**УДК 343.102**

***М. Ю. Тарасова***
*доцент кафедры*
*оперативно-розыскной деятельности и специальной техники*
*Волгоградской академии МВД России,*
*кандидат юридических наук*

# ОБ АКТУАЛЬНЫХ СПОСОБАХ СОВЕРШЕНИЯ МОШЕННИЧЕСТВ НА СОВРЕМЕННОМ ЭТАПЕ

Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы в качестве приоритетного направления внутренней политики определяет развитие информационных и коммуникационных технологий, формирование информационного пространства и соответствующей инфраструктуры [1]. Информационные технологии все глубже проникают в повседневную жизнедеятельность большинства граждан. С середины 2000-х годов электронные средства массовой информации, информационные системы, социальные сети, технологии беспроводного доступа в сеть Интернет, мобильная связь постепенно становились частью повседневной жизни общества.

Стремительный рост дистанционных хищений, непрерывно появляющиеся способы совершения преступлений с использованием информационно-телекоммуникационных технологий в условиях сложной социально-политической обстановки в стране и мире являются предпосылками для формирования инновационного пространства, более эффективного обеспечения информационной безопасности, повышения состояния защищенности в развивающейся информационной среде, совершенствования правовой, кадровой, организационно-управленческой деятельности.

В период с 2018 года по настоящее время наблюдается рост преступлений, совершенных с использованием информационно-телекоммуникационных технологий (далее — ИТТ) или в сфере компьютерной информации, а также увеличивается количество зарегистрированных фактов мошенничеств. Так, например, в 2017 году было зарегистрировано 90 587 преступлений, совершенных с использованием ИТТ или в сфере компьютерной информации, 222 772 фактов мошенничеств (всех видов), в 2018 году — 174 674; 215 036, в 2022 году — 522 065; 343 085 соответственно [2].

В 2022 году в структуре преступлений против собственности преобладают кражи (59,6 %) и мошенничества всех видов (29,3 %). 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 [3, с. 31].

В настоящее время наиболее распространенными способами совершения дистанционных хищений являются:

1. Кража денежных средств с похищенных банковских карт.

2. Поступление звонков от операторов, сотрудников службы безопасности банков. Преступник сообщает своему собеседнику о несанкционированном списании денежных средств с его банковской карты (счета), начислении баллов «Спасибо» от Сбербанка» или совершении какой-либо покупки в сети Интернет. При этом злоумышленник узнает, какие именно банковские карты находятся в пользовании гражданина, их реквизиты и, произведя нехитрые манипуляции в сети Интернет, получает доступ к личному кабинету (online-bank) потерпевшего. Узнав СМС-коды, преступник похищает денежные средства. Преобладающее большинство массовых звонков будущим жертвам, равно как и СМС-сообщений, поступает из мест лишения свободы, где лица, осужденные за иные преступления, отбывают наказание [4]. Так, на номер абонента поступает звонок или текстовое сообщение с привлекательным предложением и просьбой перевода незначительной суммы денег по номеру мобильного телефона или банковской карты.

3. Отмечается сохранение тенденции увеличения криминальной активности хищений, совершенных путем неправомерного доступа к компьютерной информации (с использованием вредоносного программного обеспечения). Преступник при помощи спам-рассылок и мобильных приложений получает доступ к персональным данным банковских карт граждан (мобильным банкам) и при помощи транзакций совершает хищение денежных средств путем банковских переводов и покупок в интернет-магазинах.

4. Размещение на специализированных ресурсах заведомо ложных объявлений о продаже товара либо предоставлении услуг с условием обязательной предоплаты.

5. Введение в заблуждение граждан путем оказания брокерских услуг на биржевых «псевдоплатформах».

Повышение количества зарегистрированных фактов мошенничеств обусловлено появлением новых способов их совершения, связанных с социально-экономической обстановкой в стране, последствиями санкций, проводимой специальной военной операцией на территории Украины, частичной мобилизацией. Среди уже известных способов совершения дистанционных мошенничеств появляются новые, осуществляемые:

1) при использовании запрещенных в России социальных сетей;

2) посредством осуществления 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 псевдокриптовалюты.

