С.М. Белозерцев

ПРОФИЛАКТИКА МОШЕННИЧЕСТВ С ИСПОЛЬЗОВАНИЕМ МОБИЛЬНЫХ УСТРОЙСТВ И БАНКОВСКИХ КАРТ В ИРКУТСКОЙ ОБЛАСТИ: ПРОБЛЕМЫ И ПУТИ ИХ РЕШЕНИЯ

На основе статистических данных и примеров из практики обосновывается точка зрения о том, что несмотря на изменения уголовного законодательства, эффективность работы правоохранительных органов по противодействию мошенничеству снизилась, основной причиной стало появление нового способа совершения преступлений. Предложены ключевые направления по противодействию данному виду преступности.

Ключевые слова: профилактика преступлений, мошенничества, «Интернет-мошенничество», мошенничество с использованием банковских карт, профилактика преступности.

S. M. Belozertsev

PREVENTING FRAUD WITH USE OF MOBILE DEVICES AND CASH CARDS IN THE IRKUTSK REGION: PROBLEMS AND WAYS OF THEIR DECISION

On the basis of statistical data and examples from practice the point of view locates that despite changes of the criminal legislation, overall performance of law enforcement agencies on counteraction to frauds decreased, emergence of a new way of commission of these crimes became the main reason. The key directions on counteraction to this type of crime are offered.

Keywords: prevention of crimes, frauds, Internet frauds, frauds with use of cash cards, prevention of crime.

Компьютеризация и технический прогресс, происходящий в обществе в XXI веке, был предсказан еще в 60-х годах прошлого века. Учеными из компьютерной индустрии был замечен и описан базовый принцип современного электронного прогресса, который получил название закон Гордона Мура, согласно которому удвоение числа транзисторов в электронных устройствах будет происходить примерно каждые два года, соответственно рост производительности компьютеров будет расти по экспоненте и также будет происходить значительное удешевление этих технологий, и рано или поздно компьютеризацией так или иначе будут охвачены все сферы общества [1].

Главный и базовый вывод, который, как нам кажется, не был в полной мере учтен в практической деятельности правоохранительных органов в целом и российских правоохранителей в частности, заключается в том, что компьютерные технологии, во-первых, вырастут стремительно и значительно

быстрее, чем ожидается, а, во-вторых, станут чем-то обыденным, перестав быть сферой использования исключительно компьютерных специалистов, как только будет превышена некоторая «критическая масса» таких устройств и технологий. Неизбежно появятся новые способы совершения вполне обычных преступлений вроде краж или мошенничества, которые не будут исключительно сложными, но будут приносить колоссальный ущерб населению.

Данный процесс происходит на наших глазах, причем зачастую в сферах жизни, весьма далеких от передовых информационных технологий. Например, с 2012 г. в Иркутской области стало увеличиваться количество зарегистрированных мошенничеств, при этом раскрываемость снизилась с 72,6 в 2009 г. до 41,3 % в 2014 [2].

Таблица 1

Количество мошенничеств в Иркутской области с 2009 по 2014 г.

Год / Показатель	2009	2010	2011	2012	2013	2014
Зарегистрировано	4113	2442	1987	2381	2491	2763
Прирост к предыдущему году, в %	-	-40,6	-18,6	+19,8	+4,6	+10,9
Раскрываемость, в %	72,6	57,8	52,2	45,5	47,2	41,3

Анализ правоприменительной практики показал, что рост числа зарегистрированных мошенничеств происходил, в основном, за счет увеличения числа посягательств с использованием мобильной связи и сети «Интернет», а также хищений с банковских карт. Количество остальных видов преступлений оставалось относительно стабильным.

Удельный вес преступлений в 2013 г. составил 25 % (629) от количества всех мошенничеств, в 2014 г. уже 31 (855), а по итогам 8 месяцев 2015 г. составляет практически 60 % (1109).

Основная масса преступлений совершается схожим способом:

- хищение денег, посредством телефонного (либо СМС) общения, в том числе с последующим использованием возможностей «онлайн-банка»;

- приобретение, продажа либо оплата услуг через сервисы «Интернет».

Под различными предлогами злоумышленники получают банковские реквизиты и (или) учетные данные онлайн-клиента распространенных банков (как правило, ПАО «Сбербанк») после чего похищают денежные средства.

К сожалению, изменения УК РФ, произошедшие в конце ноября 2012 г., когда были введены новые составы мошенничеств (ст.ст. 159.1–159.6 УК РФ) фактически никак не повлияли на ситуацию. Квалификация описанных преступлений в подавляющем большинстве случаев происходит по основному составу (ст. 159 УК РФ).

