УДК 343.9

КРИМИНОЛОГИЧЕСКАЯ ХАРАКТЕРИСТИКА МОШЕННИЧЕСТВА В СЕТИ ИНТЕРНЕТ

Квасникова Т.В.

к.ю.н., доцент,

Дальневосточный федеральный университет,

Россия, Владивосток

Левша Н.Ю.

студентка 4-ого курса Юридической школы,

Дальневосточный федеральный университет,

Россия, Владивосток

Коробейников И.В.

студент 4-ого курса Юридической школы,

Дальневосточный федеральный университет,

Россия, Владивосток

Аннотация. Целью настоящей статьи является исследование института мошенничества в сети Интернет, причин, которые обуславливают совершение такого рода преступлений, изучение личности преступника, в том числе на основании статистических данных о состоянии преступности, анализ организации и деятельности органов государственного контроля за совершением преступлений с применением IT технологий, отражение примеров возможных способов совершения данной категории преступлений, выработка мер предупреждения мошенничества в сети Интернет. Отмечается, что больше всего на снижение количества мошеннических преступлений может оказать повышенная личная, правовая ответственность граждан, которые могут оказаться жертвами преступных действий.

Ключевые слова: интернет, мошенничество, преступные схемы, причины и условия совершения мошенничества в сети Интернет, предупреждение мошенничества в сети Интернет.

CRIMINOLOGICAL CHARACTERISTICS OF FRAUD ON THE INTERNET

Kvasnikova T.V.

Candidate of Law, Associate Professor

Far Eastern Federal University,

Russia, Vladivostok

Levsha N.Yu.

4th year student of Law School,

Far Eastern Federal University,

Russia, Vladivostok

Korobeinikov I.V.

4th year student of Law School,

Far Eastern Federal University,

Russia, Vladivostok

Annotation. The purpose of this article is to study the institution of fraud on the Internet, the reasons that determine the commission of such crimes, study the identity of the offender, including on the basis of statistical data on the state of crime, analyze the organization and activities of state control bodies for committing crimes using IT technologies, reflection of examples of possible ways of committing this category of crimes, development of measures to prevent fraud on the Internet. It is noted that most of all to reduce the number of fraudulent crimes can have increased personal, legal responsibility of citizens who may be victims of criminal acts.

Keywords: Internet, fraud, criminal schemes, reasons and conditions for committing fraud on the Internet, preventing fraud on the Internet.

Современный цифровой век внедрил высокие технологии и создал новые возможности: появление безналичных платёжных систем, банковских карт, значительно облегчает людям жизнь, позволяя оплачивать товары и услуги не выходя из дома, но в то же время все эти новшества привели к появлению новой области преступности, где люди используют технологические достижения в преступных целях.

По статистике, приведённой МВД России, число зарегистрированных преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации выросло на 69,7 процентов в сравнении с прошлым годом. В 2019 году за период с января по октябрь правоохранительными органами было зарегистрировано 240 209 преступлений, предварительно расследовано 53 706 из них. Для совершения таких преступлений используются различные средства. Большинство преступлений совершаются с использованием сети Интернет, таких преступлений было зарегистрировано 126276, из них раскрыто правоохранительными органами было 28656, удельный вес также составляет мошенничество с использованием пластиковых (расчётных) карт - всего зарегистрировано 27727 преступлений, раскрыто 12470 из них [1].

Мошенничество с использованием сети Интернет происходит по разным причинам. Наиболее частой причиной преступлений в интернете становится банальная невнимательность пользователей, либо недостаток знаний о правилах безопасности.

Что касается причин, по которым злоумышленники идут на совершение мошенничества с использованием интернета, то можно выделить следующие. Во-первых, это уверенность злоумышленника в том, что его личность не будет раскрыта. Очевидно, что в условиях анонимности любой человек ощущает возможность безнаказанно совершать поступки негативного характера, при этом отсутствие эффективных механизмов порицания только усиливает желание лица совершать неправомерные действия. Действительно, Интернет сегодня даёт

возможность практически 100-процентной анонимности, например, преступник использует специальное программное обеспечение, чтобы скрыть IP-адрес компьютера, по которому правоохранительные органы смогли бы определить местонахождение его владельца либо использует электронный кошелёк, на который жертва переводит денежные средства, при этом они не позволяют идентифицировать пользователя, которому денежные суммы переводятся. Злоумышленник может зарегистрировать такой кошелёк на любое имя, номер телефона, принадлежащий другому человеку, все это позволяет ему оставаться неизвестным.

Интернет-мошенников привлекает возможность лёгкого и быстрого заработка. Так, например, зачастую мошенниками размещаются объявления о сдаче квартиры в аренду с первоначальным переводом залоговой суммы. В населённых пунктах, где большой спрос на жилые помещения велика вероятность стать жертвой мошенника. Кроме того, денежные средства, переведённые за оплату работ/услуг, вещей и др. вернуть невозможно, даже если сумма была переведена на банковскую карту, банк не может отозвать платёж, если он уже исполнен, так как денежные средства были переведены добровольно и являются к тому времени собственностью злоумышленника. Существуют и другие способы, например, на сегодняшний день очень актуальны опросы, за прохождение которых в сети обещают получение денежных средств, практикуется такое мошенничество на базе социальных сетей. Одной из самых популярных социальных сетей сегодня является Instagram, где зачастую известные люди с многомиллионной аудиторией просят пройти такого рода опросы и гарантируют денежное вознаграждение, однако после прохождения опроса необходимо заплатить самому, чтобы денежные средства якобы были зачислены на банковскую карту, но после оплаты зачисления денежной суммы не происходит. Исходя из приведённых нами примеров становится понятно, почему сеть Интернет притягивает мошенников - здесь не нужно общаться с человеком, входить к нему в доверие - все это долгий процесс, который может и

не дать необходимый мошеннику результат. С Интернетом все гораздо проще, разместить объявление на сайте в сети Интернет или в социальных сетях, заплатить известному человеку за рекламу, завести электронный кошелёк, создать сайт для якобы продажи товаров не составляет большого труда.

