УДК 343.9
ББК 67.51

DOI 10.22394/1682-2358-2021-4-52-60

D.A. Brekhov, *post-graduate student of the Criminology Department, V.Ya. Kikot' Moscow University of the Ministry of Internal Affairs of the Russian Federation*

METHODS OF COMMITTING FRAUD USING THE INTERNET, MOBILE COMMUNICATIONS AND REMOTE BANKING SYSTEMS

The article deals with the problems associated with the lack of a clear specification and a unified approach in the terminology used in the implementation of quantitative accounting and classification of new ways of committing crimes in the field of information technology. A typology of these crimes is proposed, which makes it possible to create a single mechanism for accounting and analytical operations in assessing the state and dynamics of cybercrime.

Key words and word-combinations: cybercrime, Internet fraud, information technology crime.

Д.А. Брехов, *адъюнкт кафедры криминологии Московского университета МВД России им. В.Я. Кикотя (email: 89266666634@mail.ru)*

СПОСОБЫ СОВЕРШЕНИЯ МОШЕННИЧЕСКИХ ДЕЙСТВИЙ С ИСПОЛЬЗОВАНИЕМ СЕТИ «ИНТЕРНЕТ», СРЕДСТВ ПОДВИЖНОЙ СВЯЗИ И СИСТЕМ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ

Аннотация. Рассматриваются проблемы, связанные с отсутствием конкретизации и единого подхода в терминологии, применяемой при осуществлении количественного учета и классификации новых способов совершения преступлений в сфере информационных технологий. Предлагается типология этих преступлений, что дает возможность создать единый механизм учетно-аналитических операций при оценке состояния и динамики киберпреступности.

Ключевые слова и словосочетания: киберпреступность, мошенничество в сети «Интернет», преступления в сфере информационных технологий.

В условиях постоянного роста преступлений в сфере информационных технологий на территории государств — участников Содружества Независимых Государств происходит консолидация

усилий правоохранительных органов стран Содружества по ряду направлений международного взаимодействия [1].

В связи с появлением новых способов совершения преступлений в сфере информационных технологий приходится констатировать, что принимаемых мер по противодействию этому виду криминала явно недостаточно. Особенно остро обозначилась проблема распространения вредоносных компьютерных программ, представляющих угрозу государственным и транснациональным информационным ресурсам. Правоохранительные органы фиксируют активные попытки криминальных структур использовать открытые телекоммуникационные и ведомственные информационные сети для проведения крупных финансовых махинаций и мошеннических акций.

Особую тревогу правоохранительных органов стран Содружества вызывает практика использования информационных технологий террористическими организациями по поиску и вербовке граждан, манипуляции массовым сознанием и распространению экстремистских взглядов.

Основную долю компьютерных инцидентов составляет распространение вредоносных программ, предназначенных для хищения учетных записей пользователей Интернета, и преступления, связанные с электронными платежными системами. Способы совершения подобных преступлений обусловлены особенностями предмета и средств их совершения, использованием в преступных целях установленного порядка осуществления банковских операций по переводу безналичных денежных средств, находящихся на счетах банковских платежных карт, с использованием средств мобильной связи, а также порядка оказания услуг подвижной (мобильной) связи операторами.

Мошеннические действия, в том числе с использованием мобильных средств связи, путем перевода денежных средств со счетов банковских карт потерпевших на счета третьих лиц в большинстве случаев совершаются в отношении держателей банковских карт и подключенных к системам дистанционного банковского обслуживания.

Анализ материалов судебной практики позволяет классифицировать способы завладения чужими денежными средствами, находящимися на счетах банковских карт потерпевших.

Цифровая революция принесла не только блага, новейшие технологии все активнее берет на вооружение и криминалитет: «Посредством Интернета совершаются хищения чужого имущества, ведется торговля наркотиками, оружием, людьми, распространяется экстремистская литература, вербуются новые члены террористических группировок. Среди новых угроз — мошенничества с использованием сотовой связи, а

также средств IP-телефонии. Преступники научились подменять подлинные телефонные номера кредитных организаций, государственных служб, выдавая себя за их работников. В прошлом году число противоправных деяний, совершенных с применением информационных технологий, увеличилось в два раза, в январе — сентябре текущего года — почти на 70%» [2].

