ТАРАСОВА М.Ю.,
кандидат юридических наук, доцент кафедры оперативно-разыскной деятельности и специальной техники Волгоградской академии МВД России
tarasovawo.mariya@yandex.ru

УДК 343.9:343.72

О СОВРЕМЕННЫХ СПОСОБАХ И ВИДАХ МОШЕННИЧЕСТВА, СОВЕРШАЕМОГО С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Дистанционное хищение, мошенничество, преступление в сфере компьютерной информации, преступление против собственности, способ совершения преступления, меры по противодействию мошенничеству.

Стремительный рост числа выявляемых дистанционных хищений, появляющиеся новые способы совершения преступлений с использованием информационно-телекоммуникационных технологий в условиях сложной социально-политической обстановки в стране и мире являются причинами, обусловливающими необходимость формирования инновационного пространства, более эффективного обеспечения информационной безопасности, повышения состояния защищенности в развивающейся информационной среде, совершенствования правовой, кадровой, организационно-управленческой деятельности в этой сфере. В статье рассмотрены наиболее распространенные в настоящее время и недавно появившиеся способы совершения мошенничества с применением высоких технологий, представлены организационно-управленческие меры по противодействию таким преступлениям.

В настоящее время в мире происходит цифровизация всех сфер жизни общества, что дает широкий простор для активной криминальной деятельности, обусловливает рост количества зарегистрированных фактов противоправных деяний, совершенных с использованием информационно-телекоммуникационных технологий (далее - ИТТ). Так, в период с 2017 по 2022 год наблюдалось резкое увеличение числа преступлений, совершенных с применением ИТТ или в сфере компьютерной информации, а также зарегистрированных случаев мошенничеств[1] (см. таблицу 1).

Приведенные в таблице 1 данные свидетельствуют о стремительном увеличении показателей киберпреступности и мошенничества. Эта тенденция прослеживается и в 2023 году, поскольку только за первые два месяца уже было зарегистрировано 62922 преступления, совершенных в сфере высоких технологий, и 93372 мошеннических преступлений. Если выявленный нами тренд к концу 2023 года не изменится, то вполне очевидным будет прирост количества преступлений рассматриваемых видов.

В 2022 году в структуре преступлений против собственности преобладали кражи (59,6%) и мошенничества всех видов (29,3%) [1, с. 31], в структуре киберпреступлений - также мошенничества (47,88%) [1, с. 67]. Согласно статистическим данным МВД России, количество преступлений, совершенных с использованием ИТТ или в сфере компьютерной информации на территории Российской Федерации, в 2022 году превысило полмиллиона и составило четверть от всех уголовно наказуемых деяний[2]. Доля киберпреступлений в общей структуре преступности на территории России за последний год увеличилась незначительно: с 25,8% в 2021 году до 26,5% в 2022 году. Однако существенно вырос размер ущерба от таких деяний. По IT-преступлениям, выявленным органами внутренних дел, он составил 91 миллион 941 тысячу 183 рубля [1, с. 64]. Согласно данным российской телекоммуникационной компании «ТрансТелеКом»[3], киберпреступность остается самым высоколатентным видом преступности, и статистические

[1] Состояние преступности // МВД России: официальный сайт // URL: https://мвд.рф/reports/1/ (дата обращения: 01.04.2023).
[2] Выступление Президента Российской Федерации В.В. Путина на расширенном заседании коллегии МВД России // Кремль: сайт // URL: http://www.kremlin.ru/events/president/transcripts/deliberations/70744 (дата обращения: 01.04.2023).
[3] ТрансТелеКом - российская телекоммуникационная компания, входящая в число крупнейших магистральных операторов связи. Основной ее акционер - ОАО «РЖД». Компания является одним из основных поставщиков магистральных услуг связи в России, а также одним из лидеров среди провайдеров услуг широкополосного доступа в Интернет, телевидения и телефонии для конечных пользователей в регионах. Абонентская база составляет 1,8 млн абонентов.