Кроме того, на сегодняшний день отсутствует эффективный государственный контроль над виртуальным компьютерным пространством. Конечно, государственными органами предпринимаются определённые меры в этом направлении. Например, 31 декабря 2017 года был подписан Федеральный закон № 482-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» [2], которым обеспечено законодательное закрепление возможности проведения удалённой идентификации, то есть банкам разрешается собирать биометрические данные клиентов. Данная мера должна помочь обезопасить клиентов банков от случаев мошенничества. Однако, данное нововведение встретило немало критики. Поэтому, необходимо отметить, что государственные органы, пытаясь установить контроль над Интернет-пространством и оградить граждан от мошенничества в сети, зачастую наталкиваются на активное сопротивление со стороны общественных институтов представители которого усматривают в этом ущемление прав граждан и вмешательство в их частную жизнь.

А.А. Комаровым выделяется ещё одна детерминанта мошенничества в Интернете - недостатки в правоохранительной деятельности [3, с. 90]. Раскрываемость преступлений, связанных с использованием сети Интернет составляет всего четвертую часть от числа зарегистрированных преступлений, совершенных данным способом. Становится ясно, что во многих случаях раскрытие и расследование преступлений связано с определёнными трудностями. Субъектам расследования мошенничества в сети Интернет необходимо совершенствовать свои знания в области правоприменения параллельно с изучением различных аспектов развития сферы IT-технологий. Это будет способствовать повышению квалификации следователей, позволит им

более эффективно расследовать уголовные дела, возбуждённые по фактам интернет-мошенничества [4, с. 591].

Основной чертой интернет - мошенничества является то, что потерпевший не знает преступника в лицо, и оно оставляет мало следов преступлений. В связи с этим достаточно сложно установить личность мошенника.

Личность преступника. В 2018 году по статьям 159.3 и 159.6 всего было осуждено 293 человека, из них 22 % составили женщины. Характеризуя личность преступника по социальному положению отметим, что большинство осуждённых трудоспособные лица без постоянного источника дохода, их доля составляет 60 % от общего числа осужденных, на втором месте рабочие - 23 %, 7 % составили служащие коммерческих и иных организаций, меньшинство осужденных это студенты - 3 %. Что касается уровня образования, то преобладающее число преступников имеет среднее профессиональное образование - 39 %, среднее общее образование имеют 31 % осужденных, в меньшинстве лица, имеющие высшее и среднее начальное образование - 5 % и 2 % соответственно [5].

Меры предупреждения Интернет-мошенничества. Прежде всего, пользователям Интернет-пространства самим необходимо применять определенные меры безопасности: не сообщать пароли от банковских карт посторонним лицам; обращать внимание на цену товара или услуги, если на данном рынке она является явно заниженной, то отказаться от сомнительной сделки; разумно оценивать тот факт, что никто не будет платить Вам огромные деньги за прохождение интернет-опроса или за розыгрыш, в котором вы участвовали [6, с. 4-5].

Резюмируя вышесказанное, хочется еще раз обратить внимание, что мошенничество в сети интернет становится новой угрозой не только для имущественного благосостояния физических лиц, но и для безопасности всего общества в целом. Именно поэтому при пользовании интернет-технологиями стоит проявлять бдительность, не давать свои личные данные незнакомым

людям не будучи уверенным, что этот человек не является злоумышленником, ни при каких обстоятельствах не сообщать коды подтверждения операций и иные сведения, позволяющие получить доступ к счетам и электронному кошельку. Кроме того, следует помнить, что «если кто-то хочет получить от вас хоть какие-то деньги, предлагая заработок – это мошенничество. Всегда. Исключений – нет» [7, с. 74].

Библиографический список

1. Состояние преступности / Официальный сайт МВД России. URL: https://media.mvd.ru/files/application/1703551 (дата обращения: 23.12.2019).

2. О внесении изменений в отдельные законодательные акты Российской Федерации [Электронный ресурс]: федеральный закон от 27.12.2017 № 482-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс». Загл. с экрана.

3. Комаров А.А. Криминологические аспекты мошенничества в глобальной сети Интернет: дисс. … канд. юрид. наук. Саратовская государственная юридическая академия. Саратов, 2011. 262 с.

4. Стельмах С.Р., Жирнова Н.А. Мошенничество в сети Интернет // В сборнике: Экономика. Образование. Право. Научные исследования состояния и развития современного общества^ Сборник научных трудов по материалам международной научно-практической конференции. 2016. С. 588-591.

5. Сводные статистические сведения о состоянии судимости в России за 2018 год / Официальный сайт Судебного департамента при Верховном суде Российской Федерации. URL: http://www.cdep.ru/index.php?id=79&item=4894 (дата обращения: 23.12.2019).

6. Гренева К.В., Мухина О.О. Мошенничество в Интернете / К.В. Гренева О.О. Мухина // Дневник науки. - 2017. - № 7. - С. 7.

7. Магомедов, Ш.М. Финансовое мошенничество в сети «Интернет» / Ш.М. Магомедов // Эффективность бизнеса в условиях международной нестабильности: сборник материалов международной научно-практической

конференции, Симферополь, 31 мая-02 июня 2017 г. Симферополь: Изд-во Автономной некоммерческой образовательной организации высшего образования «Крымский институт бизнеса», 2017. С. 60-74.

Оригинальность 77%