Научная статья
УДК 343.98
DOI 10.18101/2658-4409-2021-1-21-28

КРИМИНАЛИСТИЧЕСКАЯ ПРОФИЛАКТИКА ИНТЕРНЕТ-МОШЕННИЧЕСТВ: ПРОБЛЕМЫ РАСКРЫТИЯ И РАССЛЕДОВАНИЯ

© Батров Баради Баярович
аспирант,
Бурятский государственный университет имени Доржи Банзарова
Россия, 670000, г. Улан-Удэ, ул. Смолина 24а
bbatrov@gmail.com

Аннотация. Анализируются статистические данные, свидетельствующие о значительном росте интернет-мошенничеств в общем массиве преступлений с использованием информационно-телекоммуникационных технологий. В статье рассматриваются затруднения, возникающие в ходе расследования и раскрытия данного вида преступлений, а также обстоятельства, осложняющие установление виновных лиц. С учетом этого предлагаются способы решения имеющихся проблем с использованием методов и средств криминалистической профилактики. Особое внимание уделяется вопросам правильной квалификации преступлений, связанных с интернет-мошенничеством, разработке государственных программ по борьбе с преступлениями с использованием интернет-технологий, а также вопросам международного сотрудничества в области борьбы с корыстными посягательствами, применяя современные цифровые технологии.
Ключевые слова: уголовное право; корыстные преступления; интернет-мошенничество; расследование; криминалистическая профилактика; информационно-телекоммуникационные технологии; вредоносные программы; деанонимизация.

Для цитирования
Батров Б. Б. Криминалистическая профилактика интернет-мошенничеств: проблемы раскрытия и расследования // Вестник Бурятского государственного университета. Юриспруденция. 2021. Вып. 1. С. 21–28.

Большую тревогу и беспокойство у сотрудников правоохранительных органов вызывает факт непрекращающегося роста регистрации совершения интернет-мошенничеств. В век высоких технологий благодаря нескольким манипуляциям на телефоне, планшете, ноутбуке или персональном компьютере можно попасть в виртуальный мир, в котором зачастую не действуют закон и общепринятые нормы морали. Существующие способы «анонимизации» пользователей, охват огромной аудитории, относительно небольшая стоимость используемых орудий совершения преступлений, высокая скорость распространения информации позволяют подготавливать, совершать, изобретать все новые способы мошеннических действий в сети Интернет.

О широкой распространенности обозначенных преступных посягательств свидетельствуют и статистические данные. Рассмотрим их в динамике на примере одного из субъектов Российской Федерации — Республики Бурятия.

За 6 месяцев 2020 г. зарегистрировано 1503 преступления (6 мес. 2019 г. — 689, +118,1%), совершенных с использованием информационно-телекоммуникационных технологий (ИТТ), раскрыто 377 (6 мес. 2019 г. — 178, +111,8%), приостановлено 897 уголовных дел (6 мес. 2019 г. — 453), раскрываемость составила 29,6% (6 мес. 2019 г. — 28,2%)[1].

Необходимо отметить, что значительная часть совершаемых на территории республики преступлений с использованием ИТТ — это противоправные деяния, связанные с хищением чужой собственности путем мошенничества и кражи.

За указанный период времени зарегистрировано 431 мошенничество, совершенное с применением ИТТ (6 мес. 2019 г. — 280, +53,9%), раскрыто 15 (6 мес. 2019 г. — 12), приостановлено 371 уголовное дело (6 мес. 2019 г. — 257), раскрываемость составила 3,9% (6 мес. 2019 г. — 4,5%, – 0,6%).

По пункту «г» ч. 3 ст. 158 УК РФ возбуждено 710 уголовных дел (6 мес. 2019 г. — 166), направлено в суд 176 (6 мес. 2019 г. — 39), приостановлено 423 уголовных дела (6 мес. 2019 г. — 66), раскрываемость составила 29,4% (6 мес. 2019 г. — 37,1%, –7,7%)[2].

