УДК 349

О.А. Старостенко

ПРИРОДА И СПОСОБЫ СОВЕРШЕНИЯ МОШЕННИЧЕСТВА С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Статья посвящена рассмотрению вопросов, касающихся природы и способов совершения мошенничества с использованием информационно-телекоммуникационных технологий. В статье рассматривается и анализируется официальная статистика преступлений в глобальной сети Интернет за 2019 г., а также причиненный данными преступлениями материальный ущерб. Раскрыто понятие способа мошенничества и определена его важнейшая роль в характеристики интернет-мошенничества. Особое внимание обращается на наиболее популярные способы совершения рассматриваемого преступления, такие как фишинг, нигерийские письма, создание личного бизнеса, интернет-магазины, магические кошельки, свободная связь, усовершенствованная МММ, указываются их характерные признаки и выделяются перспективные направления изучения вышеуказанной темы. С целью систематизации данных автором предлагается разделение рассматриваемых способов на группы. Также в статье проанализированы новые, в полном объеме еще не изученные способы мошеннических действий в сети Интернет, и предложены защитные меры в целях предотвращения угрозы информационно-телекоммуникацинного мошенничества.

Ключевые слова: способы мошенничества, компьютеризация, жертва, злоумышленники, метод, криминология, характеристика, структура.

DOI: 10.35634/2412-9593-2020-30-4-576-582

Поступательное движение науки на основе широкого познания и освоения внешних сил является результатом научно-технического прогресса, негативным последствием которого выступает возникновение киберпреступности. Наиболее часто совершаемым преступлением в сети Интернет является мошенничество. Об этом свидетельствуют многочисленные исследования ученых и официальная статистика[1].

Президент Российской Федерации 28 февраля 2019 года утвердил перечень поручений по вопросам реализации национальной программы «Цифровая экономика Российской Федерации»: «По обеспечению ограничения доступа к информации, распространение которой в Российской Федерации запрещено, и к информации, наносящей вред, содержащейся в сети интернет[2]; по мониторингу и обеспечению безопасности при подключении и предоставлении доступа к государственным, муниципальным, иным информационным системам и к сети Интернет»[3].

Из перечня поручений следует сделать вывод, что интернет прочно обосновался в нашей жизни. На сегодняшний день это не только среда для социального общения и поиска различной информации, но и комфортное место для совершения различных преступлений. Как отмечает А.Л. Осипенко, «становление новых социальных отношений и форм собственности в информационной сфере, тесно связанное с развитием глобальных компьютерных сетей, оказывает все более ощутимое влияние на большинство важных процессов функционирования современного общества. Сетевые информационные технологии создают предпосылки как для существенного изменения способов совершения ”традиционных” преступлений, так и для появления новых видов преступной деятельности» [1].

На фоне новейших достижений в глобальной сети Интернет происходит интеллектуализация и трансформация экономической преступности. Интернет становится не только местом получения информации, но и средством незаконного проникновения в частные (приватные) данные физических и юридических лиц с целью незаконного обогащения. Усовершенствуются формы и методы соверше-

[1] Официальный сайт МВД России. [Электронный ресурс] URL: https://мвд.рф/reports/item/19007735/ (дата обращения: 25.01.2020 г.)

[2] Перечень поручений по вопросам реализации национальной программы «Цифровая экономика Российской Федерации», 28 февраля 2019 года, 10:05. Пр-300, п.1 г). [Электронный ресурс]. URL: http://kremlin.ru (дата обращения: 29.01.2020)

[3] Перечень поручений по вопросам реализации национальной программы «Цифровая экономика Российской Федерации», 28 февраля 2019 года, 10:05. Пр-300, п.1 д). [Электронный ресурс]. URL: http://kremlin.ru (дата обращения: 29.01.2020)

ния указанных деяний, увеличивается сумма ущерба. Из вышеуказанного следует, что интернет-мошенничество необходимо рассматривать как глобальную и общемировую проблему.

За период с января по декабрь 2019 года зарегистрировано 294,4 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий, что на 68,5 % больше, чем за аналогичный период прошлого года. Материальный ущерб от указанных преступлений (по оконченным и приостановленным уголовным делам) составил 447,2 млрд руб. [2] Учитывая латентный характер данного вида преступности, можно предположить, что реальное количество преступлений намного больше.

