

Костюк М.Ф., Кунц Е.В.

ПРОФИЛАКТИКА ДИСТАНЦИОННОГО МОШЕННИЧЕСТВА

Kostyuk M.F., Kuntz E. V.

REMOTE FRAUD PREVENTION

Предотвращение и пресечение преступлений находятся в определенной зависимости от того, насколько эффективна профилактика. Чем ниже эффективность профилактики, тем чаще правоохранительные органы, общественные организации и просто граждане будут вынуждены прибегать к предотвращению и пресечению преступлений. Существенная роль в предупреждении преступлений отводится уголовному законодательству, которому изначально присуща цель общей превенции. Данная деятельность несет в себе большой социально позитивный потенциал, и по ряду признаков преимущественно отличается от других направлений борьбы с этим злом. В настоящей статье раскрываются вопросы профилактики дистанционного мошенничества.

Ключевые слова: дистанционное мошенничество, профилактика, предупреждение, законодательство, уголовный закон.

Prevention and suppression of crimes are to a certain extent dependent on how effective prevention is. The lower the effectiveness of prevention, the more often law enforcement agencies, public organizations and ordinary citizens will be forced to resort to preventing and suppressing crimes. A significant role in the prevention of crimes is assigned to criminal legislation, which is originally inherent in the goal of general prevention. This activity carries a great socially positive potential, and by a number of features it mainly differs from other areas of struggle against this evil. This article covers the issues of prevention of remote fraud.

Keywords: remote fraud, prevention, prevention, legislation, criminal law.

Согласно Стратегии национальной безопасности РФ [1], утвержденной Указом Президента РФ от 02.07.2021 № 400, несмотря на принимаемые меры, в России остается высоким уровень преступности в отдельных сферах. Совершается большое количество преступлений против собственности, в сфере использования водных биологических и лесных ресурсов, в сфере жилищно-коммунального хозяйства, а также в кредитно-финансовой сфере. Растет число преступлений, совершаемых с использованием информационно-коммуникационных технологий.

На современном этапе развития общества профилактика дистанционного мошенничества является одной из приоритетных его задач. Об этом свидетельствует развитие уголовного законодательства и криминологические показатели этого социально-правового явления.

Федеральным законом от 29.11.2012 № 207 [2] уголовное законодательство

дополнено ст. 1591 – 1596 6 УК РФ, предусматривающих ответственность за мошенничество, совершаемое в сфере кредитования, предпринимательской деятельности, страхования, компьютерной информации, а также при получении выплат или использования платежных карт. Особенность данных составов преступлений состоит в том, что они могут совершаться дистанционно, без непосредственного контакта с потерпевшим и наличия сведений о предполагаемой жертве, что позволяет говорить о дистанционном мошенничестве. При необходимости такие сведения персонального характера можно получить из различных источников, доступных мошенникам, что рассматривается нами как одна из наиболее распространенных проблем совершения рассматриваемых преступлений, требующая комплексного законодательного регулирования.

Такая дифференциация ответственности за мошенничество призвана учиты-

вать специфику совершаемых преступлений в различных сферах деятельности, способ их совершения. Вместе с тем наглядно проявились и проблемы применения данных норм, их конструктивные особенности.

Актуальность дистанционного мошенничества подтверждается криминологическим анализом зарегистрированной преступности. Так, в 2020 г. в Российской Федерации зарегистрировано 2 044 221 преступлений (+1,0%). Общее число преступлений против собственности в этот год возросло на – 4,1% (1220806). При этом мошенничество (ст.ст. 159-1596 УК РФ) возросло до 335631 преступлений, или на (+30,5%) [3]. Рост мошенничества обусловлен многими факторами, в том числе, условиями пандемии. За время самоизоляции в России на 76% отмечен рост числа уголовных дел о телефонном и интернет-мошенничестве [4].

Выявлена корреляционная зависимость между ограничением передвижения людей, их вынужденная изоляция в связи с пандемией, ростом оказываемых дистанционных услуг с использованием с использованием информационно - телекоммуникационных услуг и дистанционным мошенничеством. С ростом оказываем услуг увеличивается и число зарегистрированных случаев мошенничеств, что свидетельствует о недостаточной финансовой грамотности населения, их доверчивости и беспечности.

