

УДК 343.9

DOI <https://doi.org/10.17308/vsu.proc.law.2021.2/3404>

**ПРОФИЛАКТИКА ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ  
С ДИСТАНЦИОННЫМИ МОШЕННИЧЕСТВАМИ,  
ОСУЩЕСТВЛЯЕМАЯ ОВД РФ**

**М. С. Сирик**

*Филиал Кубанского государственного университета (г. Тихорецк)*

**А. Г. Озерская**

*Отдел МВД России по Тихорецкому району,  
филиал Кубанского государственного университета (г. Тихорецк)*

Поступила в редакцию 8 апреля 2021 г.

**Аннотация:** рассматриваются основные профилактические мероприятия, проводимые в настоящее время сотрудниками ОВД РФ с учетом имеющихся средств и возможностей, а также представлены направления деятельности, которые могут способствовать пресечению преступлений данной категории.

**Ключевые слова:** уголовная ответственность, дистанционное мошенничество, основные виды дистанционных мошенничеств, органы внутренних дел РФ, профилактика преступлений, связанных с дистанционными мошенничествами, технический прогресс.

**Abstract:** the article discusses the main preventive measures currently carried out by the police officers of the Russian Federation, taking into account the available means and capabilities, and also presents the areas of activity that I believe could contribute to the suppression of crimes of this category.

**Key words:** criminal liability, remote fraud, main types of remote fraud, internal affairs bodies of the Russian Federation, prevention of crimes related to remote fraud, technical progress.

За время карантина, связанного с эпидемией коронавируса, статистика преступности в России изменилась кардинально. Так, в 2020 г. число преступлений против личности уменьшилось на 5,1 %, в то время как количество преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, увеличилось на 73,4 % по сравнению с предыдущим годом. В общем числе зарегистрированных преступлений удельный вес преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, увеличился с 14,5 % в 2019 г. до 25,0 % в 2020 г. Больше половины таких преступлений (52,4 %) относится к категориям тяжких и особо тяжких: 267,6 тыс. (+87,5 %); больше половины (58,8 %) совершается с использованием сети «Интернет»: 300,3 тыс. (+91,3 %), почти половина (42,9 %) – средств мобильной связи: 218,7 тыс. (+88,3 %). За январь-февраль 2021 г. в Российской Федерации зарегистрировано на 29,4 % больше IT-пре-

ступлений, чем год назад, в том числе совершенных с использованием сети «Интернет» – на 48,3 % и при помощи средств мобильной связи – на 32,6 %. Если в январе-феврале 2020 г. удельный вес преступлений в IT-сфере составлял 19,3 %, то за первые 2 месяца текущего года он увеличился до 26,3 %. Рост преступности произошел в основном за счет телефонного и интернет-мошенничества. Телефонные онлайн-мошенники похитили у граждан более 150 млрд рублей<sup>1</sup>.

Согласно предоставленным данным только за 2020 г. на территории Краснодарского края зарегистрировано 19 000 преступлений, совершенных с использованием информационно-телекоммуникационных технологий, из них порядка 16 000 – это дистанционные мошенничества, кражи с банковской карты. На 100 тыс. населения в Краснодарском крае приходится около 300 преступлений<sup>2</sup>.

Уголовное законодательство РФ четко регламентирует ответственность за деяния в сфере дистанционного мошенничества. Ответственность за мошенническое использование электронных средств платежа наступает по ст. 159.3 УК РФ. Под мошенничеством в сфере компьютерной информации понимается хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей (ст. 159.6 УК РФ).

Так, приговором Новороссийского гарнизонного военного суда Краснодарского края от 21 мая 2020 г. № 1-22/2020 было установлено, что подсудимый М., незаконно воспользовавшись паспортом и мобильным телефоном своего сослуживца Р., посредством информационно-телекоммуникационной сети «Интернет» осуществил вход на сайт ООО МКК «Макро» (Moneza), на котором путем обмена уполномоченного работника названной кредитной организации оформил в электронном виде заявку на получение займа в размере 12 000 руб. якобы от имени Р., при этом сообщив оператору названной организации заведомо ложные сведения относительно личности заёмщика, в результате чего, обманным путем незаконно получил заём денежных средств в размере 12 000 руб. на имя Р., которыми распорядился по своему усмотрению, причинив указанному потерпевшему значительный ущерб. Подсудимый М. был признан виновным по ч. 2 ст. 159.3 УК РФ<sup>3</sup>.