Мошенничество в глобальной сети Интернет характеризуется совокупностью преступлений, совершаемых с использованием информационных технологий с целью обмана человека или группы лиц, а также мотивацией преступной деятельности и использованием новейших, еще не изученных способов совершения указанных деяний.

Согласно Толковому словарю русского языка С.И. Ожегова, «способ» понимают как действие или систему действий, которые применяются при выполнении какой-либо работы или при осуществлении чего-либо [3]. В криминологии под способом понимается выяснение криминологической характеристики преступлений, анализ состояния и динамики отдельных категорий преступлений, установление их причин и условий, а также разработка мер предупреждения преступлений [4]. Из данного определения следует сделать вывод о том, что важнейшим элементом характеристики интернет-мошенничеств выступает способ их совершений. Специфика мошенничества, совершаемого с использованием информационно-телекоммуникационных технологий, заключается в способе его совершения ввиду того, что, в отличие от других преступлений, способ действий преступника носит информационный характер, строится на особых доверительных отношениях между жертвой и виновным.

Исходя из анализа эмпирического материала можно выделить несколько способов совершения мошенничества в сети Интернет.

1. *Фишинг*. Разновидность интернет-мошенничества, цель которого заключается в получении доступа к конфиденциальной информации, принадлежащей компьютерным пользователям – учетным записям, паролям и логинам [5]. Используя данный метод, мошенники от имени популярных брендов, производят массовую рассылку электронных писем, например, от имени какого-либо банка, организации и др. Как правило, письмо подтверждается ссылкой, перейдя на которую, пользователь переходит на страницу данной организации, внешне схожей с настоящей. Попавшись в сети злоумышленников, пользователь сети Интернет начинает подвергаться различным психологическим приемам и методам, цель которых очевидна – получение логина и пароля от учетной записи на сайте и дальнейшее их использование для доступа к банковским счетам, киви кошелькам, электронным деньгам, мобильным счетам и др.

Для борьбы с преступлением производители многих веб-обозревателей совокупными усилиями внедрили специальные способы информирования своих посетителей – «Антифишинг». При открытии лицом подозрительной ссылки происходит информирование клиента и дается рекомендация срочно покинуть сомнительный сайт. Также в указанных целях применяются усложненные процедуры авторизации, мониторинг, различные спам-фильтры.

На сегодняшний день поддельные веб-сайты стали лишь одним из направлений фишинга. Фальшивые банковские письма, полученные пользователями, могут сообщать о срочной необходимости позвонить по указанному номеру ввиду возникших проблем с расчетным банковским счетом. Данная тактика называется голосовой фишинг. Позвонив по указанному номеру, жертва мошенничества получает конкретные инструкции и рекомендации по вводу номера своего счета и пароля, которые озвучивает автоответчик. Аналогичные преступления совершаются и посредством смс-фишинга.

2. *«Казино»*. Жертва данного вида мошенничества получает электронное письмо, которое содержит уникальный код или кодовое слово, вводя которое получит беспроигрышную комбинацию и пополнение баланса на довольно внушительную сумму. Как правило, обещанные деньги появляются, но с ними невозможно производить никаких финансовых операций, а секретный код является недействительным. Обычно сами онлайн-казино и выступают создателями и отправителями данных писем в целях расширения клиентской базы и, соответственно, увеличения своего заработка.

3. *Создание личного бизнеса*. Способ интернет-мошенничества, который основывается на секретной стратегии (методике), приносящий огромный доход и окупающий свою стоимость примерно в течение 6-10 месяцев (в зависимости от обозначенной продавцом стоимости бизнеса). Злоумышлен-

ники также обещают сопровождение и помощь при ведении бизнес-проекта, но после продажи пропадают, а конфиденциальная инструкция зачастую включает в себя информацию об организации бизнеса аналогично схеме, реализуемой преступниками.

Набирает активные обороты «заработок на дому» за набор текста. Будущей жертве предлагается набрать небольшой текст в качестве тестового задания за небольшую плату. Успешно справившись с поставленной задачей, соискатель получает даже небольшое материальное вознаграждение за свой труд. После этого предлагается перевести некоторую сумму на счет издательства онлайн-фирмы для того, чтобы повысить свой статус и получить прибавку к зарплате.