По способу совершения преступлений с использованием ИТТ наиболее типичными являются:

- кража денежных средств посредством дополнительных опций, предлагаемых кредитными организациями (мобильный банк, переводы посредством СМС и другое);
- преступления мошеннического характера, направленные на хищение денежных средств, а также материальных ценностей как в сети Интернет, так и с использованием стационарной и мобильной сотовой связи;
- размещение в информационном поле вредоносных программ, устройств компьютерного взлома, методических рекомендаций по применению хакерского инструментария.

Типичны способы хищения, совершаемые с использованием:

- расчетных (пластиковых) карт — 749 (6 мес. 2019 г. — 69), раскрыто 226 (6 мес. 2019 г. — 26);
- компьютерной техники — 85 (6 мес. 2019 г. — 45), раскрыто 20 (6 мес. 2019 г. — 15);
- сети Интернет — 675 (6 мес. 2019 г. — 239), раскрыто 96 (6 мес. 2019 г. — 39);
- средств мобильной связи — 651 (6 мес. 2019 г. — 212), раскрыто 114 (6 мес. 2019 г. — 39)[3].

Приведенные статистические данные наглядно показывают значительный рост совершения преступлений в сфере ИТТ, в частности рост практически в два раза регистрации мошенничеств. При этом раскрытие интернет-мошенничеств, как и иных хищений в сфере ИТТ, остается чрезвычайно низким.

Так, одной из проблем при расследовании уголовных дел о преступлениях рассматриваемой категории остается порядок направления и получения запросов из сотовых компаний и финансово-кредитных учреждений, время получения

[1] Статистические данные ИЦ МВД по РБ.

[2] Там же.

[3] Там же.

ответов на них во многих случаях превышает 2 месяца. Эти сведения получены в процессе изучения следственной практики. Длительность ответов на направляемые запросы связана прежде всего с тем, что у операторов сотовой сети, также как и в финансово-кредитных учреждениях, ввиду оптимизации штатов представители, уполномоченные на взаимодействие с правоохранительными органами, находятся не в регионах, а в большинстве случаев в крупных городах федеральных округов. Случаи заключенных соглашений об электронном документообороте между операторами сотовой связи, кредитно-финансовыми учреждениями и Министерством внутренних дел единичны. В практической деятельности наличие договоров требуется со всеми организациями, оказывающими услуги связи и в финансово-кредитной сфере.

Указанный фактор значительно влияет на затягивание процедуры получения ответов на запросы. Больших временных затрат требует получение информации о соединениях между абонентами и абонентскими устройствами, что включает в себя время от подготовки и направления соответствующих материалов в суд до исполнения решения суда оператором сотовой связи.

Исходя из анализа имеющейся практики, безусловно, на эффективность расследования уголовных дел влияет отсутствие у органов дознания возможностей в ходе проведения оперативно-разыскных мероприятий без соответствующего решения суда запрашивать в кредитных организациях сведения о вкладах и счетах физических лиц, операциях и счетах юридических лиц и граждан, осуществляющих предпринимательскую деятельность без образования юридического лица.

Также не всегда учитывался в правоприменительной практике конкретный способ хищения денежных средств с банковских счетов, что вызывало различия при квалификации со стороны органов следствия, прокуратуры и суда. Например, до недавнего времени оставался нерешенным вопрос о сумме причиненного ущерба, что порождало разногласия в квалификации преступлений органами следствия полиции и органами прокуратуры в связи с применением ч. 2 ст. 14 УК РФ, в части малозначительности деяния при хищении на сумму менее 2,5 тыс. рублей. Федеральным законом от 23.04.2018 г. № 111-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации»[1] усилена уголовная ответственность за хищение денежных средств с банковского счета или электронных денежных средств, в том числе с использованием электронных средств платежа.

Изменения, внесенные в Уголовный кодекс Российской Федерации данным Федеральным законом, направлены на повышение уголовно-правовой защиты граждан и организаций путем усиления уголовной ответственности за хищение чужого имущества, совершенного с банковского счета, а равно электронных денежных средств, в том числе потому, что общественную опасность указанных деяний усиливает специфика способа совершения преступления — использование удаленного доступа к банковскому счету при помощи технических средств, позволяющего лицу оставаться анонимным и совершать преступление из любой точки мира. При этом такие действия виновного могут найти разную уголовно-правовую квалификацию.

