УДК 343.9.01

О.А. Старостенко

АНАЛИЗ СХЕМ IT-МОШЕННИЧЕСТВА: КЛАССИФИКАЦИЯ И ПРОТИВОДЕЙСТВИЕ

В статье проведен анализ распространенных преступных схем IT-мошенничества, рассмотрена динамика кибермошеннических действий на территории России за период 2019–2020 гг. Выявлено, что важнейшим элементом механизма преступного поведения кибермошенника выступает способ совершения преступления. Эмпирический анализ взглядов ученых-криминологов на способ совершения IT-мошенничества позволил выделить три его основных свойства (действия должны совершаться в процессе преступного деяния; действия направлены на достижение преступного результата; в действиях отражаются индивидуальные особенности преступления). Анализ преступных схем позволил систематизировать данные, разработать авторские критерии их классификации (в зависимости от каналов коммуникации; по области воздействия; по референтивным средствам; по степени психоэмоционального воздействия на жертву), а также традиционные и криминологические способы противодействия IT-мошенничеству, которые смогут помочь пользователю избежать смешения и пересечения понятий, систематизировать данные, укрепить личную и имущественную безопасность в киберпространстве.

Ключевые слова: IT-мошенничество, преступная схема, способ, безопасность, жертва, Интернет, злоумышленник, механизм поведения.

DOI: 10.35634/2412-9593-2021-31-6-1072-1077

В настоящее время информационно-телекоммуникационные технологии являются одной из быстроразвивающихся областей. Использование сети Интернет и осуществление профессиональных обязанностей в режиме онлайн становятся повседневным явлением. Прогресс в области цифровых технологий сопровождается активным развитием преступной деятельности, а такие действия, как повышенная активность в социальных сетях, покупка товаров, оказание коммерческих услуг и обмен документами посредством использования электронной почты особенно сильно привлекают внимание IT-мошенников.

Согласно официальной статистике Генпрокуратуры, за четыре месяца 2020 г. число случаев кибермошенничества выросло на 78 % по сравнению с первыми шестью месяцами 2019 г. Мошеннические способы продолжают усложняться, а идентифицировать преступное поведение пользователя информационно-телекоммуникационными технологиями становится все труднее[1].

Как правило, механизм преступного поведения кибермошенника состоит из преступной мотивации, психологических свойств личности, выбора способа совершения преступления, характера поведения жертвы и конкретной ситуации[2].

В науке криминологии мотив занимает существенное место в объяснении движущих сил поведения индивида. Г.А. Аванесов под мотивом понимает внутренне побуждение к тому или иному поступку и рассматривает его как непосредственную причину преступления. Автор полагает, что изучение мотива позволяет выделить основные составляющие противоправного поведения лица в конкретной жизненной ситуации[3].

Ю.М. Антонян считает, что мотив представляет собой важнейший компонент личности, выступающий внутренним стимулом поведения, то, ради чего оно реализуется. Это не цель, не задача, которую ставит перед собой человек, это смысл поведения[4].

А.Н. Леонтьев рассматривал мотив в качестве определенной потребности[5].

---

[1] Статистические данные о зарегистрированных преступлениях на территории Российской Федерации в маеиюне 2020 года. Генеральная прокуратура Российской Федерации. URL: http://genproc.gov.ru (дата обращения: 16.03.2021)

[2] Криминология: учебник / под ред. В.Н. Кудрявцева, В.Е. Эминова. М.: Юристъ, 1997. 512 с.

[3] Аванесов Г.А. Популярная криминология. Очерки общей части: учеб. пособие. М.: Юнити-Дана; Закон и право, 2014. 159 с.

[4] Антонян Ю.М. Криминология: учебник для академического бакалавриата. 3-е изд., перераб. и доп. М.: Юрайт, 2018. 388 с. Сер.: Бакалавр. Академический курс.

[5] Леонтьев А.Н. Деятельность. Сознание. Личность. М.: Смысл, Академия, 2005.

С.Л. Рубинштейн к числу мотивов относил человеческие интересы и потребности, определяя первых как преломленные в сознании движущие силы поведения индивида[6].