Приговором Октябрьского городского суда Республики Башкортостан от 29 июля 2020 г. № 1-243/2020 подсудимая Д. была признана виновной в совер-

<sup>1</sup> Состояние преступности в России // Официальный сайт МВД России. URL: <https://xn--b1aew.xn--p1ai/folder/101762> (дата обращения: 06.04.2021).

<sup>2</sup> Интервью А. С. Бондарева // МК на Кубани. URL: <https://yandex.ru/turbo/kuban.mk.ru/s/social/2021/01/25/polkovnik-bondarev-rasskazal-kak-ne-poddat-sya-gipnozu-distancionnykh-moshennikov.html?prefetch=1> (дата обращения: 06.04.2021).

<sup>3</sup> Приговор Новороссийского гарнизонного военного суда Краснодарского края от 21 мая 2020 г. № 1-22/2020 по делу М. // Судебные и нормативные акты РФ. URL: <https://sudact.ru/> (дата обращения: 07.04.2021).

шении преступлений, предусмотренных п. «б», «в» ч. 3 ст. 159.6 и ч. 3 ст. 272 УК РФ. Было установлено, что Д., являясь специалистом офиса обслуживания и продаж в г. Октябрьский ПАО «Вымпелком», имея навыки работы в компьютерной программе «1С», ознакомившаяся с нормативными документами и требованиями по информационной безопасности, имея присвоенный индивидуальный и конфиденциальный логин и пароль, необходимый для работы в указанной компьютерной программе, содержащей персональные данные клиентов ПАО «Вымпелком» и персональные данные их лицевых счетов, которые охраняются Федеральным законом «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ, умышленно из корыстной заинтересованности, используя свое служебное положение, с целью неправомерного доступа к охраняемой законом компьютерной информации, содержащей персональные данные клиентов ПАО «Вымпелком» и персональные данные их лицевых счетов, с целью ее модификации, под своими индивидуальными и учетными данными осуществила доступ в компьютерную программу «1С», используемую сотрудниками ПАО «Вымпелком» для сервисного обслуживания абонентов оператора сотовой связи «Билайн», не имея соответствующего заявления клиента, выбрала абонентский номер, зарегистрированный на Ф.Ю.В., с привязанным к нему лицевым счетом, подделав заявление клиента на замену СИМ-карты, произвела перевыпуск СИМ-карты и модификацию компьютерной информации, получив возможность пользоваться лицевым счетом с находящимися на нем деньгами, принадлежащими ПАО «Вымпелком». Продолжая осуществлять свой преступный замысел, Д. умышленно из корыстных побуждений модифицировала компьютерную информацию, используя выпущенную СИМ-карту и свой сотовый телефон, с лицевого счета абонента в сети «Интернет» оплатила несколько покупок, а также перевела на счет своей банковской карты деньги, тем самым совершив хищение денег в сумме 32414,83 рублей, принадлежащих ПАО «Вымпелком»<sup>4</sup>.

Несомненно, преступность – это крайне негативное явление, оказывающее влияние на социально-экономическое состояние общества. Профилактика правонарушений – это одна из важнейших государственных задач. Правовую основу профилактики правонарушений составляет Федеральный закон от 23 июня 2016 г. № 182-ФЗ «Об основах системы профилактики правонарушений в Российской Федерации»<sup>5</sup>. Осуществление ОВД РФ надлежащей и своевременной профилактики правонарушений, связанных с дистанционными мошенничествами, представляет собой очень важное значение, которое с каждым годом только набирает свою актуальность и практическую значимость.

Исходя из официальной статистики, дистанционное мошенничество разделяется на мошенничество:

- осуществляемое через сеть «Интернет»;
- осуществляемое посредством использования мобильной связи<sup>6</sup>.

<sup>4</sup> Приговор Октябрьского городского суда Республики Башкортостан № 1-243/2020 от 29 июля 2020 г. // Судебные и нормативные акты РФ. URL: <https://sudact.ru/> (дата обращения: 07.04.2021).

<sup>5</sup> URL: <http://www.pravo.gov.ru> (дата обращения: 07.04.2021).

<sup>6</sup> См.: *Efremova M. A. Computer fraud // European Science Review. 2015. № 1/2. С. 126–128.*

Не является секретом, что основными жертвами «дистанционных мошенников» становятся либо пожилые граждане, либо молодежь в силу своей неопытности и повышенной доверчивости, которые представляют для злоумышленников наиболее «привлекательные объекты» для их преступной деятельности.