[1] О внесении изменений в Уголовный кодекс Российской Федерации : федер. закон от 23 апреля 2018 г. № 111-ФЗ // Российская газета. 2018. № 88(7551). 25 апр.

Так, в ч. 3 ст. 158 УК РФ был введен п. «г» — кража, совершенная с банковского счета, а равно в отношении электронных денежных средств (при отсутствии признаков преступления, предусмотренного ст. 159.3 УК РФ).

Разногласия позиций в квалификации между следствием и прокуратурой в связи с введением в действие п. «г» ч. 3 ст. 158 и п. «в» ч. 3 ст. 159.6 УК РФ возникали, как правило, в случаях, когда преступник, совершивший преступление, установлен. В таком случае уголовное дело не возбуждалось, составлялся административный протокол по ст. 7.27 КоАП РФ «Мелкое хищение» и событие признавалось мелким хищением, а если преступник установлен — возбуждалось уголовное дело.

Остро стоит вопрос о неисполнении большинством операторов связи отдельных норм, предусмотренных Федеральным законом от 7 июля 2003 г. № 126-ФЗ «О связи», в части хранения в течение установленного времени соответствующей информации. С 1 июля 2018 г. вступили в силу Правила хранения операторами связи текстовых сообщений пользователей услуг связи, голосовой информации, изображений, звуков, видео и иных сообщений пользователей услуг связи, утвержденные постановлением Правительства РФ от 12 апреля 2018 г. № 445[1]. В настоящее время практически все поставщики данного рода услуг, ссылаясь на отсутствие технических возможностей, не исполняют норму закона, в соответствии с которой они обеспечивают хранение в технических средствах накопления информации, голосовой информации и текстовых сообщений пользователей услугами связи в полном объеме в течение 6 месяцев с даты окончания их приема, передачи, доставки и (или) обработки[2].

Значительные трудности своевременного установления реального владельца сим-карты связаны с оформлением сотовыми компаниями на одно юридическое лицо большого количества сим-карт, которые в дальнейшем попадают мошенникам и используются для массовой рассылки СМС-сообщений с последующим незаконным получением денег от физического лица.

К обстоятельствам, осложняющим расследование, относятся:

- использование преступниками сим-карт, оформленных на вымышленных лиц, несуществующих юридических лиц либо лиц без определенного места жительства;

- совершение преступлений данной категории жителями других субъектов России, в том числе отбывающими наказание в исправительных учреждениях;

- наличие средств анонимизации действий мошенников в сети «Интернет» (программные технологии «VPN», «TOR», «I2P», позволяющие менять IP-адрес пользователя в сети Интернет, создавать динамические или нераспознаваемые IP-адреса, а также применение ими технологий «подменных» абонентских номеров посредством SIP-телефонии, не позволяющих идентифицировать причастных к преступлениям лиц, а также использование зарубежных платежных систем и криптовалюты).

[1] Об утверждении Правил хранения операторами связи голосовой информации, изображений, звуков, видео- и иных сообщений пользователей услугами связи: постановление Правительства РФ от 12 апреля 2018 г. № 445.

[2] Правила хранения операторами связи текстовых сообщений пользователей услугами связи, голосовой информации, изображений, звуков, видео- и иных сообщений пользователей услугами связи с изменениями и дополнениями от 20.11.2018 г.

- отсутствие на «вооружении» подразделений МВД специальных программ и технических средств, позволяющих деанонимизировать пользователей мессенджеров, интернет-ресурсов, виртуальных бирж и платежных систем;
- отсутствие технических средств для проведения поисковых мероприятий по всем частотам диапазона 4G;
- сложность в получении данных от мессенджеров «Viber», «WhatsApp», «Telegram» ввиду нахождения их офисов за рубежом;
- отсутствие государственного контроля за криптовалютным оборотом, виртуальными биржами и обменниками;
- отсутствие системного подхода к формированию региональными органами внутренних дел (ОВД) подсистемы «Дистанционное мошенничество», а также необходимости интеграции в данную подсистему массивов данных, ранее формируемых отдельными региональными ОВД. В соответствии с указанием МВД России от 09.10.2019 г. № 1/11348 с 28 октября 2019 г. введено в опытную эксплуатацию специальное программное обеспечение подсистемы «Дистанционное мошенничество» программно-технического комплекса ИБД-Ф на базе ФКУ «ГИАЦ МВД России»[1]. Данная система позволит своевременно выявлять пересечения интересов на региональном и межрегиональном уровне, устанавливать личности предполагаемых мошенников, действующих как на обслуживаемой территории, так и на территориях иных субъектов РФ, организовывать взаимодействие с оперативными подразделениями данных субъектов.
- дефицит следователей и представителей органов дознания, имеющих специальные познания в сфере ИТТ и расследовании преступлений данной категории.