4. *Нигерийские письма*. Весьма распространенный способ мошенничества, основывающийся на массовой рассылке спам-сообщений. Название данный способ получил вследствие распространения в Нигерии таких писем по обычной почте задолго до появления Интернета. Обычно мошенники просят у получателей писем поддержки и помощи во многомиллиардных денежных операциях, обещая немалые проценты с совершенной сделки. При положительном согласии «партнера по бизнесу», злоумышленники постепенно выманивают внушительные суммы денежных средств, обосновывая их необходимостью уплаты сборов и налогов, дачи взяток чиновникам, оформления свидетельств и сделок. Нередко в ходе незаконного получения денежных средств мошенники используют психологическое давление и уверяют в том, что нигерийская сторона для уплаты сборов заложила дом, продала все свое личное имущество, ручную кладь. Естественно, «заработанных процентов» жертва никогда не получит, их просто не существует. И хотя данный способ мошенничества существует много лет, массовость рассылки приводит к появлению все новых жертв. Нигерийские письма часто приходят и из других африканских стран, рассылка спам-сообщений началась в середине 1980-х гг. Приведем некоторые примеры содержания указанных писем:

– письмо об имеющейся вакансии за рубежом по вашей специальности, но имеется необходимость перед выездом оплатить проживание и билеты за перелет;

– жертва получает письмо от адвоката убитой сестры, в котором отражена информация о гибели родственника в авиакатастрофе и необходимости срочно получить наследство в денежном эквиваленте. Для этого мошенники требую указать номер банковского счета и реквизиты, с которых благополучно списывают все имеющиеся средства;

– письмо о лотерейном выигрыше по номеру сотового телефона, который был выбран мобильным оператором случайным образом. Для получения выигрыша просят оплатить налог на прибыль.

– пожертвование денег несуществующей церкви;

– социальные сети и сайты знакомств;

– доски электронных объявлений, интернет – аукционы;

5. *Интернет-магазины*. Товар продается либо с огромной скидкой, либо уцененный. Как правило, мошенники требуют стопроцентную предоплату. Заказав товар, жертва либо не получает его вовсе, либо забирает на почте пустую посылку.

6. *Мошенничество с использованием телекоммуникационных технологий*. Жертву убеждают отправить СМС на указанный номер в целях разблокировки учетной записи, после чего автоматически на телефоне подключается платная ежедневная подписка.

7. *«Магические кошельки»*. Злоумышленники убеждают, что обнаружили «магический кошелек», перечисляя на который деньги, возвращаешь обратно в увеличенном размере. Цель данных действий очевидна: внушить доверие, вернув первоначальные взносы с обещанными процентами, вводя жертву в некий азарт от полученного заработка, намекая на более крупную сумму ставки и, соответственно, выигрыша и выманить так называемую магическую сумму.

В настоящее время прогрессирует мошенничество, суть которого заключается в предложении возмещения переводов со счетов безналичных банковских карт. Для обмана потенциальной жертвы мошенники используют всемирно известный бренд «Сбербанк», который, как правило, пользуется у населения доверием.

8. *«Свободная связь»*. Жертве предлагается за небольшое вознаграждение скачать специализированную программу, которая позволит звонить на любые абонентские номера, совершать рассылку сообщений и пользоваться мобильным интернетом совершенно бесплатно. После полной оплаты жертва становится счастливым обладателем программы-пустышки.

9. *Усовершенствованная МММ*. Идея мошенничества основана на классической финансовой пирамиде. Основатели и представители маркета привлекают клиентов необыкновенно мизерной це-

ной на новые модели iPhone, 50–60 тыс. руб. – рыночная стоимость, 28–38 тыс. руб. – предполагаемая цена. Ошеломленные покупатели с огромным удовольствием соглашаются на предложенные условия. Условия мошенников традиционные: стопроцентная предоплата и реклама в кругу друзей и близких. Далее самые первые покупатели получают свои смартфоны, а вновь прибывающие клиенты продолжают жить мечтой.

10. *«Осторожно, лотерея!»*. Клиент невнимательно читает договор, который подписывает с фальшивой брокерской компанией. Когда жертва пытается получить свои деньги, компания отказывает, ссылаясь на договор, где указано, что клиент участвовал в лотерее, исход которой определяется удачей.