Важным направлением профилактической деятельности должно быть своевременное внесение изменения как в законодательство, в том числе законы об оперативно-розыскной деятельности, о связи, о банковской деятельности, об информации, так и в ведомственные нормативные акты, направленные на повышение эффективности борьбы с подобными правонарушениями [5].

Без должного реагирования по-прежнему остается бытовое дистанционное мошенничество. Например, работа кассира, выполняемые операции с покупателем с использованием обмана. Эффективным способом противодействия этому является видеонаблюдение и фиксация его действий. Хотя такая проверка на практике, явление редкое.

Дистанционное мошенничество отличается своим многообразием, появляются новые схемы его проявления, растет число пострадавших. К сожалению, жертвы таких преступлений не знают, как им поступать, что делать. Обращение в правоохранительные органы из-за незначительного ущерба представляется нецеле-

сообразным, бытует неуверенность в эффективности их деятельности. К тому же, если ущерб не значительный и есть чувство собственной вины в случившемся.

Такую тенденцию целесообразно менять. Должна выработаться потребность в обращении к защите от противоправных действий злоумышленников, сообщать в полицию о случаях противоправных действий. В этом смысле важно просвещение граждан и формирование установок на безопасное финансовое поведение. Важно мотивировать жертв мошенничеств обращаться в полицию для расследования [5] подобных случаев.

Содержанием предупреждения дистанционного мошенничества является его предотвращение на стадии подготовки и планирования, при «обнаружении умысла» их совершения. На этой стадии возможен добровольный отказ от совершения противоправных действий. Затем следует пресечение дистанционного мошенничества, что возможно на этапе начала или предшествующего этому периоду времени. В это время преступный результат еще не наступил. Целью такой деятельности является недопущения развития преступной деятельности.

Наиболее эффективным и гуманным методом противодействия дистанционному мошенничеству, является его профилактика, направленная, прежде всего, на причинный комплекс совершения указанных противоправных деяний. Это деятельность по выявлению и исключению действия причин, условий и других негативных факторов совершаемых преступлений. В отличие от предупреждения и пресечения, профилактические меры направлены не столько на уголовно-правовое воздействие, сколько на иные меры воздействия на лиц, поведение которых свидетельствует о противоправном поведении.

Если в числе субъектов предупредительной деятельности являются, преимущественно, сотрудники правоохранительных органов, то применительно к профилактике дистанционного мошенничества таковыми являются государственные органы, трудовые коллективы, общественные организации и отдельные граждане. Принимаемые ими меры направлены на недопущения или повторения совершаемых преступлений.

Это наиболее важный уровень борьбы с преступностью, который в этом случае оказывает воздействие на самые криминальные факторы, то есть факторы, порождающие совершение преступления [7, с. 180].





Объектам профилактики дистанционного мошенничества являются, прежде всего, физические лица и банки, которым в результате совершаемых преступлений, причиняется материальный ущерб, а банки, помимо этого, несут репутационные потери, подвергается сомнению их надежность.

Меры профилактики определяются с учетом предмета преступного посягательства, потерпевшего и способа совершения дистанционного мошенничества, не требующего большого вложения средств.

Анализ судебной практики и публикаций по этой проблеме позволяет выявить наиболее распространенные проявления мошенничества. Применительно к банковской сфере это предложения вкладов под более высокий процент. При этом преследуется цель получения доступа к банковским картам с последующим хищением находящихся там средств. Затем следует завладение банковской картой и совершение операций, как правило, в виде покупок.

В рамках дистанционного мошенничества представляется целесообразным выделить комбинированное мошенничество, в основе которого лежит предварительная дистанционная обработка клиента с последующим хищением денежных средств. В качестве примера можно назвать действия с заменой экономных счетчиков расходования воды, электроэнергии и другого оборудования. В результате таких действий потребитель вводится в заблуждение и оплачивает оказываемые услуги под воздействием обмана.

Распространенным является мошенничество с лекарственными средствами, когда вместо качественного препарата предлагается препарат, не соответствующий заявленным свойствам.

Практикуется, также, дистанционное мошенничество, которой условно можно назвать «зов о помощи». Это сообщения о совершенном правонарушении, когда для предотвращения нежелательных последствий необходимо перевести определенную сумму денег, аварии с источником повышенной опасности (автомобилей). При этом злоумышленники настойчиво рекомендуют, подсказывают каким образом и на какой счет перевести деньги, называют «более надежный» для этого банк и счет.