Основным мотивом IT-мошенничества является корысть и осознанное желание обогатиться, в отдельных случаях – зависть и желание самоутвердиться. Реализуя корыстную цель, кибермошенник удовлетворяет свои корыстные побуждения.

Зарубежная киберкриминология раскрывает основные элементы IT-мошенничества, образующие так называемый квадрат кибермошенничества:

– нехватка денежных средств;

– возможность скрывать электронные следы мошеннических действий;

– сетевая анонимность;

– безнаказанность ввиду «юрисдикционной дилеммы».

Согласно исследованиям A Banerjee, D Barman, M Faloutsos, в 90 % случаев IT-мошенничества побуждающим фактором выступили нехватка денежных средств и приверженность к сетевым азартным играм[7].

Определяющим элементом индивидуального преступного поведения кибермошенника является выбранный им способ совершения преступного деяния, который представляет собой не просто образ действий, а определенную целостную структуру поведения. Способов совершения IT-мошенничества весьма много: от элементарных, примитивных до сложно выстроенных схем преступного деяния.

В криминологическом сообществе способ совершения преступления принято рассматривать как составной элемент механизма преступного поведения, представляющего собой процесс, основанный как на действиях, способных оказывать влияние на внешнюю среду, так и на психологических явлениях, определяющих генезис противоправного поведения.

Как правило, способ совершения преступления обладает тремя основными свойствами:

1) действия должны совершаться в процессе преступного деяния;

2) действия направлены на достижение преступного результата;

3) в действиях отражаются индивидуальные особенности преступления.

Полагаем, что способ необходимо рассматривать не просто как элемент механизма преступного поведения, но и его планирования: «Планирование преступного поведения зависит непосредственно от личности преступника и текущей обстановки, а способом совершения преступления выступает совокупность преступных приемов»[8].

Рассмотрим актуальные на сегодняшний день способы совершения мошеннических действий (преступные схемы) в информационной среде.

1. *Использование уязвимости*. Существующие требования социального дистанцирования (в связи с пандемией COVID-19) привели к возникновению виртуального взаимодействия. Режим дистанционного взаимодействия начал осуществляться с использованием приложений систем онлайн-обучения (LMS) и видео-конференц-связи (Zoom)[9]. Много случаев выявления и использования IT-мошенниками уязвимостей в вышеупомянутых системах было зафиксировано и в России. Сообщается, что одна популярная, но уязвимая платформа была взломана из-за слабого механизма безопасности и пароля, в результате чего злоумышленники смогли захватить сеансы видео-конференц-связи и получить доступ к содержимому конференции.

2. *Ложные благотворительные фонды*. Преступники спекулируют на человеческих чувствах (путем обмана или злоупотребления доверием): принуждают участвовать в благотворительных денежных сборах (пожертвованиях).

3. *Создание фиктивных Всемирных организаций здравоохранения, осуществляющих поддержку граждан в период пандемии COVID-19*. Жертве путем обмана или злоупотребления доверием навязывают ошибочное мнение, в результате которого она сознательно оплачивает услуги здравоохранения в фонд поддельной клиники.

---

[6] Рубинштейн С.Л. Основы общей психологии. СПб.: Питер, 2000. С. 430.

[7] Banerjee A. et al. Cyber-fraud is one typo away //IEEE INFOCOM 2008-The 27th Conference on Computer Communications. IEEE, 2008. С. 1939-1947.

[8] Шиханцов Г.Г. Криминология / ГрГУ имени Янки Купалы. URL http://ebooks.grsu.by/criminal/2-prichiny-i-usloviyaprestupnosti-nesovershennoletnikh-i-ikh-preduprezhdenie.htm (дата обращения: 16.04.2021).

[9] Alves-Foss J., Barbosa S. Assessing computer security vulnerability // ACM SIGOPS Operating Systems Review. 1995. Vol. 29, no. 3. P. 3-13.