Процесс глобальной компьютеризации населения влечет за собой изменения структуры преступности, техник и методик совершения преступлений, на смену существующим приходят новые, в полном объеме не изученные способы:

1. *Шпионское ПО.* Угроза связана со сбором сведений о пользователях, которые в дальнейшем используются в мошеннических целях. Источниками таких угроз являются отслеживание файлов cookie, рекламное ПО и всплывающие окна. Не приводя к непосредственным сбоям в работе компьютера, они вторгаются в личные данные пользователя и получают неправомерный доступ к информации. К шпионскому ПО относятся программы, собирающие личные данные с компьютера пользователя без его разрешения. В числе этих данных могут оказаться пароли и банковские реквизиты. Шпионское ПО обычно устанавливается незаметно для пользователя при загрузке файла, установке другой программы или щелчке мышью во всплывающем окне. Одним из видов шпионского ПО считаются файлы cookie. Они фиксируют информацию о посещении сайтов определенным пользователем Интернета и могут быть полезны для персонализации настроек. Многие веб-сайты, в том числе и сомнительные, при подключении пользователя требуют, чтобы файлы cookie были разрешены. Таким образом, мошенники создают уникальный программный код по внедрению на компьютеры пользователей cookie-файлов третьих сторон. Подмена cookie позволяет преступникам незаконно получать, например, партнерские отчисления или проценты за посредничество, если пользователь совершит покупку в интернет-магазине.

Рекламное ПО – вид шпионского ПО для сбора сведений о пользователях, посещающих вебсайты. Собранные сведения в дальнейшем используются в мошеннических целях. Часто рекламное ПО попадает к пользователю вместе с «бесплатным» продуктом. Когда пользователь открывает окно браузера, рекламное ПО может запускать новые экземпляры браузера с рекламой товаров и услуг, отражающей интересы пользователя в Интернете.

2. *Ботнеты и зомби*. Рост значимости электронных коммуникаций сопровождается еще одним досаждающим явлением – несанкционированными массовыми рассылками по электронной почте. В некоторых случаях продавцы намеренно не прибегают к целевому маркетингу и стараются разослать рекламу товара или услуги по электронной почте максимальному числу получателей в расчете на то, что заинтересованный покупатель «несуществующего» товара обязательно найдется. Этот широко распространенный подход к мошенничеству в Интернете получил название спама. Один из основных путей распространения спама – использование ботнета или бота.

«Бот» – производное от слова «робот», которое описывает поведение зараженных устройств. Вредоносное ПО бота заражает хост обычно через электронное сообщение или ссылку на вебстраницу путем загрузки и установки средства дистанционного управления. Зараженный компьютер-зомби связывается с серверами, которыми управляет создатель ботнета. Эти серверы играют роль центра управления и контроля для всей сети взломанных устройств (ботнета). Зараженные компьютеры часто могут передавать ПО на другие незащищенные устройства в сети, что приводит к негативным последствиям и риску получения приватных данных.

3. *Вредоносные программы* (вирусы, интернет-черви, трояны). Для реализации преступного умысла в первую очередь необходима активация вируса, после чего начинается его распространение и размножение. Вирусы имеют предрасположенность к заполнению свободной памяти персонального компьютера, остановке работы windows, обеспечению доступа к конфиденциальным данным жертвы.

Основным источником распространения вирусов является электронная почта, социальные сети, загружаемые файлы, USB устройства, компакт-диски.

Интернет-черви идентичны вирусам. Особенность заключается в том, что внедряться в существующую программу им не требуется.

Интернет-червь рассылает копии самого себя по сети на все подключенные хосты. Интернет-черви могут функционировать независимо и интенсивно распространяться. Для их работы не требуется активация. Ущерб от саморазмножающихся сетевых интернет-червей может в несколько раз превышать последствия вируса.

Троян – программа, которая имитирует законную программу, но на самом деле служит инструментом атаки. Он не может самореплицироваться. Успешное выполнение трояна зависит от успешности его маскировки под программу, которую пользователь согласится запустить. Некоторые «троянские кони» также открывают «черный ход» в систему для мошенника.

Мошенники также могут получить доступ в сеть, эксплуатируя уязвимости в ПО, атакуя оборудование или даже используя такие изящные приемы, как угадывание чужого имени пользователя и пароля.

Мошенник, получивший доступ в сеть, становится источником четырех видов угроз:

– хищение информации;

– хищение персональных данных;

– хищение денежных средств.

