DOI: 10.47026/2499-9636-2022-3-47-54

УДК 343.9
ББК Х515

Ю.А. КУЗЬМИН

ПРЕДУПРЕЖДЕНИЕ ТЕЛЕФОННОГО МОШЕННИЧЕСТВА (криминологический аспект)

Ключевые слова: *криминология, преступность, мошенничество, телефонное мошенничество, предупреждение телефонного мошенничества.*

Актуализируются проблемы совершения мошенничества с использованием телефонной связи.
Обосновывается актуальность вопросов, связанных с предупреждением телефонного мошенничества, прежде всего спуфинга идентификатора вызывающего абонента и фишинга.
Анализируются такие методы предупреждения телефонного мошенничества, как возможность установления номера мошенников через электронные поисковые сервисы, специальные бесплатные сервисы, мессенджеры Viber и WhatsApp, Сбербанк Онлайн, определитель номеров входящих звонков по «Avito» и «Юле», через приложения для iPhone и Android, определитель номеров от «Лаборатории Касперского» – Kaspersky Who Calls, через поисковую систему в Интернете «Yandex» и другие приложения.
Рекомендуется применение методов виктимологического противостояния телефонным мошенникам, таких как психологическая самозащита, критичность (осмотрительность) в собственных действиях (главным образом, финансового характера), безопасное поведение в нестандартной ситуации, критический уровень доверия, осознание возможных рисков.
Необходимо принимать меры предосторожности, чтобы не стать жертвой телефонного мошенничества, не терять самообладания и бдительности, использовать все возможности для проверки источника телефонного мошенничества, сообщать о подобных случаях в правоохранительные органы. Личная заинтересованность в сохранении собственной безопасности, стремление к самозащите и своевременное информирование правоохранительных органов станут преградой на пути распространения телефонного мошенничества.

Одной из важнейших задач криминологии является предупреждение преступлений. Мошенничество – преступное деяние, состоящее в хищении чужого имущества, приобретении права на чужое имущество путём обмана или злоупотребления доверием. Совершая такое деяние, преступники прибегают к сознательному искажению истины или умолчанию об истине. В результате обманутые потерпевшие сами передают своё имущество мошенникам. Актуальность нашего исследования состоит в том, что в последнее время участились случаи телефонного мошенничества, в результате которого обманутые потерпевшие отдают преступникам свои денежные средства.

Цель исследования – раскрыть основные формы телефонного мошенничества, показать способы предупреждения и противодействия данному виду преступлений.

В силу своей специфики криминология широко использует метод кумулятивизма, позволяющий большинству потенциальных потерпевших получать и развивать знания (в том числе о возможных преступлениях) путем получения

все большего количества необходимой информации (количественного роста знания), постепенного прибавления новых положений к уже накопленной сумме знаний, одним словом, кто предупрежден – тот вооружен.

Особое место в структуре современной преступности занимает телефонное мошенничество, посягающее на экономические, личные, информационные права граждан. Телефонное мошенничество – особый вид мошенничества в области информационных технологий, представляющий собой несанкционированные действия и неправомерное пользование ресурсами и услугами, хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, модификации информации или другого вмешательства в работу средств обработки или передачи данных информационно-телекоммуникационных сетей [4. С. 15].

Мошенники сегодня становятся все более высокотехнологичными. Все знают, что индустрия мобильных телефонов переживает колоссальный подъем, а количество пользователей мобильных телефонов постоянно увеличивается. Преступники звонят или отправляют на телефон намеченной жертвы фальшивые сообщения, чтобы побудить сделать то, что содержится в их сообщении. Звонки, поступающие с неизвестных номеров, становятся большой проблемой. Сегодня мошенники не испытывают проблем с получением номеров телефонов потенциальных жертв. Списки телефонных номеров граждан и организаций можно незаконно приобрести в Интернете, у служащих телефонных компаний, банков, коллекторских фирм, страховых агентств, колл-центров и т.д.

Сами преступники при совершении мошеннических действий пользуются огромным количеством телефонных номеров, чтобы избежать возможности быть разоблаченными и задержанными правоохранительными органами. Их номера могут быть зарегистрированы как в России, так и за ее пределами, это могут быть номера обычные, подменные или зарегистрированные на подставных лиц и т.д. Все используемые злоумышленниками номера, разумеется, невозможно перечислить [2. С. 89]. Составить список наиболее популярных телефонных номеров, которые используют мошенники, также довольно проблематично, так как данные номера постоянно меняют своих владельцев.