4. *Оказание помощи в получении пособий*. Злоумышленники запрашивают персональные данные жертвы для оформления несуществующих государственных компенсаций ущерба от распространяемых вирусов с целью незаконного обогащения. Также актуальной мошеннической схемой выступает отсрочка платежей и урегулирование взысканий по обязательной предоплате, получив которую преступник скрывается.

5. *Поддельные курьерские службы заказы еды и лекарств с обязательной оплатой заказа на сайте*. Внешне сайты не имеют отличий от «подлинных», но по факту оплата проходит в пользу злоумышленника.

6. *Поддельные агентства по трудоустройству*. Злоумышленники создают фиктивные кадровые агентства, осуществляющие прием граждан на работу в удаленном формате. Соискатель вносит в анкету персональные данные, после чего получает письмо о принятии на работу и необходимости перевести деньги за «некое оборудование», в результате чего становится жертвой мошеннических действий[10].

7. *Нарушение конфиденциальности*. Получение доступа к персональным данным вопреки протоколам защиты данных путем целенаправленного воздействия на серверы, компьютеры, смартфоны и хищение денежных средств (ст.159.6 УК РФ).

8. *Перехват компьютерных данных*. Обеспечение неправомерного доступа к компьютерной системе, например, когда злоумышленник обходит брандмауэр, используя вредоносное ПО, получает доступ к компьютерной системе и др. и совершает хищение денежных средств[11] (ст. 159.6 УК РФ).

9. *Онлайновый фишинг* (англ. Phishing от fishing – рыбная ловля, выуживание), направленный на хищение денежных средств. Разновидность IT-мошенничества, подразумевающего под собой хищение денежных средств посредством использования злоумышленником разнообразных психологических методов и техник, направленных на обман пользователей с целью незаконного получения денежных средств[12].

Используя данный метод, мошенники от имени различных компаний осуществляют массовую рассылку электронных писем (например, по поручению какого-либо банка, организации и др.). Как правило, в письме содержится ссылка, перемещающая пользователя на фиктивный сайт организации, которая осуществляет продажу какого-либо товара с онлайн-оплатой.

На сегодняшний день поддельные веб-сайты стали лишь одним из направлений фишинга. Фиктивные банковские письма, полученные пользователями, могут сообщать о срочной необходимости позвонить по указанному номеру из-за возникших проблем с расчетным банковским счетом и др. Данная тактика называется голосовой фишинг (вишинг). Позвонив по указанному номеру, жертва получает конкретные инструкции и рекомендации по незамедлительной оплате для разблокировки карты, которые озвучивает автоответчик. Аналогичные преступления совершаются и посредством смс-фишинга[13].

10. *Тайпсквоттинг* (англ. Typosquatting ‘опечатка’) – разновидность кибersквоттинга (захват чего-либо с использованием доменных имен в киберпространстве[14]). Злоумышленники приобретают в личное пользование домены, регистрируют их, присваивая наименования известных брендов, совершив при этом умышленную опечатку: «Ростнефть.ру; Лугойл.com; rembler.ru» и т.д.

Как правило, мошенники используют их для построения прибыльного бизнеса (используют сайты в качестве рекламы, на которые можно отслеживать несколько тысяч просмотров; продают от имени официального представителя несуществующий товар). Как правило, опечатка влечет за собой угрозу потери идентификационных данных и денежных средств[15].

11. *Ноах-программы* (оболочка для управления базой данной). Цель данной программы заключается в навязывании пользователю персонального компьютера или смартфона (планшета) ложной истины о легко доступной возможности материального обогащения[16].

---

[10] Сбербанк России: Официальный сайт. URL: https://www.sberbank.ru/ru/person (дата обращения: 20.05.2021).

[11] Официальный сайт сетевой академии CISCO. URL https://www.netacad.com/country/russia (дата обращения: 01.02.2021).

[12] Сазонов М.М. Виды мошенничеств с банковскими картами и совершенствование мер виктимологического предупреждения // Виктимология. 2018. № 2 (16). С. 55-60.

[13] Воройский Ф.С. Информатика. Энциклопедический систематизированный словарь-справочник. М.: Физматлит, 2006. С. 432.