4. *Злоупотребление доверием пользователей*. В настоящее время чаще всего с целью получения информации непосредственно у авторизованных пользователей мошенники применяют метод претекстинга. Данный способ характеризуется использованием вымышленного предлога, побуждающего жертву разгласить информацию или выполнить определенное действие. Контакт с жертвой обычно осуществляется посредством телекоммуникационной связи. Данный прием эффективен в том случае, если злоумышленнику удается завладеть доверием своей цели, или жертвы. Злоумышленник во многих случаях изначально должен располагать некоторыми знаниями или наблюдениями. Например, если ему известен номер счета жертвы, он сможет воспользоваться этой информацией для вхождения в доверие к жертве. После этого выудить дополнительную информацию будет проще.

Как известно, в науке криминологии нет четкого разделения способов совершения компьютерного мошенничества на группы по схожим признакам, что приводит к смешению и пересечению понятий. С целью систематизации данных, вполне обоснованно классифицировать указанные способы компьютерных мошенничеств следующим образом:

– способы, основанные на внедрении и использовании электронной коммерции. Примером выступает развитие интернет-торговли; сферы представления онлайн-услуг, интернет-банков и др.;

– традиционно используемые способы мошенничества, перешедшие в виртуальную реальность (заключение ложных договоров в интернет-пространстве; подписание контрактов; оказание коммерческих услуг и т.д.);

– способы организации онлайн-азарта (коммерческие и азартные игры на деньги);

– заведомо ложная интернет-реклама (основана на спаме и предложении несуществующих услуг по выгодным ценам);

– онлайн-аукционные способы мошенничества (покупка автомобилей за границей, одежды, бытовой техники);

– сигнатурные способы (вредоносное программное обеспечение).

На основе изученных теоретических данных необходимо сделать вывод о том, что, приняв защитные меры, можно избежать угрозы информационно-телекоммуникационного мошенничества. Для обеспечения безопасности возможно применять как простые, недорогие способы, например, регулярное обновление ПО, так и сложные реализации брандмауэров и систем обнаружения вторжений. Некоторые из наиболее эффективных процедур защиты просты в реализации и не требуют обширных технических знаний. Имя пользователя и пароль – два элемента информации, которые необходимы пользователю для входа в компьютер или приложение. Если злоумышленнику известен один из этих элементов, ему необходимо только взломать или узнать другой элемент для получения доступа к компьютерной системе. Важно менять имена пользователей по умолчанию для таких учетных записей, как администратор и гость, поскольку эти имена пользователей по умолчанию широко известны. Большинство пользователей выбирают пароли, которые можно легко угадать или получить на основе известной информации о пользователе, такой как день рождения, имя домашнего питомца или любимая спортивная команда. Важно относиться к паролям как к ключу доступа к ценным данным и создавать их максимально надежными.

Безопасность информационных технологий волнует пользователей по всему миру. Для того чтобы не стать жертвой мошенников, необходимо укреплять личную и имущественную безопасность следующими способами:

1. *Исправления и обновления ПО*. Одним из распространенных способов, к которому прибегает злоумышленник для получения доступа к хостам и сетям, являются уязвимости в ПО. Важно использовать актуальные версии ПО, устанавливая текущие исправления для укрепления безопасности и обновления для нейтрализации угроз. Исправление – небольшой фрагмент кода, устраняющий определенную проблему. Обновление, в свою очередь, может не только содержать исправления ряда проблем, но и расширять программный пакет дополнительными функциональными возможностями. Поставщики ОС (Linux, Windows и т. п.) и приложений постоянно выпускают обновления и исправления, устраняющие известные уязвимости ПО. Кроме того, поставщики часто выпускают так называемые пакеты обновлений — сборники исправлений и обновлений. Для удобства во многих операционных системах предусмотрена функция автоматического обновления с загрузкой обновлений ОС и приложений и установкой их на хост.

2. *Антивирусная защита*. Антивирусное ПО может использоваться как для профилактики, так и для реагирования. Оно предотвращает заражение, а также обнаруживает и удаляет вирусы, интернет-черви и трояны. Антивирусное ПО должно быть установлено на всех компьютерах, подключенных к сети. Для обнаружения новых вирусов и предотвращения заражения компьютера антивирусное ПО использует известные сигнатуры вирусов. Сигнатуры вирусов — это шаблоны в программах, характерные для других вредоносных программ, которые уже были признаны опасными. При обнаружении новых вирусов в Интернете файлы сигнатур для антивирусного ПО соответствующим образом обновляются. Чтобы защитить систему от заражения, важно регулярно обновлять программу проверки на вирусы с учетом последних сигнатур.