«Агрессивное» дистанционное мошенничество, когда звонок осуществляется от имени сотрудников следственного комитета, службы безопасности и других лиц, представляющихся наделенными

определенными полномочиями. К примеру, ваш телефон зафиксирован возле места совершения преступления. Сейчас к вам подъедут два сотрудника и отвезут вас для опознания. Где вы находитесь? Укажите свои паспортные данные.

По содержанию меры профилактики целесообразно классифицировать на организационно-управленческие; инженерно-технические; научно-образовательные и виктимологические.

Организационно-управленческие меры находят свое выражение в разъяснении мер безопасности клиентам банка, в том числе при дистанционном обслуживании.

Такие меры возложены, на оператора по переводу денежных средств, который обеспечивает выполнение требований к обеспечению защиты информации при осуществлении переводов денежных средств.

Профилактический аспект дистанционного мошенничества определяется тем, что оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают реализацию запрета несанкционированного расширения прав доступа к защищаемой информации; назначение своим работникам минимально необходимых для выполнения их функциональных обязанностей прав доступа к защищаемой информации [8].

Профилактика дистанционного мошенничества должна быть основана на прочной законодательной базе, обеспечивающей информационную безопасность граждан и финансовых организаций. К числу первоочередных следует отнести возможность Банка России и Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций блокировку фишинговых сайтов, содержащих ложную информацию. С их помощью злоумышленники стремятся получить информацию о банковских картах граждан для последующего совершения хищений.

Научно-образовательные меры нацелены на повышение правовых знаний и выработка навыков информационной безопасности:

- повышение финансовой и технической грамотности, что позволит снизить доступ к счетам граждан;
- обращение к здравому смыслу о невозможности получения высокого дохода, основываясь на его обещании от выполнения сомнительных сделок на финансовом рынке. Излишняя доверчивость

к дистанционной информации позволяет мошенникам получить необходимую информацию для последующего хищения.

Инженерно-технические меры профилактики отличаются своей функциональностью. Они включают анализ схем доступа конфиденциальных сведений (код или пароль) к интернет-банку путем общения с использованием обмана. В качестве метода дистанционного воздействия может быть информация корыстного характера в виде выигрыша, поступления социальных выплат, надбавок и т.п. Внушается,

также, чувство страха от несанкционированного доступа к банковскому счету клиента, совершаемых с денежными средствами операциях. Для их предупреждения предлагается назвать код доступа и т.п.

Самостоятельным направлением профилактики дистанционного мошенничества является своевременное выявление копий сайта банка и вирусов, с помощью которых можно получить логин, пароль и другую информацию для последующего хищения денежных средств.

Литература

1. Указ Президента РФ от 2 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации» // Собрание законодательства РФ, 2021. 05. 07. 327 (часть II). Ст. 5351.
2. Федеральный закон «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» от 29.11.2012 № 207-ФЗ [Электронный ресурс]. - URL: http://www.consultant.ru/document/cons_doc_LAW_138322/ (дата обращения: 15.11.2021).
3. Состояние преступности в России за январь-декабрь 2020 г. [Электронный ресурс]. - URL: <https://мвд.рф/reports/item/22678184/> (дата обращения: 16.11.2021).
4. Число дел о мошенничестве рекордно выросло на фоне пандемии. [Электронный ресурс]. - URL: <https://www.rbc.ru/society/31/08/2020/5f48ea169a79477e21e25d9d> (дата обращения: 12.11.2021).
5. Генпрокуратура: три четверти мошенничеств в России совершаются онлайн [Электронный ресурс]. - URL: https://tass.ru/interviews/11435813?utm_source=yxnews&utm_medium=desktop (дата обращения: 18.11.2021).
6. Прийти в платформу: в России появился ресурс для борьбы с мошенниками [Электронный ресурс] URL: https://iz.ru/1166990/anna-kaledina/priiti-v-plattformu-v-rossii-poiavilsia-resurs-dlia-borby-s-moshennikami?utm_source=yxnews&utm_medium=desktop (дата обращения: 18.11.2021).
7. Антонян, Ю.М. Криминология: Учебник для бакалавров / Ю.М. Антонян. - 2-е изд. перераб. и доп. - М.: Издательство Юрайт, 2014. - 388 с.
8. Положение Банка России от 09.06.2012 N 382-П (ред. от 07.05.2018) «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств» (п.2.6.4– 2.14.5) // Вестник Банка России». 2012. 22.06. №32.