За последние несколько лет многое сделано для повышения результативности предупреждения и пресечения таких преступлений, сокращения возможности использовать передовые технологии в незаконных целях. Совершенствуется нормативная правовая база, в частности, ужесточена ответственность по отдельным видам IT-преступлений и административных правонарушений. В практическую деятельность внедряются новые формы и методы противодействия им. Заключены соглашения об информационном взаимодействии в электронном виде между МВД России и государственными органами, а также рядом финансово-кредитных организаций на федеральном и региональном уровнях. Для качественного расследования уголовных дел этой категории создаются следственно-оперативные группы из числа наиболее подготовленных сотрудников.

В 2020 и в начале 2021 г. в полтора-два раза выросло число раскрытых IT-преступлений и направленных в суд уголовных дел. В два раза больше установлено виновных лиц. С 2018 г. в московском регионе задержаны организованные группы, общей численностью почти тридцать человек, совершавших мошеннические действия в отношении пожилых граждан на территории пяти субъектов РФ. Используя мобильную связь, они представлялись сотрудниками банков, социальных служб и под видом получения компенсации за покупку ранее приобретенных товаров или лекарств похищали сбережения пенсионеров. Доказана причастность фигурантов к 87 эпизодам [3].

В мае 2021 г. пресечена деятельность группы, управлявшей сетью медицинских клиник в ряде регионов России, в том числе в Москве и Санкт-Петербурге. Злоумышленники через колл-центры приглашали пациентов, вводили их в заблуждение о наличии заболеваний, требующих неотложного дорогостоящего лечения, и для оплаты фиктивных медицинских услуг склоняли к оформлению кредитов на суммы до полумиллиона рублей. Установлено более 11 тысяч потерпевших. По предварительным данным, общая сумма ущерба превышает миллиард рублей [3].

Важной задачей сегодня является мониторинг, блокировка и удаление противоправного контента: «Во взаимодействии с Генеральной прокуратурой, Роскомнадзором, а также сайтов и страниц, через которые распространяются наркотики, детская порнография, требуется разработка механизмов оперативной блокировки и мошеннических колл-центров, фишинговых сайтов, интернет-пирамид».

1. *Введение потерпевшего в заблуждение относительно целей перевода денежных средств путем совершения ему телефонных звонков или направления СМС-сообщений.*

Под воздействием заблуждения потерпевший самостоятельно производит перевод денежных средств со своего счета на счета третьих лиц с использованием систем «Интернет-банкинг» и «Мобильный банкинг» через терминалы банков или иным способом.

1.1. Побуждение потерпевшего к совершению действий по переводу денежных средств со своего счета на счета третьих лиц путем сообщения ему по телефону или направлением СМС-сообщения ложных сведений о внезапно возникших у его близких родственников серьезных неприятностей и проблем, связанных с несчастными случаями, совершением дорожно-транспортного происшествия, причинением вреда здоровью третьих лиц, задержанием за хранение наркотических средств, совершением других преступлений либо с долговыми обязательствами, для незамедлительного решения которых срочно требуется определенная сумма денег.

При этом злоумышленники осуществляют звонки или направляют СМС-сообщения потерпевшим по случайно подобранным абонентским номерам телефонов, как мобильных, так и стационарных, представляются от имени их родственников, друзей, знакомых или сотрудников правоохранительных органов, а также указывают абонентский номер телефона или номер банковской карты, на который следует осуществить перевод и сумму денежных средств, которую необходимо перечислить. Во многих случаях мошенничество данным способом совершают лица, отбывающие наказание в местах лишения свободы.

1.2. Уведомление потерпевшего по телефону (в основном путем рассылки СМС-сообщений) о выпавшем ему крупном призе при розыгрыше лотереи и необходимости перевода определенной суммы денежных средств на указанный номер телефона или платежного средства в качестве налоговых или иных платежей как условия получения приза.

