

СТРАУНИНГ ЮЛИЯ АНАТОЛЬЕВНА

Московский университет МВД России имени В.Я. Кикотя
(Москва, Россия)

sohmet07@mail.ru

ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ МОШЕННИЧЕСТВУ, СОВЕРШАЕМОМУ С ИСПОЛЬЗОВАНИЕМ МОБИЛЬНОЙ СВЯЗИ

Аннотация. В статье отмечается, что мошенничество стало иметь ряд новых криминологически значимых отличий от предыдущего периода. Существенно возросли как ущерб, причиняемый данным видом преступления, так и профессионализация преступников в данной сфере. Мошенничество стало приобретать форму организованной преступности. Появились новые способы совершения преступления. Авторы статьи отмечают, что современные технологии способствуют развитию данной тенденции, что приносит государству и обществу несоизмеримый ущерб, и предлагают ряд мер, которые будут способствовать противодействию мошенничеству посредством использования мобильной связи.

Ключевые словосочетания: мошенничество с использованием мобильной связи, детерминанты мошенничества, личность мошенника, предупреждение мошенничества

Для цитирования: Страунинг Ю.А. Проблемы противодействия мошенничеству, совершаемому с использованием мобильной связи // Вестник ВИПК МВД России. – 2023. – № 3(67). – С. 152-156; doi: 10.29039/2312-7937-2023-3-152-156.

STRAUNING JULIA A.

Moscow University of the Ministry of Internal Affairs of Russia named after V.Ya. Kikot
(Moscow, Russia)

PROBLEMS OF COUNTERING FRAUD COMMITTED USING MOBILE COMMUNICATIONS

Annotation. The article says that fraud has begun to have a number of new criminologically significant differences from the previous period. The damage caused by this type of crime has significantly increased, the professionalization of criminals in this area has increased. In addition, fraud began to take the form of organized crime. New ways of committing a crime have appeared. The authors of the article note that modern technologies contribute to the development of this trend, which brings incommensurable damage to the state and society and propose a number of measures that will contribute to countering fraud by means of using mobile communications.

Key words and word combinations: fraud using mobile communications, determinants of fraud, identity of the fraudster, fraud prevention

For citation: Strauning Ju. A. Problems of countering fraud committed using mobile communications // Vestnik Advanced Training Institute of the MIA of Russia. – 2023. – № 3(67). – P. 152-156; doi: 10.29039/2312-7937-2023-3-152-156.

Современное мошенничество в новых реалиях развивается огромными темпами. Сегодня можно утверждать, что мошенничество стало иметь ряд новых криминологически значимых отличий от предыдущего периода. Существенно возросли ущерб, причиняемый данным видом преступления, профессионализация преступников в данной сфере, которая влечет за

собой латентность преступников и привлечение новых лиц для реализации своих преступных замыслов. Помимо этого, мошенничество стало приобретать форму организованной преступности. Появились новые способы совершения преступления. Современные технологии способствуют развитию данной тенденции, что приносит государству и обществу несоизмеримый ущерб.

Преступники стали использовать различные способы манипуляций с людьми. Они теперь работают бесконтактно, через информационно-коммуникативные технологии (Интернет, мобильная связь и другие производные [1, с. 3], способствующие реализации преступной деятельности).

В наше время человек без мобильного телефона не может существовать, настолько он сейчас необходим, что прошлые методы связи с людьми попросту устарели и не могут быть реализованы. И это как раз играет на руку современным преступникам.

В таких условиях привлечь к уголовной ответственности лиц, совершающих данные противоправные деяния, становится невозможно. Это обусловлено значительным уровнем латентности преступников. Дело в том, что преступники могут находиться на территории РФ и вне её. Возросший уровень подготовки и образования мошенников позволяет им использовать сложные схемы для реализации своей деятельности. Этому способствуют современные технологии [2].