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

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 иностранной сети ресторанов быстрого питания и предприятий, объявивших об уходе с российского рынка; при продаже фиктивных справок для получения отсрочки от мобилизации;

8) также для предоставления «услуг» по исключению из списка мобилизованных;

9) под предлогом освобождения родственников-военнослужащих из плена на Украине;

10) со стороны псевдомобилизованных и псевдородственников мобилизованных [3, с. 28].

Совершив дистанционное хищение денежных средств, преступники обычно используют следующие основные способы вывода похищенных денежных средств:

1. Перевод похищенных денежных средств с банковской карты на карту, где в дальнейшем происходит физическое обналичивание через банкоматы различных банков. Следует отметить, что банковские карты, используемые в преступных целях, зарегистрированы на асоциальных граждан, приобретены через сеть Интернет или посредников. Также в современных банкоматах отсутствуют камеры видеонаблюдения, что усложняет идентифицировать лицо, производящее снятие наличных денежных средств.

2. Переводы на QIWI-Банк, кошельки (виртуальные карты), переводы в электронную валюту (биткоин), вывод денежных средств через букмекерские организации и биржевые фонды, где зачастую при оформлении счетов не требуется подтверждение личности либо существует дистанционная регистрация при направлении фотокопии паспорта гражданина.

3. Приобретение различных товаров через интернет-магазины, которые в дальнейшем забираются неустановленными лицами с различных точек выдачи при предъявлении электронного онлайн-чека.

Ущерб от хищений денежных средств, совершенных с применением ИТТ, в Российской Федерации в 2022 году составил 91 941 183 тыс. руб. [3, с. 64].

В этой связи Президент Российской Федерации В. В. Путин на Расширенном заседании коллегии Министерства внутренних дел России обратил внимание на активизацию деятельности правоохранительных органов, направленную на предупреждение преступлений в сфере ИТТ, повышение цифровой грамотности населения [5].

Министр внутренних дел генерал полиции В. А. Колокольцев отметил достигнутые результаты в противодействии IT-преступности усилиями профильных ведомств и регуляторов финансового рынка, обратил внимание на риски дистанционных хищений, сопряженных с фактами утечки персональных данных граждан, обозначил необходимость создания дополнительных механизмов их защиты, а также заявил о повышении уровня раскрываемости рассматриваемых преступлений в результате наработанных средств и методов документирования IT-преступлений [5].

Изучение оперативными сотрудниками и следователями способов совершения и разновидностей «дистанционных» мошенничеств играет важную роль в вопросах противодействия рассматриваемым преступлениям, имеет большое практическое значение для раскрытия и расследования преступлений, так как от осведомленности о структуре, содержании, об особенностях поведения мошенника, его технических возможностях вывода похищенных денежных средств во многом зависят выбор тактики раскрытия противоправного деяния, необходимость привлечения специалистов, организация взаимодействия с различными органами и службами, разработка профилактических мер.

1. О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы [Электронный ресурс] : Указ президента Рос. Федерации, 9 мая 2017 г., № 203. Доступ из справ.-правовой системы «КонсультантПлюс». Вернуться к статье

2. Состояние преступности Официальный сайт МВД России [Электронный ресурс] // Официальный сайт Министерства внутренних дел Российской Федерации. URL: https://мвд.рф/reports/1/ (дата обращения: 01.04.2023). Перейти к источнику Вернуться к статье

3. Комплексный анализ состояния преступности в Российской Федерации по итогам 2022 года и ожидаемые тенденции ее развития / М. В. Гончарова [и др.]. М. : ФГКУ «ВНИИ МВД России», 2023. 102 с. Вернуться к статье

4. Кудрявцев Р. В. Организация деятельности по раскрытию дистанционных мошенничеств [Электронный ресурс] // Молодой ученый. 2019. № 24 (262). С. 218–221. URL: https://moluch.ru/archive/262/60528/ (дата обращения: 02.04.2023). Перейти к источнику Вернуться к статье

5. Расширенное заседание коллегии МВД [Электронный ресурс] // Администрация Президента России. URL: http://www.kremlin.ru/events/president/transcripts/deliberations/70744 (дата обращения: 01.04.2023). Перейти к источнику Вернуться к статье