показатели не отражают ее истинных размеров. При увеличении в 2022 году количества раскрытых мошенничеств (всех видов) по сравнению с 2021 годом в 2,2 раза (с 316 до 681; +365) отмечается рост числа приостановленных уголовных дел на 5,1% (с 3666 до 3854; +188). Уровень раскрываемости преступлений рассматриваемого нами вида увеличился на 7,1%, достигнув 15%, что во многом было обусловлено следующими факторами:

1) обеспечение быстрой внесудебной блокировки мошеннических сайтов по запросу в Генеральную прокуратуру Российской Федерации;

2) внедрение практики, обязывающей кредитные организации по решению суда оперативно предоставлять справки по операциям и счетам юридических лиц, индивидуальных предпринимателей и физических лиц;

3) противодействие Банком России нелегальной деятельности на финансовом рынке посредством внесудебной блокировки сайтов финансовых пирамид;

4) публикация списка компаний с выявленными признаками нелегальной деятельности на финансовом рынке.

Несмотря на повышение уровня раскрываемости мошенничеств, с каждым годом отмечается их незначительный прирост. Стабильно высокий показатель количества зарегистрированных хищений денежных средств граждан (в период с 2020 по 2022 год) обусловлен появлением новых способов их совершения, связанных с социально-экономической обстановкой в стране, последствиями санкций и другими причинами. В настоящее время наиболее распространенными способами совершения дистанционных хищений являются:

1) кража денежных средств с похищенных банковских карт;

2) мошенничество с использованием электронных средств платежа.

Чаще всего преступники имитируют звонки от операторов колл-центров финансовых структур, сотрудников служб безопасности банков. Преступник в телефонном разговоре сообщает своему собеседнику о несанкционированном списании денежных средств со счета его банковской карты, о начислении баллов «Спасибо» от Сбербанка или совершении какой-либо покупки в сети Интернет. При этом он выясняет, какие именно банковские карты находятся в пользовании гражданина, их реквизиты и, произведя нехитрые манипуляции в Интернете, получает доступ к личному кабинету потерпевшего на сайте банка (online-bank). Узнав у жертвы присланный банком в СМС-сообщении код, которым подтверждается совершение операции, преступник похищает денежные средства.

Согласно некоторым исследованиям, преобладающее количество звонков будущим жертвам, а также СМС-сообщений, имеющих признаки подготавливаемого мошенничества, поступает из мест лишения свободы, где отбывают наказание лица, осужденные за совершение преступлений [2]. Отмечается сохранение тенденции увеличения криминальной активности «телефонных» мошенников, действующих с территории Украины[1]. В России правоохранительные органы выстроили достаточно эффективную систему выявления мошеннических колл-центров, вытесняющую владельцев этого «бизнеса» за пределы страны. Украина в этом смысле является максимально удобным местом для мошенников, поскольку препятствий для их деятельности практически не существует: международное сотрудничество правоохранительных органов фактически свернуто, любые «выпады», в том числе криминальные, в сторону России и ее граждан поощряются. Действуют целые организованные группы по 200-400 человек, иногда - до тысячи человек[2].

Еще одной разновидностью интересующего нас способа совершения преступлений являются так

Таблица 1.

Количество преступлений, совершенных с применением информационно-телекоммуникационных технологий или в сфере компьютерной информации, а также количество мошенничеств

Год	2017	2018	2019	2020	2021	2022
Количество преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации	90 587	174 674	294 409	510 396	517 722	522 065
	–	+84 087	+119 735	+215 987	+7 326	+4 343
Количество зарегистрированных фактов мошенничества (всех видов)	222 772	215 036	257 187	335 631	339 606	343 085
	–	–7 736	+42 151	+78 444	+3 975	+3 479

[1] Охота на россиян. Как Украина превратилась в фабрику телефонных мошенников // АиФ: сайт // URL: https://aif.ru/society/safety/ohota_na_rossiyan_kak_ukraina_prevratilas_v_fabriku _telefonnyh_moshennikov (дата обращения: 01.04.2023).

[2] Телефонное мошенничество - и как с ним бороться? Большинство россиян за последние полгода сталкивались с телефонными мошенниками, при этом денежный ущерб понес каждый десятый // ВЦИОМ: сайт // URL: https://wciom.ru/analytical-reviews/analiticheskii-obzor/telefonnoe-moshennichestvo-i-kak-s-nim-borotsja (дата обращения: 01.04.2023).

