк».

[1] Постановление о приостановлении дознания в связи с неустановлением лица подлежащего привлечению в качестве обвиняемого по уголовному делу № 2014230407 // Архив Отдела МВД России по Фурмановскому району Ивановской области.

3. Проводить анализ неочевидных уголовных дел о преступлениях данной категории с целью выявления совпадений по абонентским номерам телефонов, номерам банковских карт, расчетным счетам, Интернет-адресам. При выявлении совпадений направить поручения (задания) в органы внутренних дел, где выявлены совпадения для организации совместного расследования данных уголовных дел.

4. Более активно проводить работу по вопросу раскрытия преступлений по фактам мошенничеств, совершенных в условиях неочевидности, и по преступлениям «прошлых лет», с проведением анализа, выработкой конкретных мероприятий, направленных на раскрытие преступлением, установлением исполнителей и сроков.

5. При отработке жилого сектора участковыми уполномоченными полиции продолжить проведение профилактических бесед по вопросам сохранности денежных средств, уделив особое внимание пожилым гражданам.

6. Продолжить работу по освещению в средствах массовой информации преступлений о кражах и мошенничествах, совершенных с использованием банковских карт, посредством средств мобильной связи и сети Интернет.

В свою очередь, перечень неотложных следственных действий и оперативных мероприятий, очередность их проведения будут определяться конкретной следственной ситуацией, в которой начинается расследование, а сама следственная ситуация характеризуется прежде всего объемом и достоверностью исходной криминалистически значимой информации, имеющейся в распоряжении следователя и оперативного сотрудника. Следует

подчеркнуть, что в рамках уголовно-процессуальной деятельности наиболее часто применяемым способом использования специальных знаний при расследовании уголовных дел в сфере компьютерной информации является такое процессуальное действие, как судебная экспертиза. Например, судебная компьютерная экспертиза представляет собой род криминалистической экспертизы, проводимой в целях получения доказательств по уголовным и гражданским делам, устанавливаемых на основе изучения закономерностей функционирования информации в средствах вычислительной техники. Специальные познания в области компьютерной экспертизы составляют автоматизация и вычислительная техника (в том числе программирование), информационные системы и процессы, электроника, электротехника, радиотехника и связь.

Полноценная организация компьютерной экспертизы подразумевает наличие в подразделении специалистов по различным операционным системам, прикладному программному обеспечению, бухгалтерским программам, базам данных, программированию, криптоанализу, мультимедиа, сетевым и Интернет-технологиям, аппаратным компонентам компьютера и машинным носителям информации, связи.

Российским законодательством определено, что лицо, обладающее специальными знаниями, может оказывать содействия судам, судьям, органам дознания, лицам, производящим дознание, следователям в установлении обстоятельств, подлежащих доказыванию по конкретному делу, либо в качестве эксперта, либо в качестве

специалиста[1]. Однако, как показывает практика, нередко возможности специалистов и экспертов используются нерационально, их привлекают к участию в деле неумело и с нарушениями требований уголовно-процессуального закона. Все же использование помощи специалистов (экспертов) является неотъемлемой частью расследования мошенничеств в сфере компьютерной информации и обеспечивает всесторонний анализ уголовного дела требующего применения специальных знаний. Таким образом, следует отметить, что раскрывать и расследовать преступления в сфере компьютерной информации довольно сложно, так как нередко преступники прибегают к различным уловкам, маскируют свои преступные деяния под те обстоятельства, которые имеют место в действительности (например, сбой в работе ЭВМ и программного обеспечения, средств электросвязи, энергообеспечивающего оборудования; замыкания в электропроводке и т.п.).

O.P. Berdnikova
candidate of legal sciences
assistant professor of the department of criminalistics
Ural law Institute of MIA of Russia

[1] Приказ МВД России от 29.06.2005 № 511 «Вопросы организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации» URL: http: // www.consultant.ru; Приказ МВД России от 09.01.2013 № 2 «Вопросы определения уровня профессиональной подготовки экспертов в системе МВД России» URL: http: // www.consultant.ru; Федеральный закон от 31 мая 2001 г. № 73-ФЗ «О государственной судебно-экспертной деятельности в Российской Федерации». URL: http: // www.consultant.ru.

Ekaterinburg, Russian Federation
E-mail: berdnikovs@inbox.ru

O.P. Vinogradova
candidate of law sciences
senior lecturer of the department of criminalistics
Ural law Institute of MIA of Russia
Ekaterinburg, Russian Federation
E-mail: olga10vin@mail.ru

THE WAY TO THE COMMISSION OF AN OFFENCE AS AN ELEMENT OF CRIMINAL CHARACTERISTIC OF CRIMES IN THE SPHERE OF INFORMATION TECHNOLOGIES

Abstract

In this article, with specific examples, current tendencies are reviewed in the field of committing crimes with the use of information technologies. Separate offers are formulated to increase the effectiveness of their investigation and disclosure.

Keywords

Crime, information technologies, the way to the commission of an offence, mobile banking, electronic means of payment.