С конца 2018 г. на территории Республики Бурятия участились случаи совершения хищений с использованием услуг IP-телефонии для общения с потерпевшими. При этом сигнал передается через сеть Интернет, и используемый впоследствии номер не имеет ничего общего с обычными городскими или абонентскими номерами операторов связи. Регистрация на использование услуг IP-телефонии может осуществляться дистанционно через интернет без предоставления каких-либо документов, подтверждающих личность пользователя.

Большую сложность для установления виновных лиц в совершении преступлений в сфере ИТТ вызывает дополнительное использование ими программ по подмене номера, отображаемого при звонке потенциальным потерпевшим. Это происходит следующим образом: номер, предоставленный в качестве используемого оператором услуг IP-телефонии, при звонке потерпевшему никак не регистрируется либо имеются факты копирования номеров финансово-кредитных учреждений на схожие с ними. В детализации телефонных соединений отображается ненастоящий номер. Зачастую бывали случаи, когда номером, который используется преступниками в качестве прикрытия, может пользоваться другой вполне реальный человек или организация. Практика по установлению точного места, откуда осуществлялись подобного рода звонки, в настоящее время на территории Республики Бурятия отсутствует.

Таким образом, учитывая, что дистанционные мошенничества в большинстве своем совершаются с использованием IP-телефонии, при совершении которых

[1] Указание МВД России от 09.10.2019 г. № 11/11348.

имеющимися техническими средствами установить виновных лиц не представляется возможным, считаем необходимым для сокращения регистрации данного рода преступлений, вплоть до значительного уменьшения их количества, определить основную задачу — борьбу путем применения мер криминалистической профилактики.

Определение такой профилактики позволяет заключить, что она нацелена на выявление причин и способствующих преступлению условий, объектов криминалистическо-профилактического воздействия, а также связана с разработкой и применением специфических профилактических мер, затрудняющих совершение новых аналогичных преступлений, и пресечением или прерыванием преступной деятельности конкретных лиц. Думается, применение мер профилактики является важной предпосылкой для достижения успеха на пути к снижению числа совершаемых интернет-мошенничеств и иных преступлений в сфере ИТТ.

Системный анализ научной и иной литературы о правоприменительной деятельности позволяет определить в числе действенных направлений в криминалистической профилактике преступлений анализируемой категории как минимум следующие:

1. Информирование населения и профилактика преступлений через СМИ, размещение агитационной информации в общественных местах. Необходимо создавать, транслировать видеоролики просветительского характера. В них может и должна найти отражение информация о типичных способах совершения преступных посягательств, а также информация о наиболее оптимальном поведении лиц, оказавшихся или могущих оказаться жертвами мошенников. Такие видеоролики могут распространяться путем привлечения специалистов профильных служб, на информационных экранах городов, в торгово-развлекательных комплексах, общественном транспорте, в кинотеатрах перед показами фильмов, газетах, а также в эфире телеканалов, во всевозможных социальных сетях и мессенджерах, что позволяет использовать их для демонстрации в эфире региональных и федеральных телевизионных каналов.

2. Организация тесного взаимодействия с представителями жилищно-коммунального хозяйства республики, представителями единых расчетных центров, МУП «Водоканал», комитета городского хозяйства и иных служб и организаций с целью размещения в подъездах жилых домов, в почтовых отделениях связи, а также на бланках оплаты коммунальных услуг агитационных материалов с информацией о видах и мерах предупреждения преступлений в сфере ИТТ.

3. Подключение к вопросам профилактики финансово-кредитных учреждений с целью организации работы с клиентами, проведения комплекса мер по предупреждению мошенничеств и краж со счетов граждан, улучшение мер по аутентификации личности при дистанционном банковском обслуживании. Важно обеспечить филиалы банков наглядной агитацией при операциях, проводимых в банкоматах, личных кабинетах, в сети установить баннерную рекламу профилактического характера.