[14] Golinveaux J. What's in a domain name: Is cybersquatting trademark dilution // USFL Rev. 1998. Vol. 33. P. 641.

[15] Thangamuthu P. et al. Cybercrime // Encyclopedia of Criminal Activities and the Deep Web. IGI Global, 2020. P. 1-22.

[16] Мошенничество в Интернете / Государственный Департамент США. URL: http://www.infousa.ru/information/internet_fraud.htm (дата обращения: 25.09.2020).

К таким программам зачастую относят коммерческие утилиты, разработанные и внедренные в процесс виртуальной реальности. Подобные программы запускаются обычно только в пробной версии на небезопасных сайтах путем перехода по сомнительным веб-ссылкам. Установив программу, жертва обнаруживает всплывающее окно, где указывается наложенное ограничение из-за пользования пробной версией (бесплатной) программы и рекомендации по приобретению расширенного пакета «Премиум», позволяющего в будущем окупить свою стоимость и работать на индивидуальный баланс. После поступления денежных средств на расчетный счет злоумышленника происходит следующее: на электронный адрес жертвы приходит письмо, содержащее код активации полного пакета услуг. Ввод кода активации отключает программу, вызывая при этом полную перезагрузку системы. При повторном запуске файл не открывается, а система указывает на повреждение или некорректную работу. Также исход события может определяться получением на почтовый адрес письма о том, что лицо подверглось розыгрышу.

Данный перечень способов совершения мошенничеств не является исчерпывающим. Наряду с прогрессом в сфере IT-технологий, происходят изменения и в преступной среде, создаются новые схемы реализации противоправного умысла, что требует глубокого анализа и изучения данной проблематики.

Анализ устоявшихся воззрений отечественных и зарубежных криминологов на способ совершения кибермошенничества позволяет сделать выводы об отсутствии специальных знаний о способе совершения преступления, криминологической классификации мошеннических действий и наличии различий в понимания способа совершения мошенничества в криминологии, уголовном праве и криминалистике.

Для более детального отражения онлайн-действительности в сознании субъекта и снижения (недопущения) виктимизации личности, профилактики виктимного поведения, а также минимизации виртуальных рисков нами был проанализирован имеющийся и собранный материал, на основе которого была разработана универсальная типология кибермошеннических схем.

1. В зависимости от каналов коммуникации.

– *Профили пользователей чатов и социальных сетей («Вконтакте», «Одноклассники», «Инстаграмм» и т.д).* В последнее время участились случаи совершения мошеннических действий с использованием дублирования страниц социальных сетей. Как правило, объектами преступления становятся лица старшего поколения: от 45 лет[17]. Злоумышленник находит пользователя случайным образом, дублирует его имя, персональную информацию и фотографии к себе на страницу, после чего производит анализ списка друзей, добавляет их с фиктивной страницы, указывая на то, что от предыдущей страницы был забыт пароль и начинает вести диалог от имени настоящего владельца страницы. Обычно в письме содержится просьба оказать материальную помощь или предоставить краткосрочный займ путем денежного перевода.

– *Система мгновенных сообщений* используется фишерами либо киберсквоттерами для обращения к пользователям данных программ в форме предложения несуществующих товаров и услуг с обязательной предоплатой путем распространения мошеннического спама[18]. Зачастую мошенники преодолевают социальную дистанцию жертвы, притворяясь дальним родственником или бывшими коллегами.

– *Веб-сайты*. Мошенники приобретают домены и создают поддельные интернет-сайты, реализующие различную продукцию. Для того чтобы сайт набрал просмотры, они используют платную рекламу в виде всплывающих окон, а также блогерские услуги в «Инстаграмме», «Вконтакте», «Телеграмме». Аналогично предыдущему способу после получения предоплаты преступник перестает выходить на связь с жертвой.

2. По области воздействия.