Наиболее часто граждане, подвергшиеся атакам телефонных мошенников, жалуются на телефонные номера с кодом г. Москва +7 (495), а также на номера виртуальных облачных АТС [6. С. 296]. Также пользователи жалуются на сброс после звонка, на попытку мошенников выдать себя за сотрудников оператора, на то, что после принятия вызова, телефонный робот сообщает информацию об успешном одобрении кредита от какого-либо банка.

К сожалению, чтобы защитить себя от такого вида мошенничества, сегодня не представляется возможным использовать готовый список номеров телефонных мошенников для внесения его в список запрещенных номеров («черный список») на своем телефоне. Незнакомые номера придется все-таки вносить вручную в базу номеров своего телефона и таким образом определять звонившего.

Сегодня телефонные мошенники используют различные криминальные схемы для постижения своих преступных целей. Например, чтобы ограбить потенциальных жертв, они подделывают номера телефонов банков, выдают себя за банковских менеджеров, просят проверить номер на вашем дисплее онлайн, чтобы потерпевший убедился, что звонок действительно поступил из его банка. Преступники продумывают все ходы, чтобы избежать возникновения подозрений у потенциального потерпевшего относительно того, что телефонный номер может быть подделан. Если потерпевший предложит перезвонить им, они могут сказать, что позвонить на их добавочный номер напрямую невозможно и придется обратиться к оператору в головном офисе, это может занять некоторое время, а проведение определенной банковской операции не терпит отлагательств.

В последние годы получил распространение такой вид телефонного мошенничества, как спуфинг идентификатора вызывающего абонента (англ. spoofing – подменять) – маскировка под другую личность путём фальсификации личных данных, позволяющая получать незаконные преимущества. Подмена идентификатора вызывающего абонента – это когда кто-то, звонящий на ваш телефон, намеренно фальсифицирует информацию, передаваемую на дисплей идентификатора вызывающего абонента, чтобы скрыть свою личность. Обычно на вашем дисплее отображаются номер телефона и имя, связанные с линией, по которой вам звонят. Мошенники обладают достаточными знаниями о банковском счете потенциальной жертвы. Преступники сообщают, что заметили необычную активность на банковском счете жертвы и настоятельно советуют положить деньги на другой счет. Если жертва указывает, что у нее только одна учетная запись, мошенник предлагает ей так называемый «счет в хранилище» банка. Мошенник объясняет, что такой аккаунт – безопасное место для временного сохранения средств потенциальных потерпевших и деньги могут быть недоступны на таком счете в течение нескольких дней, но это лучше, чем потерять их. Если жертва начнет задавать много вопросов, мошенник скажет, что нельзя терять время из-за опасности потерять все денежные средства, находящиеся на счете. Разумеется, эта учетная запись «хранилища» принадлежит мошеннику, и весь телефонный спектакль разыгрывается только для того, чтобы жертва перевела свои деньги на эту учетную запись. После перевода денежных средств мошенники на связь не выходят.

Мошенники, как правило, совершают телефонный звонок подготовленными [3. С. 335]. Они могут владеть информацией о том, сколько денежных средств на счету потенциальной жертвы, а также о последних совершенных платежах. Существует несколько способов получения мошенниками подобного рода информации. Например, у мошенников могут быть сообщники, работающие в банке. Некоторые жертвы сообщали, что незадолго до звонка получили фишинговое письмо. Фишинг (англ. phishing – выуживание) – вид интернет-мошенничества, цель которого состоит в получении идентификационных данных пользователей (кража паролей, номеров кредитных карт и т.д.). Это достигается с помощью рассылки (или отправки) по электронной почте поддельных уведомлений от банков и других организаций о том, что клиенту

необходимо в кратчайшие сроки передать или обновить свои персональные данные. Причины могут быть любые – утрата данных, сбой в системе и др. Выдавая себя за финансовое учреждение, мошенник отправляет на e-mail потенциальной жертвы сообщение, чтобы раскрыть его личную информацию. Фишинговые сайты отражают сайт банка, и фишер может проследить за входом жертвы в реальный сайт банка. Это позволяет им просматривать данные учетной записи после входа в систему и снабжать их информацией, которую они могут использовать во время телефонного звонка.

Если информация об учетной записи жертвы, которой располагает мошенник, является результатом попытки фишинга, и банк использует метод входа в систему с двухфакторной аутентификацией, информация для входа в систему довольно быстро устареет. Успешный фишинг позволяет мошенникам войти в систему, но обычно только один раз. Они могут собрать информацию, чтобы подготовиться к звонку. Любые последующие действия, такие как совершение платежа или изменение настроек, должны быть авторизованы отдельно, и такой запрос, скорее всего, вызовет подозрения у потенциальной жертвы.