1.3. Направление потерпевшему посредством СМС-сообщений ложных уведомлений о зачислении на его банковский счет определенной суммы денег, а через некоторое время новых сообщений об ошибочном зачислении этих сумм с просьбой возврата их посредством перевода на указываемый номер телефона или банковской карты.

1.4. Осуществление звонков потерпевшим от имени оператора связи с предложением подключить новую услугу и набрать для этого под диктовку определенный код, который в действительности является комбинацией для перевода денежных средств со счета абонента на счет третьего лица.

1.5. Сообщение потерпевшему заведомо ложных сведений посредством телефонных звонков или путем направления СМС-сообщений от имени банка о якобы возникших технических или иных проблемах, препятствующих дальнейшему использованию им своей банковской карты с предложением совершить для устранения данных препятствий определенные операции по банковскому счету через системы «Интернет-банкинг», «Мобильный банкинг» или через терминал банка. Совершение потерпевшим, введенным в заблуждение, данных операций приводит в действительности к переводу денежных средств со счета его банковской карты на счет третьего лица.

Такие действия производятся лицами, совершающими мошенничество, как правило, двумя способами.

Первый способ: потерпевшему направляется ложное уведомление посредством СМС-сообщения от имени банка о временной блокировке банковской карты с предложением навести справки по указанному в СМС-сообщении номеру телефона.

В случаях, когда потерпевший, позвонив по данному номеру, пытается выяснить причину блокировки его банковской карты, лицо, совершающее мошенничество, представившись сотрудником службы безопасности банка, объясняет причины блокировки карты попытками посторонних лиц получить информацию о реквизитах банковской карты или о банковском счете, сбоями в работе сервера банка либо иными надуманными причинами.

Затем злоумышленники, в зависимости от информации, предоставленной потерпевшим при ответах на поставленные вопросы, предлагают совершить определенные действия посредством «Интернет-банкинга», «Мобильного банкинга» либо через ближайший банкомат. При этом потерпевшему сообщается о необходимости оперативного совершения данных действий, поскольку в противном случае якобы возникнет необходимость совершения операции замены карты, которая может затянуться на долгое время, в течение которого воспользоваться денежными средствами на карте будет невозможно.

В случае согласия потерпевшего на выполнение ложной операции разблокировки карты он подходит к банкомату и, перезвонив по указанному ему номеру телефона, действуя под диктовку, вставляет свою банковскую карту в банкомат, набирает на нем код доступа к карте и сообщает остаток денежных средств на карте. Затем набирает под диктовку цифры, якобы код для разблокировки карты, а в действительности переводит денежные средства со своей карты на банковскую карту или на лицевые счета абонентских номеров сотовых операторов третьих лиц, либо к его телефону подключают услугу «Интернет-бан-

кинг» или услугу «Мобильный банк», позволяющую управлять счетом его банковской карты.

При этом потерпевшему становится известно по полученным чекам или поступающим СМС-уведомлениям об осуществлении им операции перевода денежных средств. Однако потерпевшего убеждают, что переведенные им денежные средства зарезервированы и в течение нескольких часов будут возвращены обратно на его счет и предлагают не пользоваться картой до их поступления [4].

После этого лица, совершающие мошенничество, переводят поступившие денежные средства на банковские счета других лиц либо на счета до востребования через системы денежных переводов, осуществляемых отдельными кредитными учреждениями. При этом денежные средства в банке получают лица, неосведомленные об истинном их происхождении, за денежное вознаграждение и далее передают их незнакомым им лицам.

Используемые мошенниками для рассылки СМС-сообщений, разговоров с потерпевшими и для перечисления денежных средств абонентские номера операторов связи, как правило, оформляются ими на вымышленных лиц, а банковские карты, на которые перечисляются похищенные денежные средства, принадлежат, как правило, не имеющим к ним отношения лицам, которые по просьбе других лиц или по своей инициативе оформляют их на свое имя и передают за денежное вознаграждение малознакомым или вообще незнакомым лицам.