– *Частная жизнь*. В данную типологию считаем рациональным относить мошенничества, направленные на экспансивный отклик пользователя – проведение благотворительных виртуальных акций, накрутка голосов рейтинга, просьба материальной помощи и т. д. Цель описанных действий заключается в психоэмоциональном давлении на чувства сострадания, сопереживания и милосердия жертвы. Наблюдается тенденция отправки онлайн-сообщений со сторонних аккаунтов (родственни-

[17] Ali M.A. et al. Consumer-facing technology fraud: Economics, attack methods and potential solutions // Future Generation Computer Systems. 2019. Vol. 100. P. 408-427.

[18] Marchal S. Et al. PhishScore: Hacking phishers' minds //10th International Conference on Network and Service Management (CNSM) and Workshop. IEEE, 2014. P. 46-54.

ков, друзей). Это позволяет привлечь внимание и увеличить желание оказать немедленную помощь. Главная задача киберпреступника – создать идеальный образ, чтобы «влюбить» в него жертву и получить максимальную финансовую помощь.

Для иллюстрации подобной ситуации приведем пример мошеннических действий в социальной сети «Instagram». «Доброго времени суток!!! Три месяца назад нам подкинули щенка. Он был изранен и окровавлен. Я еще учусь в школе и, к сожалению, не имею возможности зарабатывать деньги сам. Каждую неделю мне дают кое-какие деньги родители для школьного обеда и оплаты репетиторов. Вместо этого, я сводил щенка к ветеринару и купил дорогой корм для своего юного друга. С первых дней знакомства мы стали «не разлей вода». Случилась беда. У отчима на животное началась острая аллергия, в связи с чем, он начал избивать его и выгонять со двора. А сегодня сказал, что выгонит вовсе. Впрочем, еще он сказал, что если бы имел деньги на дорогую противоаллергенную прививку, цена которой 100 долларов, то позволил мне бы оставить собаку. Обращаюсь к вам, мои уважаемы подписчики! Помогите! Он такой ласковый и добрый! Не оставайтесь равнодушными! Перечисляйте деньги на виртуальный счет WMZ(Q)XXXXXXXX; или по номеру счета карты XXXXXXX»[19]

– *Область деловых отношений (профессиональная деятельность)*. В первую очередь, в данную область необходимо включить киберсквоттинг и тайпсквоттинг (стремление и желание жертвы приобрести необходимый домен, находящийся в собственности мошенников), а также совокупность существующих в природе мошеннических способов, связанных с извлечением финансовой прибыли[20].

3. По референтивным средствам. IT-мошенничество можно и необходимо классифицировать по референтивным средствам, которые были использованы при его оформлении. Иными словами, разделить на оптическое, контекстное и совокупное.

К оптическим средствам, по нашему мнению, будут относиться созданные мошеннические образы и стили (всплывающие окна в виде баннеров, анимаций, 3D картинок). Их используют при рассылке спам-сообщений, рекламных объявлений, продаже товаров и услуг.

Контекстные средства сопровождаются мошенническими действиями в тексте сообщений. Средой совершения таких действий зачастую выступают ICQ-чаты; социальные сети «Вконтакте», Facebook, «Мой мир» и др.; способом совершения – Hoax-программы, тайпсквоттинг, фишинг[21].

Например, «Добрый вечер! Полгода назад я начал использовать программное обеспечение для управления электронными кошельками WebMoney Transfer, а именно браузерное приложение WebMoney Keeper Standard. Вчера вечером на электронную почту я получил приватное сообщение от службы поддержки о намерении ликвидировать мой виртуальный банковский счет, так как последние два месяца он имеет нулевой остаток. В настоящее время я являюсь студентом и, возможно, уделяю меньше времени виртуальному заработку, чем это требует программа. Сегодня я осознаю, что мой веб-кипер закроют. Уважаемые друзья и коллеги! Прошу, увидев это сообщение, не оставаться равнодушными, а по возможности оказать поддержку в размере семи центов на веб-кошелек WMR (Y) XXXXXXX или по номеру банковского счета XXXXXXXX»[22].

И как следствие, совокупные средства включают в себя оптические образы и контекстные средства.

4. По степени психоэмоционального воздействия на жертву.