Согласно статистическим данным за период с января по декабрь 2018 года выявлено 215 тыс. фактов мошенничества, из них совершено с использованием мобильной связи 101,8 тыс. преступлений, в 2019 году зарегистрировано 257,2 тыс. мошенничеств, из них совершено посредством мобильной связи 121,8 тыс., в 2020 году выявлено 335,6 тыс. фактов мошенничества, из них совершено с использованием мобильной связи 160,8 тыс. преступлений, в 2021 году – 339,6 тыс. подобных преступлений, из них 164,4 тыс. – посредством мобильной связи [3]. На основании полученных данных мы можем сделать вывод о том, что фактов мошенничества с использованием мобильной связи с каждым годом становится больше.

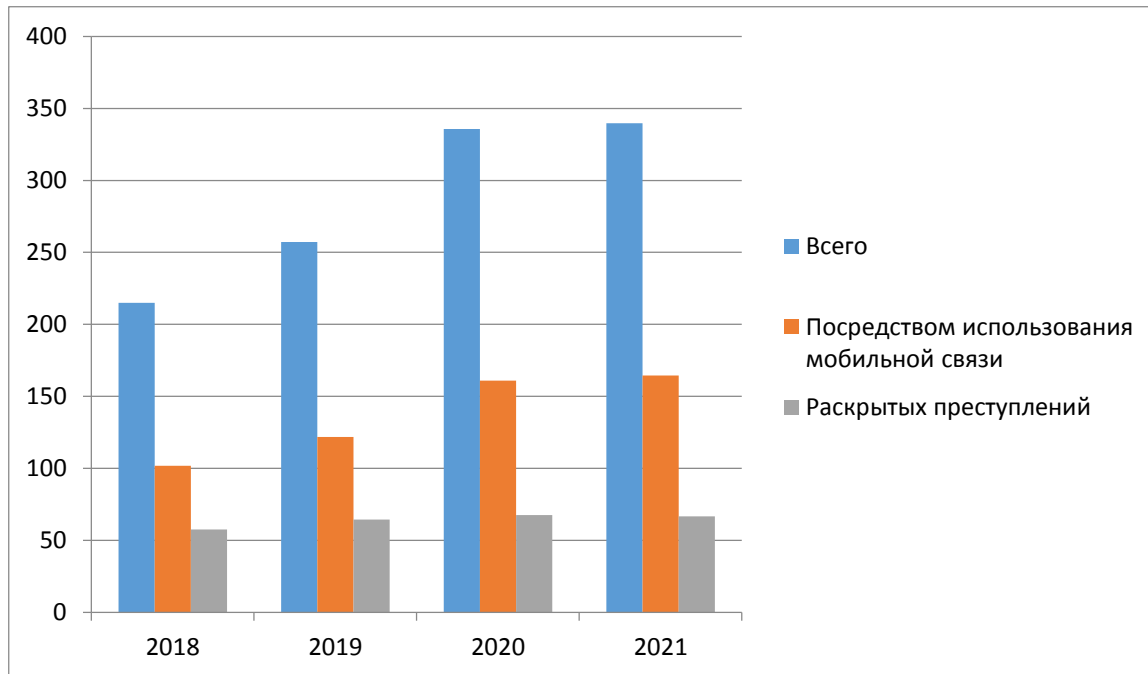


Рис. 1. Количество зарегистрированных мошенничеств в период с 2018 по 2021 год

Для того чтобы понять мошенничество, нужно изучить психологию мошенника. Как правило, эти люди являются отличными психологами, характеризуются отличительными способностями, которые позволяют им приобрести доверие у своего собеседника. Они обладают узким профилем знаний в той сфере, в которой они производят свой преступный

замысел, достаточными знаниями в правовой сфере и имеют представления о финансовой системе и потребительском рынке [4, с. 82-83].

Из ряда характерных черт важной особенностью мошенника является его многогранность. Из всех видов преступлений на данный тип преступления не оказывает влияния физиологическое состояние лица.

Говоря о возрасте преступников, следует отметить, что средний возраст мошенников колеблется от 25-40 лет. Как правило, у данной категории лиц присутствуют определенные мотивы (корыстность и недостаточный уровень материального обеспечения).

Кроме того, важным криминологическим признаком является социально-демографический, к нему относится пол. Согласно статистике в данном виде преступления преобладают мужчины, в процентном соотношении 77% на 23% среди женщин [5].