называемые «инвестиции». Алгоритм приблизительно следующий: пользователи, переходя по всплывающим на экране интернет-ссылкам, попадают на непроверенные сайты, после чего им поступают звонки от злоумышленников, которые могут представиться сотрудниками известных банков. Они предлагают инвестировать средства и обещают по ним высокую доходность. В погоне за быстрой прибылью люди нередко попадаются на уловки, и в результате переведенные ими денежные средства оказываются у преступников, которые по заранее спланированному плану осуществляют обналичивание похищенных денежных средств и скрываются.

«Фишинг» - это хищения, совершаемые путем неправомерного доступа к компьютерной информации (с использованием вредоносного программного обеспечения). Преступник при помощи спам-рассылок и мобильных приложений получает доступ к персональным данным граждан и их банковским картам (мобильным банкам) и похищает денежные средства путем банковских переводов или совершения покупок в Интернет-магазинах, за которые расплачивается деньгами с чужой банковской карты. Классические схемы «фишинга» - вхождения в доверие к жертве с последующим отъемом у нее денежных средств - выглядят следующим образом:

- размещение на специализированных интернет-ресурсах заведомо ложных объявлений о продаже товара либо предоставлении услуг с условием обязательной предоплаты;

- введение в заблуждение граждан предложением оказания брокерских услуг на биржевых платформах, которых в действительности не существует;

- предложение пользователям персональных компьютеров пройти бесплатную регистрацию на заинтересовавших их сайтах, после которой необходимо отправить бесплатное СМС-сообщение с подтверждением введенных данных (нередко в этих целях используются ссылки на сайты, занимающиеся сбором средств на лечение или поддержку больных детей, инвалидов или малоимущих семей);

- рассылка ложных объявлений с предложением перевести деньги на специальный безопасный «антикризисный» счет для сохранения от потери в результате отключения российских кредитно-финансовых учреждений от международной платежной системы либо глобальной блокировки банковских операций.

Сложность расследования преступлений, совершаемых с использованием ИТТ, заключается в отсутствии непосредственной осязаемости и видимости субъектов таких преступлений. Преступники редко совершают преступления рассматриваемого нами вида в том регионе, в котором сами проживают. С целью сокрытия следов преступления они используют SIM-карты и банковские счета, зарегистрированные на подставных лиц, чужие документы и их копии, а также виртуальные платежные системы и карты банков зарубежных государств, не выдающих России сведения об их владельцах.

Увеличение общего числа мошенничеств сопровождалось появлением их новых разновидностей, обусловленных спекуляциями на темы осложнения социально-экономической ситуации в результате санкций, проведения специальной военной операции, частичной мобилизации и т.д. В их числе выделяются мошенничества, осуществляемые:

1) с использованием запрещенных в России социальных сетей;

2) посредством высокоэффективных инвестиционных вложений для проведения операций на международном валютном рынке; посредством якобы подключения к системе быстрых платежей и льготному обмену валют;

3) посредством инвестиций в криптовалюты и пвсевдокриптовалюты;

4) через «посредничество» при оплате банковскими картами услуг зарубежных сервисов или установку VPN-сервисов;

TARASOVA M.YU.,
PhD in Juridical Sciences,
Docent of the Department
of Investigative Activities
and Special Equipment
of the Volgograd Academy
of the Ministry of the
Interior of Russia

ON MODERN METHODS AND TYPES OF FRAUD COMMITTED USING INFORMATION AND TELECOMMUNICATION TECHNOLOGIES

Remote theft, fraud, crime in the field of computer information, crime against property, method of committing a crime, measures to combat fraud.

The rapid growth in the number of detected remote thefts, the emergence of new methods of committing crimes using information and telecommunication technologies in the context of a difficult socio-political situation in the country and the world are the reasons that determine the need to create an innovative space, more effectively ensure information security, and improve the state of security in the developing information environment, improving legal, personnel, organizational and managerial activities in this area. The article discusses the currently most common and recently emerged methods of committing fraud using high technologies, and presents organizational and managerial measures to combat such crimes.