Примечательно то, что несмотря на существенные изменения в законодательстве, основная проблема возникла не в рамках правового поля, а исключительно в появлении нового способа совершения обыкновенных по своей сути мошенничеств.

Существенно осложняет данную ситуацию тот факт, что благодаря развитию современных коммуникативных технологий, появилась возможность совершать данные преступления удаленно.

Анализ сведений о регистрации абонентских номеров, используемых для совершения преступления, показал, что лишь 15 % абонентов были зарегистрированы на территории Иркутской области, 85 % телефонных звонков поступили из других регионов, в том числе Самарской, Курганской, Новосибирской, Кемеровской областей, г. Санкт-Петербурга и Ленинградской области, г. Москвы и иных регионов.

Кроме того, изучение материалов уголовных дел показало, что значительная часть звонков поступает из учреждений ГУ ФСИН России.

Исключительно со статистической точки зрения реальный рост преступлений данного вида можно нивелировать за счет отсылки материалов уголовного дела в тот регион, где фактически преступление было окончено.

Как известно, согласно правовым нормам хищение считается оконченным в том месте, где преступник получил реальную возможность распоряжаться похищенными денежными средствами.

Однако простая передача таких уголовных дел по подследственности не решит проблему реального роста преступлений. Кроме того, на практике возникает ряд сложностей.

Расследование уголовных дел данной категории специфично, осложнено продолжительными поисковыми мероприятиями владельцев сим-карт, с которых произведен звонок, а также установлением «Интернет-адресов» подозреваемых. В ходе расследования направляются запросы в телефонные сотовые компании, оперативно-технические подразделения, а также отдельные поручения в иные регионы для установления владельца сим-карты. Однако в большинстве случаев для совершения преступления используются «сайты-однодневки», при регистрации доменного имени которых вносятся вымышленные данные. Администрирование данных сайтов осуществляется посредством сети «Wi-Fi» общественных организаций, что не позволяет установить физический адрес лица, занимающегося противоправной деятельностью. Владельцы сим-карт, с использованием которых производится звонок, являются умершими, либо не существующими.

Таким образом, более 80 % таких уголовных дел после проведения полного комплекса следственных действий подлежат приостановлению по п. 1 ч. 1 ст.208 УПК РФ, а преступления входят в разряд нераскрытых.

Другим направлением решения данной проблемы могло бы стать активное взаимодействие правоохранительных органов разных субъектов РФ. Однако и здесь существуют определенные сложности.

Главная из них заключается в том, что регионы, реально пораженные данным видом криминальной активности (откуда звонили и где были сняты похищенные деньги), не испытывают всего объема ответственности за деяния, совершенные на территории их обслуживания, а следовательно не заинтересованы в проведении активных оперативно-розыскных мероприятий.

Более эффективным направлением противодействия «новым видам» мошенничества видится проведение активных профилактических мероприятий с населением и банками.

Причин тому несколько.

Во-первых, подключение большинства клиентов сбербанка-онлайн происходило, как говорится «добровольно-принудительно». Следствием стало то, что к онлайн-сервисам ПАО «Сбербанк» были подключены фактически все клиенты данного банка.

Во-вторых, подавляющему большинству клиентов ПАО «Сбербанк» не были разъяснены элементарные меры обеспечения безопасности при осуществлении расчетов с банковских карт и счетов посредством сети «Интернет».

В-третьих, значительная часть потерпевших (около 80 %) не были проинформированы относительно фактов совершения данного рода преступлений, а, следовательно, вели себя неосмотрительно (добровольно сообщали злоумышленникам полный номер банковской карты, логин и пароль онлайн-клиента банка и т.п.).

Описанная проблема относительно новая и уже сегодня требует принятия активных мер, в первую очередь профилактического характера, направленных на повышение уровня кибербезопасности граждан.

Государство в лице законодательной и исполнительной власти, безусловно, не может оставаться в стороне, между тем, как показывает практика, не все возникающие вызовы и угрозы возможно решить «любимым» способом последнего времени – очередным изменением уголовного закона.

Необходимы также меры управленческого характера, в первую очередь организационные (взаимодействие между ОВД различных субъектов) и интеллектуальные (повышение общего уровня профессионализма и квалификации сотрудников правоохранительных органов), а также профилактическая работа с гражданами и организациями.

БИБЛИОГРАФИЧЕСКИЕ ССЫЛКИ

1. Moore, Gordon E. No Exponential is Forever: But «Forever» Can Be Delayed! (англ.). URL: http://cseweb.ucsd.edu/ classes /wi10/cse241a/slides/ mooreISSCC03.pdf (дата обращения 18.11.2015 г.).

2. Статистические сведения ИЦ ГУ МВД России по Иркутской области за 2009–2014 гг., а также 8 месяцев 2015 г.