Отличием мошенника мужчины от женщины является его эмоциональная устойчивость, что как раз и влияет на преступную активность данных лиц. Наибольшая стрессоустойчивость способствует получению положительного результата при общении с потерпевшим.

Мошенники имеют устойчивую профессиональную ориентацию, по истечении времени преступники привыкают к данному роду деятельности, она становится для них работой.

Исходя из анализа криминологических особенностей современного мошенника, можно выделить следующие типы:

1. *Профессиональный тип* – характеризуется наличием у мошенника особых знаний в той или иной сфере (банковской, юридической). Особенность этого типа заключается в умении введения потерпевшего в заблуждение посредством предоставления ложной информации, не соответствующей действительности (например, мошенник представляется как сотрудник службы безопасности банка, заранее зная его личные данные, ведет с потерпевшим культурное общение, используя различные термины, присущие данной сфере).

2. *Привычный тип* отличается от профессионального по манерам общения и своему уровню образования, имеет меньшую моральную устойчивость, в психологическом плане, как правило, неустойчив. Примером может служить представление мошенника сотрудником коллекторского агентства с целью «выбить» из жертвы денежные средства различными способами.

3. *Случайный тип*, в отличие от выше приведенных типов, характеризуется ситуативностью, т.е. как получится завести разговор с потерпевшим, так и будет складываться общая обстановка для мошенника.

Мошенники – хорошие психологи, их задача – заставить человека добровольно отдать свои денежные средства. Как правило, они не работают в одиночку, это в основном группа лиц или организованная группа. Для того чтобы человек отдал свои деньги сам, преступники используют несколько способов:

1. Списание денежных средств происходит со счета владельца самим мошенником.
2. Человек сам производит денежный перевод на счет или номер мошенника.

Проблемы выявления мошенников связаны как раз с использованием ими VPN-подключения и сквозного шифрования [6]. Анонимизация с помощью VPN достигается благодаря созданию подключения к удаленному серверу с использованием шифрования. Сетевой трафик, проходя через удаленный сервер, маскируется под трафик, исходящий из данного сервера. Таким образом происходит подмена IP-адреса и шифрование данных, которые передаются по подключению. Удаленный сервер, как правило, находится за рубежом, что является проблемой выявления настоящего IP-адреса, с которого производится тот или иной звонок.

Сквозное шифрование представляет собой технологию шифрования телефонного звонка или сообщения, при которой исходное сообщение шифруется на устройстве отправителя и расшифровывается на устройстве получателя. Проблема выявления преступников заключается в крайне высокой сложности дешифровки содержания звонка или сообщения, если сотрудники не имеют доступа к одному из аккаунтов собеседников или ключа дешифровки. В данной ситуации правоохранители могут знать собеседников, но не могут знать содержания их разговора.

Также довольно частым способом сокрытия личности при совершении телефонного звонка является подмена номера телефона. Компании, получив лицензии на использование интернет-телефонии SIP, могут создать сервисы по предоставлению доступа к ней. Особенностью данного вида телефонии является возможность изменения номера телефона

во время совершения вызова на любой не занятый другими операторами. Именно поэтому потерпевшие при попытке перезвонить на номер мошенника узнают, что данного номера телефона нет.

Анализируя комплекс детерминант данного рода мошенничеств, следует отметить, что выделяются различные факторы. В первую очередь к ним относятся социально-экономические факторы [7]: бедность, корыстный мотив, целью которого является собственное обогащение и отсутствие постоянного места работы (мошенники относятся к атипичному виду людей, которые хотят облегчить себе жизнь, прилагая при этом наименьшие усилия).

На совершение мошенничества влияет острая необходимость в денежном обеспечении. Так, к примеру, отрицая необходимость в осуществлении своей трудовой деятельности, данные лица предпочитают устанавливать «выгодные» взаимоотношений с целью получения выгоды посредством причинения ущерба и нарушения прав иных лиц.

Еще одним фактором мошенничества, распространяющимся на потерпевших, является идеологический. Среди граждан достаточно доверчивых лиц, уровень юридических знаний которых не настолько высок, допустим, в той же сфере банковской деятельности. На телевидении, в СМИ постоянно проводится профилактическая работа с гражданами. Им демонстрируют примеры мошеннических схем, способы их совершения, но люди несерьезно относятся к данной информации, считая, что именно их это не коснется.