5) путем оформления псевдокомпенсаций;

6) через «посредничество» при аренде и купле-продаже по цене ниже рыночной автомобилей, автозапчастей, электронных приборов и оборудования;

7) в сфере приобретения прав на недвижимость, ранее принадлежавшую иностранным сетям магазинов, ресторанов, предприятиям, объявившим об уходе с российского рынка;

8) путем продажи фиктивных справок для получения отсрочки от мобилизации или предоставления «услуг» по исключению из списка мобилизованных;

9) под предлогом освобождения родственников-военнослужащих, оказавшихся в плену;

10) посредством введения в заблуждение псевдомобилизованными и псевдородственниками мобилизованных [1, с. 28-29].

Таким образом, можно сделать вывод о том, что некоторое особенности социально-политической обстановки в стране оказывают влияние на процессы, связанные с появлением новых способов и разновидностей хищения денежных средств у граждан. Результаты анализа статистических данных и правоприменительной практики свидетельствуют о необходимости формирования в обществе устойчивого понимания алгоритма преступных операций мошенников и представлений о соответствующих собственных действиях для сохранения своих финансовых ресурсов, разработки инновационных подходов к противодействию данным преступлениям, совершенствования правовой, кадровой, организационно-управленческой деятельности [3, с. 199].

Президент Российской Федерации В.В. Путин на расширенном заседании коллегии МВД России отметил активизацию деятельности правоохранительных органов, направленной на предупреждение преступлений в сфере ИТТ, повышение цифровой грамотности населения[1]. Министр внутренних дел В.А. Колокольцев отметил достигнутые благодаря усилиям профильных ведомств и регуляторов финансового рынка результаты в противодействии IT-преступности. Он обратил внимание на риски дистанционных хищений, сопряженные с утечкой персональных данных граждан, обозначил необходимость создания дополнительных механизмов их защиты. А также заявил о повышении уровня раскрываемости преступлений рассматриваемого нами вида в результате наработанных средств и методов их документирования[2].

В связи с этим руководителям территориальных органов внутренних дел целесообразно продолжать положительную практику контроля за организацией и тактикой выявления и раскрытия преступлений, совершаемых в сфере ИТТ; организации разработки эффективных и новых мер по предупреждению хищений денежных средств и повышения финансовой грамотности населения; контроля за информированием населения, за использованием электронного документооборота в сервисе «Госзапросы», в рамках которого налажено взаимодействие с целью получения от различных банков информации о счетах. Необходимо также проводить в подразделениях анализ состояния оперативной обстановки, заслушивать отчеты по результатам работы территориальных органов, осуществлять проверку документации оперативно-разыскного производства и в случае выявления нарушений - назначать служебные проверки, своевременно оказывать организационную и методическую помощь, внимательно подходить к решению вопросов подбора кадров для комплектования подразделений по борьбе с противоправным использованием информационно-коммуникационных технологий. Перечисленные меры в комплексе с регулярными межведомственными совещаниями с отделениями Центрального Банка России, региональной прокуратурой будут препятствовать росту количества преступлений, совершаемых с использованием ИТТ, а в идеале - способствовать его снижению. ■

Библиографический список:

1. Комплексный анализ состояния преступности в Российской Федерации по итогам 2022 года и ожидаемые тенденции ее развития / М.В. Гончарова, С.А. Невский, М.М. Бабаев, Р.В. Черкасов, Е.Б. Аблиязова, Е.М. Тимошина, Г.Ф. Коимшиди, Г.Э. Бицадзе. М.: ВНИИ МВД России, 2023. 102 с.

2. Кудрявцев Р.В. Организация деятельности по раскрытию дистанционных мошенничеств // Молодой ученый. 2019. № 24 (262). С. 218-221.

3. Маркова Е.А. Уголовно-правовая характеристика хищения, совершаемого с использованием электронных средств платежа: Дис. … канд. юрид. наук. СПб, 2021. 251 с.

[1] Выступление Президента Российской Федерации В.В. Путина на расширенном заседании коллегии МВД России // Кремль: сайт // URL: http://www.kremlin.ru/events/president/transcripts/deliberations/70744 (дата обращения: 01.04.2023).

[2] Выступление Министра внутренних дел Российской Федерации В.А. Колокольцева на расширенном заседании коллегии МВД России // Кремль: сайт // URL: http://www.kremlin.ru/events/president/ transcripts/deliberations/70744 (дата обращения: 01.04.2023).