Второй способ: введение в заблуждение (в том числе с помощью методов социальной инженерии, то есть с использованием познаний в области психологии) держателя банковской карты (владельца счета) относительно сущности операций, для получения информации, необходимой для несанкционированного доступа, либо вынуждения потерпевшего совершить необходимые злоумышленнику действия.

Лица, совершающие мошенничество, при первом телефонном разговоре с потерпевшим выясняют, что абонентский номер его телефона подключен к системе дистанционного банковского обслуживания. Поводом к образованию доверительных отношений с потерпевшим может стать, например, то, что преступник представляется сотрудником службы социального обеспечения либо сотрудником банка, целью которого является перечисление дополнительной социальной выплаты и т.п.

Затем злоумышленники предлагают потерпевшему посредством данной системы совершить для разблокировки банковской карты операции якобы по временному резервированию денежных средств, находящихся на его банковском счете, а в действительности по переводу их на счета третьих лиц. После этого потерпевший, введенный в заблуж-

дение, переводит под диктовку денежные средства со своего счета на указанный ему счет банковской карты или абонентский номер, будучи уверенным, что переведенные им денежные средства в течение суток поступят обратно на его банковский счет.

К разновидностям введения в заблуждение потерпевшего также следует отнести перевод средств со счета потерпевшего посредством использования системы «СМС-банкинга» — разновидности технологии дистанционного банковского обслуживания с использованием СМС-сообщений, в которой доступ к банковским счетам и операциям по банковским счетам предоставляется в любое время с использованием номера мобильного телефона клиента, предварительно зарегистрированного в банке. Эта технология, помимо пассивного СМС-оповещения о проведенных операциях и состоянии счета, позволяет осуществлять «активное» СМС-оповещение — отправку СМС-сообщений в ответ на получаемые от клиента СМС-запросы, например, запрос баланса банковской карты или счета, мини-выписки или блокировки банковской карты, а также отправлять банку через сеть оператора подвижной связи команды на проведение операций с денежными средствами клиента банка-владельца сим-карты.

Лица, совершающие мошенничество, также используют способ совершения операций по USSD-запросам, когда обращаются к потерпевшему с просьбой набрать USSD-команду или отправить СМС на специализированный номер банка для совершения перевода.

1.6. Вмешательство в функционирование средств хранения, обработки и передачи компьютерной информации и информационно- телекоммуникационных сетей путем блокирования абонентского номера потерпевшего, восстановления его на дубликат сим-карты и перечисления денежных средств с банковского счета потерпевшего посредством системы «Мобильного банкинга», перевод денежных средств с банковской карты потерпевшего на счета третьих лиц.

В некоторых случаях для получения дубликата сим-карты, установленной в телефоне потерпевшего, мошенники могут вступать в сговор с представителями оператора связи, работающими в офисах продаж и обслуживания клиентов. В отдельных случаях данные преступления совершаются представителями оператора связи самостоятельно.

Особенностью указанных способов совершения мошенничества является отсутствие непосредственного контакта лиц, их совершающих, с потерпевшими, поскольку последние вводятся в заблуждение и побуждаются к совершению определенных действий посредством средств дистанционной коммуникации.

2. *Использование найденного, похищенного, приобретенного либо случайно оказавшегося у субъекта преступления чужого телефонного*

аппарата с абонентским номером владельца, подключенного к услуге «Мобильный банкинг».

Потерпевший, у которого телефонный аппарат по тем или иным причинам выбыл из владения (утерян, похищен, продан вместе с сим-картой), своевременно не обращается в банк с просьбой отключить от его абонентского номера услугу «Мобильный банк» либо сам передает свой телефонный аппарат другому лицу для временного пользования или оставляет его временно без присмотра. Лица, совершающие мошенничество, обнаружив при пользовании телефоном, что тот подключен к указанной услуге, совершают хищение денежных средств, находящихся на банковском счете потерпевшего.