4. Проработка вопроса с операторами сотовой связи «Теле-2», «МТС», «Мегафон», «Вымпел-Коммуникации» о возможной рассылке клиентам СМС-сообщений профилактического характера.

5. Достижение соглашений с финансово-кредитными учреждениями и операторами сотовой связи в целях установления электронной системы документооборота с МВД и другими заинтересованными правоохранительными органами в целях оперативного обмена информацией и своевременной реакции на факты совершенных преступлений.

6. При одобрении со стороны научного сообщества, практических работников правоохранительных органов направление предложений депутату Государственной Думы РФ от Республики Бурятия для рассмотрения их и возможного внесения законодательной инициативы в Государственную Думу в соответствии с действующим законодательством и внесения дополнений в ФЗ «Об оперативно-разыскной деятельности». Данные дополнения позволят в рамках оперативно-разыскного мероприятия «наведение справок» получать в финансово-кредитных учреждениях без судебного решения сведения о подозрительных счетах, используемых и пополняемых денежными средствами из разных регионов. Также рассмотреть возможность временной блокировки подозрительных расчетных счетов и оперативного получения сведений о движении денежных средств. Быстрое получение информации позволит оперативно раскрывать преступления в сфере ИТТ.

Таким образом, криминалистическая профилактика интернет-мошенничеств является в сложившихся условиях одним из наиболее эффективных способов предупреждения преступлений, совершаемых в сфере ИТТ. Что касается мирового сообщества, оно также признает необходимость консолидации совместных усилий и разработки договора, в котором могут быть изложены основные принципы работы в глобальной сети, обязательные для исполнения. Об этом говорит, в частности, британский программист Тим Бернер-Ли, один из создателей технологии «World Wide Web (Всемирная паутина, WWW). Он подготовил глобальный план действий под названием «Договор сети», или «Контракт для веба», в котором призвал правительства стран, общественность и компании принять все необходимые меры для того, чтобы сделать интернет безопасной, свободной площадкой[1].

Литература

1. Баскаев М. В. Проблемы предупреждения преступлений с использованием сети Интернет // Актуальные вопросы эксплуатации систем охраны и защищенных телекоммуникационных систем : материалы всероссийской научно-практической конференции. 2020. С. 11–12. Текст : непосредственный.

2. Згадзай О. Э. Предупреждение киберпреступности. Проблемы и решения // Вестник Казанского юридического института МВД России. 2011. № 4(6). С. 12–17. Текст : непосредственный.

Статья поступила в редакцию 18.12.2020; одобрена после рецензирования 11.02.2021; принята к публикации 11.03.2021.

[1] Создатель интернета призывает сделать его безопасным. 2019. URL: https://tass.ru/obschestvo/7194953 (дата обращения: 01.02.2021). Текст: электронный.

PREVENTION OF INTERNET FRAUD: PROBLEMS OF DETECTION

Baradi B. Batrov
Research Assistant,
Dorzhi Banzarov Buryat State University
24a Smolina St., Ulan-Ude 670000, Russia
E-mail: bbatrov@gmail.com

Abstract. The article analyzes statistical data indicating a significant increase in Internet fraud in the total array of crimes with the use of information and telecommunication technologies. We have discussed the difficulties that arise in detection of this type of crimes, and the circumstances that complicate the identification of perpetrators. In view of this, we propose to solve the existing problems using the methods and means of forensic prevention. Particular attention is paid to the issues of the correct classification of crimes related to Internet fraud, the development of state programs to combat crimes with the use of Internet technologies, as well as to international cooperation in combating acquisitive crimes with the use of modern digital technologies.
Keywords: criminal law; acquisitive crimes; Internet fraud; detection; forensic prevention; information and telecommunication technologies; malicious software; deanonymization.

For citation
Batrov B. B. Prevention of Internet Fraud: Problems of Detection. *Bulletin of Buryat State University. Law.* 2021; 1: 21–28 (In Russ.).

The article was submitted 18.12.2020; approved after reviewing 11.02.2021; accepted for publication 11.03.2021.