– *Убеждение*. Данное действие характеризуется как акт коммуникации, в ходе которого IT-мошенник, используя социальные сети или электронную почту, передает жертве значимую для нее социальную информацию и убеждает в ее достоверности. Убеждение основывается на принятии жертвой фиктивных сведений и идей как истинных.

– *Внушение*. Такой метод подразумевает оказание психологического воздействия на сознание пользователя персональным компьютером, ноутбуком, планшетом, смартфоном для того, чтобы вызвать некритическое восприятие в мышлении субъекта, после чего внушить неправомерную информацию и совершить хищение денежных средств.

---

[19] Данные, полученные в ходе изучения материалов уголовных дел, возбужденных и расследованных следственными подразделениями ОВД РФ в 9 субъектах РФ.

[20] Golinveaux J. What's in a domain name: Is cybersquatting trademark dilution // USFL Rev. 1998. Vol. 33. P. 641.

[21] Hayes D. et al. The war on fraud: Reducing cheating in the classroom // Journal of College Teaching & Learning (TLC). 2006. Vol. 3, no. 2.

[22] Данные, полученные в ходе изучения материалов уголовных дел, возбужденных и расследованных следственными подразделениями ОВД РФ в 9 субъектах РФ.

– *Мотивация*. Используя техники психологического воздействия, мошенники посредством виртуальной переписки с жертвой мотивируют ее под различными предлогами перевести денежную сумму.

Полагаем, что использование указанной классификации, а также наличие обособленного криминологического института способов мошенничества помогут избежать смешения и пересечения понятий, систематизировать данные, а также укрепить личную и имущественную безопасность.

Кроме того, обеспечить необходимый уровень безопасности возможно с помощью применения традиционных и криминологических способов противодействия.

К первым будут относиться:

– регулярное обновление программного обеспечения;

– использование брандмауэров и систем обнаружения вторжений и т. д.

Ко вторым:

– выявление, ослабление и нейтрализация причин IT-мошенничества;

– выявление мотивирующих факторов, побуждающих к совершению преступления;

– установление лиц, обладающих повышенным криминальным риском;

– оказание воздействия с целью снижения установленного риска;

– установление лиц по психологическим факторам, указывающим на их способность совершать преступления, и соответствующее корректирующее воздействие на них[23].

Поступила в редакцию 11.10.2021

Старостенко Олег Александрович, адъюнкт кафедры уголовного права и криминологии
Краснодарский университет МВД России
350005, Россия, г. Краснодар, ул. Ярославская, 128
E-mail: olegstaros94@gmail.com

O.A. Starostenko

ANALYSIS OF IT FRAUD SCHEMES: CLASSIFICATION AND COUNTERACTION

DOI: 10.35634/2412-9593-2021-31-6-1072-1077

The article analyzes common criminal IT fraud schemes, examines the dynamics of cyber fraudulent actions on the territory of Russia for the period 2019–2020. It was revealed that the most important element of the mechanism of the criminal behavior of a cyber fraudster is the method of committing a crime. An empirical analysis of the views of criminologists on the way IT fraud is committed made it possible to single out its three main properties (actions must be performed in the course of a criminal act; actions are aimed at achieving a criminal result; actions reflect the individual characteristics of a crime). The analysis of criminal schemes made it possible to systematize the data, develop the author's criteria for their classification (depending on the communication channels; by the area of influence; by referential means; by the degree of psychoemotional impact on the victim), as well as traditional and criminological methods of countering IT fraud that can help the user avoid confusion and intersection of concepts, organize data, strengthen personal and property security in cyberspace.

Keywords: IT fraud, criminal scheme, method, security, victim, Internet, intruder, mechanism of behavior.

Received 11.10.2021

Starostenko O.A., adjunct of the Department of Criminal Law and criminology
Krasnodar University of the Ministry of Internal Affairs of Russia
Yaroslavskaya st., 128, Krasnodar, Russia, 350005
E-mail: olegstaros94@gmail.com

[23] Старостенко О.А., Старостенко Н.И. Система криминологических и правовых мер противодействия мошенничеству в сети интернет // Проблемы правовой и технической защиты информации. 2020. № 8. С. 111-113.