Разумеется, службы безопасности банков осведомлены о подобного рода мошенничестве и предпринимают меры по защите вкладов своих клиентов, например, предлагают им использовать кардридеры для сканирования QR-кодов для авторизации входа и платежей. Это делает таких клиентов менее уязвимыми в сравнении с клиентами, отправляющими обычные текстовые сообщения, поскольку имитировать QR-коды на фишинговом сайте банка сложнее, чем создать поле ввода для кода подтверждения.

Еще одним способом надежной защиты кладов потенциальных жертв являются использование лимитов на трансакции, которые установлены по умолчанию для некоторых банков. Часто они ограничиваются довольно небольшими суммами, и клиентам придется увеличить лимит, если они хотят произвести более крупные платежи. Когда банк просит клиента увеличить этот лимит, а не наоборот, это должно стать для последнего тревожным сигналом.

В одних банках предусмотрена страховка от банковского мошенничества, но другие банки могут заявить, что жертва сама перевела средства, и банк в том случае не несет ответственности за убытки. В большинстве стран клиенты защищены законом от мошеннических платежей при определенных условиях. Одно из этих условий обычно можно сформулировать как «клиент не должен быть беспечным», и клиент может считаться беспечным, если он добровольно предоставит свои учетные данные для входа. Вопрос о том, является ли ввод этих учетных данных на фишинговом сайте фальшивого банка, который выглядит точно так же, как сайт реального банка, неосторожным, остается предметом споров.

Особым видом мошенничества, имеющим много общих уголовно-правовых черт с вымогательством, являются телефонные звонки потерпевшим, где им сообщается, что их близкие попали в беду, в полицию и т.д. и что за помощь в решении возникшей проблемы им необходимо перечислить на определенный счет некоторую сумму денег. Мошенники используют телефон, чтобы обмануть свою жертву и выманить у них денежные средства, играя на их чувствах.

Преступники подвергают потерпевших психологической атаке. Эти телефонные мошенники могут назваться близкими родственниками, например внуком пожилого человека, и послать ему сообщение типа: «дедушка, это твой внук, я совершил ДТП, мне срочно нужно 10 тысяч рублей, чтобы меня не забрали в полицию, переведи деньги на такой-то номер». Конечно, не все сразу переводят деньги, кто-то не верит сообщению и не делает перевод, но преступники таких сообщений делают не одну сотню в день в надежде, что кто-нибудь да переведет им деньги.

В случае возникновения подобных ситуаций необходимо прежде всего проверить достоверность информации. Следует помнить о таких способах виктимологического противостояния мошенникам, как психологическая самозащита, критичность (осмотрительность) в собственных действиях (главным образом, финансового характера), безопасное поведение в нестандартной ситуации, критический уровень доверия, осознание возможных рисков.

Телефонные звонки мошенников сегодня становятся все более распространенным способом противоправного посягательства [1. С. 301]. Мошенники обучены профессионально разговаривать с потенциальными жертвами. Они часто говорят с людьми о поддельных продуктах или услугах, которые в целом им выгодны. Во многих случаях мошенники выдают себя за сотрудников сервисных центров и часто создают фальшивые уведомления, в которых они создают у потерпевших ощущение срочности в отношении исполнения услуги. В некоторых других случаях мошенники звонят жертвам, представляя себя представителями благотворительных организаций, с просьбой о пожертвованиях. Также были зарегистрированы случаи, когда мошенники звонили своим жертвам, представляясь представителями государственных налоговых органов, требуя заплатить пошлину за возврат налога.

Невозможно отследить законность звонка на основе разговора. Единственный способ – проверить по номеру телефона звонящего. Мошеннические звонки могут поступать откуда угодно – из-за границы, из других регионов, из мест лишения свободы [4. С. 16].

Существует несколько способов узнать, кто звонил по номеру телефона, даже если номер был скрыт.

Поиск номера через поисковые сервисы – один из самых доступных способов определения звонка с незнакомого номера. На эту процедуру затрачивается несколько минут, одной проверки бывает достаточно, чтобы опознать входящий номер. Так как в большинстве случаев с незнакомых номеров звонят банки или компании с различными «выгодными» предложениями, их определение происходит на первой же странице поисковой выдачи. Чтобы эффективно пробить номер телефона в «Google» или «Yadex», его рекомендуется вводить в разных форматах, например 89xxxxxxxxx, 8 (9xx) xxx-xx-xx, 79xxxxxxxxx, +7 (9xx) xxx-xx-xx. Определенный формат номера можно обнаружить на различных сайтах, включая те, на которых хранятся сведения о физических лицах в открытом доступе [5].