References

1. Ukaz Prezidenta RF ot 2 iyulya 2021 g. № 400 «O Strategii natsional'noy bezopasnosti Rossiyskoy Federatsii» // Sobraniye zakonodatel'stva RF, 2021. 05. 07. 327 (chast' II). St. 5351.
2. Federal'nyy zakon «O vnesenii izmeneniy v Ugolovnyy kodeks Rossiyskoy Federatsii i otdel'nyye zakonodatel'nyye akty Rossiyskoy Federatsii» ot 29.11.2012 № 207-FZ [Elektronnyy resurs]. - URL: http://www.consultant.ru/document/cons_doc_LAW_138322/ (data obrashcheniya: 15.11.2021).
3. Sostoyaniye prestupnosti v Rossii za yanvar'-dekabr' 2020 g. [Elektronnyy resurs]. - URL: <https://mvd.rf/reports/item/22678184/> (data obrashcheniya: 16.11.2021).
4. Chislo del o moshennichestve rekordno vyroslo na fone pandemii. [Elektronnyy resurs]. - URL: <https://www.rbc.ru/society/31/08/2020/5f48ea169a79477e21e25d9d> (data obrashcheniya: 12.11.2021).
5. Genprokuratura: tri chetverti moshennichestv v Rossii sovershayetsya onlayn [Elektronnyy resurs]. - URL: https://tass.ru/interviews/11435813?utm_source=yxnews&utm_medium=desktop (data obrashcheniya: 18.11.2021).
6. Priyti v platformu: v Rossii poyavilsya resurs dlya bor'by s moshennikami [Elektronnyy resurs] URL: https://iz.ru/1166990/anna-kaledina/priiti-v-plattformu-v-rossii-poiavilsia-resurs-dlia-borby-s-moshennikami?utm_source=yxnews&utm_medium=desktop (data obrashcheniya: 18.11.2021).
7. Antonyan, YU.M. Kriminologiya: Uchebnik dlya bakalavrov / YU.M. Antonyan. - 2-ye izd. pererab. i dop. - M.: Izdatel'stvo Yurayt, 2014. - 388 s.
8. Polozheniye Banka Rossii ot 09.06.2012 N 382-P (red. ot 07.05.2018) «O trebovaniyakh k obespecheniyu zashchity informatsii pri osushchestvlenii perevodov denezhnykh sredstv i o poryadke osushchestvleniya Bankom Rossii kontrolya za



soblyudeniym trebovaniy k obespecheniyu zashchity informatsii pri osushchestvlenii perevodov denezhnykh sredstv" (p.2.6.4– 2.14.5) // Vestnik Banka Rossii". 2012. 22.06. №32.

КОСТЮК Михаил Федорович, профессор кафедры экономических и финансовых расследований Высшей школы государственного аудита (факультета) МГУ имени М.В. Ломоносова, доктор юридических наук, профессор. 119992, г. Москва, ул. Воробьевы горы, МГУ. E-mail: kost-mf@yandex.ru

КУНЦ Елена Владимировна, ведущий научный сотрудник ФКУ НИИ ФСИН России, доктор юридических наук, профессор. 125130, г. Москва, ул. Нарвская, 15А, стр. 1. E-mail: 73kuntc@mail.ru

KOSTYUK Mikhail Fedorovich, Professor of the Department of Economic and financial investigations of the Graduate School of State Audit (faculty) of the Moscow State University named after M.V. Lomonosov, Doctor of Law, Professor. 119992, Moscow, st. Sparrow Hills, Moscow State University. E-mail: kost-mf@yandex.ru

KUNTS Elena Vladimirovna, Leading Researcher, PKU Research Institute of the Federal Penitentiary Service of Russia, Doctor of Law, Professor. 125130, Moscow, st. Narva, 15A, p. 1. E-mail: 73kuntc@mail.ru