Борьба с мошенничеством для государства в настоящее время является прерогативой. Для совершенствования противодействия данному роду мошенничества необходимо принятие масштабных решений.

При анализе изложенной информации и иных источников, способствующих изучению данной проблемы, необходимо определить задачи, которые будут способствовать противодействию мошенничеству.

Во-первых, следует продолжать проводить профилактическую работу в сфере телефонного мошенничества, заключающуюся в постоянной агитации на телевидении и в СМИ, описании схем и способов совершения мошенничества, даче юридической оценки данной проблемы со стороны правоохранительных органов и государства в целом, что способствует развитию правосознания у граждан.

Во-вторых, сфера «мобильного» мошенничества требует совершенствования законодательства, т.е. принятия таких нормативных правовых актов, которые будут способствовать уменьшению совершения преступлений. Примером может служить Федеральный закон «О связи» от 07.03.2003 №-126 ФЗ. В ст. 7 закона говорится, что операторы связи обязаны обеспечивать защиту данных их пользователей от несанкционированного доступа к ним. Закон подразумевает защиту данных от всяческого рода посягательств, но на практике этого добиться сложно, поэтому важно внесение в закон поправки, касающейся способов обеспечения такой защиты. Помимо внесения изменений важно учитывать, кем это будет обеспечиваться. Операторы в полной мере не в состоянии контролировать «утечку» данных пользователей. Данные полномочия необходимо передать органам внутренних дел, т.к. они более компетентны в данной сфере и обладают большим спектром полномочий по противодействию мошенничеству.

В-третьих, стоит рассмотреть вопрос совершенствования норм уголовного законодательства и ужесточения санкций за мошенничество. В ст. 159 УК РФ и её примечаниях мошенничество с использованием средств связи рассматривается отнюдь не как отдельный состав преступления, а только как способ совершения мошенничества. Следует тщательно рассмотреть данный вопрос на законодательном уровне, так как даже статистика предусматривает разделение мошенничества на различные категории, куда входит мошенничество с использованием средств связи. Максимальный срок санкции по ст. 159 УК РФ составляет до 10 лет лишения свободы. Так как данный вид преступления приобрел организационную форму, целесообразно повысить срок отбывания наказания.

1. Семенов Г.В. Расследование преступлений в сфере мобильных телекоммуникаций. – М., 2008.
2. Астишина Т.В., Маркелова Е.В. Проблемы расследования преступлений, связанных с мошенническими действиями, совершенных с использованием средств сотовой телефонной связи // Вестник Казанского юридического института МВД России. 2014. № 2 (16).
3. Министерство внутренних дел: официальный сайт [Электронный ресурс] // URL: <https://мвд.рф/>
4. Латыпова К.С., Дымошеева С.Д. // Молодой ученый. 2021. № 45 (387) [Электронный ресурс] // URL: <https://moluch.ru/archive/387/85133/>.
5. Округко В.Ю. Особенности личностных свойств и качеств современного мошенника // Перспективы государственно-правового развития России в XXI веке: материалы всероссийской науч.-теорет. конф. (23 апреля 2008 г., Ростов-на-Дону, Таганрог). – Таганрог, 2008.
6. Потапова А.В. Мошенничество в сети Интернет: криминологическая характеристика и проблемы квалификации [Электронный ресурс] // StudNet. 2020. № 6 // URL: <https://cyberleninka.ru/article/n/moshennichestvo-v-seti-internet-kriminologicheskaya-harakteristika-i-problemy-kvalifikatsii>.
7. Округко В. Ю. Основные факторы, влияющие на борьбу с мошенничеством // Социокультурные трансформации в России: исторический опыт, проблемы, перспективы: материалы науч.-практ. конф. (г. Армавир, 3-4 октября 2008 г.). – Армавир, 2009.

Информация об авторе:

Ю.А. Страунинг,
заместитель начальника
кафедры криминологии,
кандидат юридических наук, доцент

About the author:

Yu.A. Strauning,
deputy chief
Department of Criminology,
PhD, assistant professor

Статья поступила в редакцию 15.01.2023