Эффективным способом определения подозрительных номеров является их проверка через специальные бесплатные сервисы, например: neberitrubku.ru,

кто-звонит.рф, zvonkoff.net, zvonili.com. На этих сайтах происходит подборка таких номеров и размещаются отзывы граждан о них, которые часто делятся подробными комментариями о таких номерах, в том числе предупреждают о мошенниках. После запроса становится понятно, важен ли был звонок, либо это были мошенники.

Проверка номеров через популярные мессенджеры Viber и WhatsApp, в которых зарегистрировано большинство абонентов сотовых операторов. Однако не всем известно, что Viber и WhatsApp свободно раскрывают некоторые сведения о своих пользователях. Для того, чтобы «пробить» номер по одному из мессенджеров, достаточно начать добавлять его в контакты. Практически сразу можно узнать имя того, кто звонил вам со скрытого номера и получить его фотографию.

Проверка номера через «Сбербанк Онлайн» позволяет узнать имя и отчество человека, которому принадлежит неизвестный номер. Если номер не зарегистрирован в Viber и WhatsApp, для его проверки через сервис «Сбербанк Онлайн» необходимо начать выполнение процедуры перевода по номеру телефона. Можно указать в качестве суммы перевода 1 рубль и нажать «Продолжить». Этот рубль не будет снят со счета до подтверждения, выполнять которое не потребуется. После нажатия кнопки «Продолжить» нужно перейти в меню подтверждения оплаты, где будут указаны имя и отчество получателя.

Определение звонков по «Avito» и «Юле» через доску объявлений – специальный сервис, в котором собирается база объявлений по номерам телефонов. Так можно установить имя абонента, где он живет и какие объявления он подавал на популярные доски объявлений. Иногда в тексте объявлений размещается дополнительная информация.

Определение звонков через приложения для iPhone и Android. Для iPhone и Android-смартфонов есть много приложений со встроенными определителями номеров. В базах таких приложений насчитываются тысячи номеров, по каждому из которых пользователю предоставляется дополнительная информация, в том числе предупреждения в случае, если номер принадлежит мошенникам.

Существуют приложения с определителями номеров, например, «Яндекс» (iOS, Android). Приложение полностью бесплатное, содержит огромную базу номеров и умеет выдавать полезные предупреждения, например, о мошенниках или рекламе. Для оценки незнакомого номера «Яндекс» использует собственную базу «Яндекс.Справочника», отзывы пользователей приложения. Механизмы приложения оценивают частоту звонков с номеров, продолжительность разговоров и другие параметры. Все это позволяет приложению выдавать максимально точные рекомендации даже по незнакомым номерам, которых нет в базе.

Определитель номеров от «Лаборатории Касперского» – Kaspersky Who Calls (iOS, Android). В приложении огромная база номеров, которая пополняется еженедельно. Вся база хранится прямо на смартфоне пользователя. За счет этого определение номера выполняется и при отсутствии подключения мобильного устройства к Интернету. Приложение может блокировать звонки от мошенников и других нежелательных лиц еще до появления вызова. Пользователь может просмотреть заблокированные подозрительные звонки.

Многие сталкиваются с проблемой – как узнать скрытый номер. Часто назойливые звонки выполняются со скрытых номеров. На такие номера невозможно перезвонить, их нельзя занести в черный список. Из-за этого с ними связаны наибольшие неприятности. Перезванивая на неизвестный и непроверенный номер, вы можете наткнуться на платную телефонную линию. Деньги со счета вашего телефона начнут списываться еще до того, как мошенники возьмут трубку. Менее чем за минуту ваш телефонный счет может уменьшиться на 100–200 рублей. Требования вернуть деньги у оператора сотовой связи будут бесполезны. Еще одна опасность состоит в том, что неизвестные номера могут вынуждать абонента перезвонить для того, чтобы украсть его номер. Это касается владельцев «красивых» номеров, обычно полученных более десяти лет назад. За последние несколько лет зафиксированы сотни случаев подобных краж номеров сотовых телефонов. Поэтому перезванивайте на неизвестные номера только после полноценной проверки [5].

Таким образом, в наше время телефонное мошенничество является весьма распространенным видом преступности. Для его предупреждения потенциальным потерпевшим необходимо принимать меры предосторожности, чтобы не стать жертвой мошенников, быть бдительными, использовать все возможности, чтобы проверить источник мошенничества. Способов проверки источника мошенничества сегодня существует достаточное количество, о них необходимо доводить информацию до граждан. И, разумеется, своевременно сообщать о фактах телефонного мошенничества в правоохранительные органы.