3. *Использование подключенного к услуге «Мобильный банкинг» абонентского номера, ранее принадлежавшего другому абоненту.*

Данный способ совершения мошенничества заключается в использовании лицами, его совершающими, того обстоятельства, что потерпевший, осуществив замену абонентского номера своего телефона, подключенного к услуге «Мобильный банкинг», не предупредил об этом кредитную организацию, а его абонентский номер впоследствии был перерегистрирован оператором связи на имя другого лица. Обнаружив при пользовании телефоном с таким абонентским номером, что тот подключен к услуге «Мобильный банкинг», новый владелец номера производит посредством указанной услуги перевод денежных средств потерпевшего на свой банковский счет или на счета третьего лица.

Так, Н. была осуждена за совершение преступлений, предусмотренных ч. 1 и 2 ст. 159.6 УК РФ «Мошенничество в сфере компьютерной информации». Согласно приговору суда Н., получив на мобильный телефон электронное сообщение о доступном лимите денежных средств на не принадлежащем ей банковском счете, открытом на имя Ш., имела умысел на хищение указанной суммы и, реализуя его, используя принадлежащий ей мобильный телефон и сим-карту, к которой была ошибочно подключена услуга мобильного банка Сбербанка России, предоставляющая техническую возможность распоряжаться денежными средствами, находящимися на расчетном счету Ш., путем ввода компьютерной информации в форме электрических сигналов (СМС-сообщения на номер 900) посредством телекоммуникационной сети оператора сотовой связи похитила денежные средства, принадлежащие Ш. (приговор Грачевского районного суда Ставропольского края от 13 июня 2013 г. по уголовному делу № 1-82/2013 [Электронный ресурс]. Доступ из СПС «КонсультантПлюс»).

В настоящее время отмечается некоторое видоизменение схем хищения денежных средств в системах дистанционного банковского об-

служивания (ДБО). Злоумышленники адаптировались к возрастающему уровню безопасности банковских систем.

Например, российскими кредитными организациями в 2017 г. утверждены принципы «двухфакторной авторизации», предполагающей проведение операции по двум независимым каналам (аккаунт ДБО, звонок по телефону, СМС-подтверждение, код со скретч-карты или чека, электронная подпись и др.). В ответ на эти меры представители российских ОПС начали использовать методы замены сим-карт легальных владельцев банковских счетов. Ранее указанные действия были характерны для мелкого мошенничества, однако в текущем году объектами преступных посягательств стали главные бухгалтеры и руководители крупных коммерческих предприятий. Объем похищенных денежных средств в таких случаях исчисляется миллионами рублей.

В заключение отметим, что противодействие использованию информационных сетей преступными группами, специализирующимися на вымогательствах, мошенничествах и кражах, совершении преступлений в сфере компьютерной информации, а также защита важнейших информационных инфраструктур от кибератак имеют ключевое значение для внешней и внутренней безопасности как отдельно взятых государств, так и стран СНГ в целом [5].

Решение этой задачи предполагает совместную работу правоохранительных и иных государственных органов, выстраивание взаимодействия и обмена информацией на национальном и межгосударственном уровне, а также выработку и реализацию комплекса нормативно-правовых и организационных мер по противодействию деятельности террористических и иных преступных организаций и сообществ.

Библиографический список

1. *Кузнецов А.Г.* Криминальные риски использования блокчейн-технологий и криптовалюты на территории государств – участников СНГ // Вестник Поволжского института управления. 2021. Т. 21, № 1. С. 48–55.

2. *Давыдова Б.Д.* Преступление в сфере информационных технологий // Проблемы совершенствования законодательства: сборник научных статей студентов юридического факультета. Махачкала, 2020. С. 89–91.

3. Материалы заседания коллегии МВД России от 1 нояб. 2019 г. URL: https://мвд.рф/news/item/18808269/

4. *Лямцев А.Н.* Мобильные коммуникационные устройства и их использование в противоправных целях // Вопросы современной науки и практики / Университет им. В.И. Вернадского. 2014. № 4(54). С. 200–204.

5. Аналитический обзор: Новые способы совершения преступлений в сфере информационных технологий на территории государств – участников СНГ в 2017 г. / И.Б. Колчевский, В.М. Журавлев, А.Г. Кузнецов [и др.]. М., 2017.