3. *Защита от шпионского ПО*. Спам ведет к перегрузкам серверов электронной почты, может являться носителем вирусов и создает другие угрозы безопасности. Кроме того, распространители спама могут вставлять в сообщения ссылки, чтобы внедрить код, используя вирус или троян, и захватить управление хостом с целью хищения денежных средств.

4. *Средства блокирования спама*. Антиспам защищает хосты, выявляя спам и принимая нужные меры, например помещая такие сообщения в папку нежелательной почты или удаляя их. Спам-фильтры можно загрузить на отдельные пользовательские устройства, а также на серверы электронной почты. Кроме того, многие интернет-провайдеры предлагают услуги фильтрации спама. ПО для защиты от спама не способно распознать все виды спама, поэтому открывать поступившие сообщения следует осторожно. Другой недостаток состоит в том, что легитимные сообщения могут быть отнесены к спаму и обработаны соответствующим образом.

5. *Брандмауэры*. Одно из наиболее эффективных средств безопасности для защиты пользователей сети от внешних угроз. Брандмауэр обычно устанавливается между двумя или более сетями и контролирует трафик между ними, а также помогает предотвратить несанкционированный доступ. В брандмауэрах используются различные методы для определения разрешения или запрета доступа к сети.

Подводя итог вышесказанному, еще раз отметим, что проводные и беспроводные компьютерные сети играют важнейшую роль в повседневной жизни. Безопасность индивидуальных пользователей и организаций в равной мере зависят от надежной работы компьютеров и сетей в таких задачах, как электронная почта, учет, организационное управление и работа с файлами. Несанкционированное вторжение в сеть может иметь разрушительные последствия, сопровождающиеся потерей денежных средств и хищением важной информации. Рассматриваемый перечень интернет-мошенничеств не является исчерпывающим. Информационно-телекоммуникационные технологии постоянно прогрессируют, а вместе с ними и преступления в данной сфере, что и определяет острую необходимость изучения рассматриваемой темы.

СПИСОК ЛИТЕРАТУРЫ

1. Осипенко А. Л. Борьба с преступностью в глобальных компьютерных сетях: Международный опыт: монография. М.: Норма, 2004. 432 с.
2. Министерство внутренних дел Российской Федерации ФКУ «Главный информационно-аналитический центр». Состояние преступности в России за январь-декабрь 2019 года. С. 4.

3. Ожегов С.И. Толковый словарь русского языка: около 100 000 слов, терминов и фразеологических выражений / под ред. Л. И. Скворцова. 26-е изд., испр. и доп. М.: Оникс [и др.], 2009.
4. Даньшина И.М. Криминология. Харьков, 2003. 352 с.
5. Сазонова М.М. Виды мошенничеств с банковскими картами и совершенствование мер виктимологического предупреждения // Виктимология. 2018. № 2 (16). С. 55-60.

Поступила в редакцию 12.05.2020

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

NATURE AND METHODS OF COMMITTING FRAUD USING INFORMATION-TELECOMMUNICATION TECHNOLOGIES

DOI: 10.35634/2412-9593-2020-30-4-576-582

The article is devoted to the consideration of issues relating to the nature and methods of committing fraud using information and telecommunication technologies. The article considers and analyzes official statistics of crimes on the global Internet for 2019, as well as material damage caused by these crimes. The concept of a method of fraud is disclosed and its most important role in the characteristics of Internet fraud is determined. Particular attention is paid to the most popular methods of committing the crime in question, such as: phishing, Nigerian letters, creating a personal business, online stores, magic wallets, free communication, improved MMM; their characteristic features are indicated and promising areas for studying the above topic are highlighted. In order to systematize the data, the author proposes the division of the considered methods into groups. The article also analyzes new, not yet fully explored, methods of fraudulent activity on the Internet, and offers protective measures to prevent the threat of information and telecommunication fraud.

Keywords: ways of fraud; computerization; victim; attackers; method; criminology; characteristic, structure.

Received 12.05.2020

Starostenko O.A., Adjunct at 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