Литература

1. *Антонян Ю.М.* Криминология. 3-е изд., перераб. и доп. М.: Юрайт, 2019. 388 с.

2. *Загородников С.Н., Шмелев А.А*. Основы информационного права. М.: Академический Проект, 2016. 192 с.

3. Криминологи / под ред. В.Н. Кудрявцева и В.Е. Эминова. 5-е изд., перераб. и доп. М.: Юристъ, 2014. 800 с.

4. *Леваков А.К.* Телефонное мошенничество: трудности противодействия // Вестник связи. 2020. № 12. С. 15-16.

5. *Михайленко С.* Как узнать, кто звонил с неизвестного номера [Электронный ресурс]. URL: https://bloha.ru/iphone-ipad-guides/kak-uznat-kto-zvonil-s-neizvestnogo-nomera (дата обращения: 25.11.2021).

6. *Теппеев А.А.* Телефонное мошенничество // Евразийский юридический журнал. 2020. № 6(145). С. 296–297.

КУЗЬМИН ЮРИЙ АНАТОЛЬЕВИЧ – старший преподаватель кафедры уголовно-правовых дисциплин, Чувашский государственный университет, Россия, Чебоксары (kya70@mail.ru; ORCID: https://orcid.org/0000-0003-4115-9811).

Yuriy A. KUZMIN

PREVENTION OF TELEPHONE FRAUD
(criminological aspect)

Key words: *criminology, criminality, fraud, telephone fraud, prevention of telephone fraud.*

The problems of committing fraud using telephone communication are updated.
The relevance of issues related to the prevention of telephone fraud, first and foremost caller ID spoofing and phishing, is substantiated.

The article analyzes the methods of preventing telephone fraud, such as the possibility of establishing the number of fraudsters through electronic search services, special free services, Viber and WhatsApp messengers, Sberbank Online, caller ID for incoming calls on "Avito" and "Yula", through applications for iPhone and Android, caller ID from "Kaspersky Lab" – Kaspersky Who Calls, through the Internet search engine "Yandex" and other applications.

It is recommended to use the methods of victimologic counter-strategy in relation to telephone fakers, such as psychological self-defense, criticality (prudence) in their own actions (mainly those of a financial nature), safe behavior in a non-standard situation, a critical level of trust, awareness of possible risks.

It is necessary to take precautions not to become a victim of telephone fraud, not to lose self-control and vigilance, to use all opportunities to check the source of telephone fraud, to report such cases to law enforcement agencies. Personal interest in maintaining personal security, the desire for self-defense and timely informing law enforcement agencies will become an obstacle to the spread of telephone fraud.

References

1. Antonyan Yu.M. *Kriminologiya. 3-e izd., pererab. i dop.* [Criminology. 3th ed.]. Moscow, Yurayt Publ., 2019, 388 p.

2. Zagorodnikov S.N., Shmelev A.A. *Osnovyi informatsionnogo prava* [Fundamentals of Information Law]. Moscow, Akademicheskiy Proekt Publ., 2016, 192 p.

3. Kudryavtsev V.N., Eminov V.E., eds. *Kriminologiya. 5-e izd., pererab. i dop.* [Criminology. 5th ed.]. Moscow, Yurist Publ., 2014, 800 p.

4. Levakov A.K. *Telefonnoye moshennichestvo: trudnosti protivodeystviya* [Telephone fraud: difficulties countering]. *Vestnik svyazi*, 2020, no. 12, pp. 15–16.

5. Mixajlenko S. *Kak uznat', kto zvonil s neizvestnogo nomera* [How to find out who called from an unknown number]. Available at: https://bloha.ru/iphone-ipad-guides/kak-uznat-kto-zvonil-s-neizvestnogo-nomera (Accessed Date 2021, Nov. 25).

6. Teppeyev A.A. *Telefonnoye moshennichestvo* [Telephone fraud]. *Evraziyskiy yuridicheskiy zhurnal,* 2020, no. 6(145), pp. 296–297.

YURIY A. KUZMIN – Senior Lecturer of Criminal Law Department, Chuvash State University, Russia, Cheboksary (kya70@mail.ru; ORCID: https://orcid.org/0000-0003-4115-9811).

Формат цитирования: *Кузьмин Ю.А.* Предупреждение телефонного мошенничества (криминологический аспект) [Электронный ресурс] // Oeconomia et Jus. – 2022. – № 3. – С. 47–54. – URL: http://oecomia-et-jus.ru/single/2022/3/7. DOI: 10.47026/2499-9636-2022-3-47-54.