ОВД РФ в качестве профилактических действий по противодействию «дистанционным мошенничеств» применяются следующие направления деятельности:

– максимально возможное сокращение временных интервалов с момента совершения преступлений по исполнению запросов ОВД РФ. Оперативность осуществления межведомственного взаимодействия в области профилактики «дистанционных мошенничеств» представляет собой один из ключевых моментов, поскольку любое преступление эффективнее раскрывается «по горячим следам»;

– создание в ОВД РФ «специализированных отделов», которые занимались бы только раскрытием и расследованием преступлений, связанных с дистанционными мошенничествами. Соответственно, в небольших территориальных отделах ОВД РФ закрепление за расследованием уголовных дел, связанных с дистанционными мошенничествами, должно осуществляться следователем (дознавателем), специально закрепленным за данным направлением и изучившим методику расследования данной категории преступлений;

– эффективное выявление фактов продажи «sim-карт» в неофициальных торговых точках, без процедуры оформления на конкретное лицо, так как именно такие «безымянные sim-карты», как правило, и используются для осуществления разного рода преступлений, связанных с дистанционными мошенничествами. Впоследствии, в ходе расследования данной категории преступлений, следователь получает ответ от мобильного оператора, что предоставить информацию о принадлежности абонентского номера, используемого мошенником, не представляется возможным, что становится причиной неустановления лица, причастного к совершению данного преступления, и продолжение им дальнейшей преступной деятельности;

– осуществление блокировки любого типа «интернет-сети» в учреждениях для лиц, содержащихся под стражей, так как значительная часть преступлений данной категории совершается осужденными и отбывающими наказание в местах лишения свободы;

– дальнейшее ужесточение контроля за незаконным проносом в учреждения, используемые для лиц, содержащихся под стражей, sim-карт, сотовых телефонов и иных средств для осуществления связи через интернет-коммуникации;

– установление запрета на возможность получения микрозаймов, кредитов по сети «Интернет», без фактического удостоверения личности гражданина, его состояния в момент взятия финансовой услуги, установления его платежеспособности и предоставления документов, удостоверяющих личность;

– проведение периодических разъяснительных бесед и публикации в средствах массовой информации, на официальных сайтах региональных управлений МВД России сюжетов с подробным описанием методик работы мошенников, которые постоянно обновляются и приобретают новые формы.

Однако представленными выше мероприятиями тематика осуществления надлежащей профилактики преступлений, связанных с дистанционными мошенничествами, не заканчивается, поскольку данный вопрос носит многогранный характер и содержание, а также появляются новые виды дистанционных мошенничеств.

Несмотря на тот факт, что в настоящее время ОВД РФ применяются все меры профилактики «дистанционных мошенничеств», эта проблематика должна также получить и свое дальнейшее институциональное развитие, которое должно выражаться в следующем<sup>7</sup>:

– для осуществления профилактики «дистанционных мошенничеств» должны привлекаться сотрудники экспертно-криминалистических подразделений, обладающих определенными познаниями в рассматриваемой области;

– необходимо осуществлять дальнейшую выработку методических рекомендаций по противодействию всем видам «дистанционных мошенничеств»;

– все имеющиеся и известные виды «дистанционных мошенничеств», должны быть положены в основу общедокументальных методических рекомендаций по осуществлению надлежащей профилактики такого рода незаконных деяний;

– наконец, все вновь выявленные и новые виды «дистанционных мошенничеств» должны получать свою надлежащую правовую интерпретацию, чтобы ОВД РФ могли надлежащим образом противодействовать данным видам незаконных деяний и разрабатывать эффективную методику их расследования.

Мы поддерживаем мнение М. А. Яковлевой, что «с целью эффективной деятельности по профилактике киберпреступлений со стороны органов внутренних дел России следует оптимизировать систему профессионального обучения на юридических факультетах учебных заведений, включая образовательные организации системы МВД России, обеспечить обучение действующих сотрудников ОВД России (переподготовка и повышение квалификации), осуществляющих деятельность по профилактике и расследованию киберпреступлений с учетом правовой природы, темпов генезиса и специфики профилактики и расследования преступлений»<sup>8</sup>.

Итак, осуществление надлежащей профилактики преступлений, связанных с дистанционными мошенничествами, осуществляющееся ОВД РФ, позволяет значительным образом снизить их количество.

---

<sup>7</sup> См.: Кудрявцев Р. В. Организация деятельности по раскрытию дистанционных мошенничеств // Молодой ученый. 2019. № 24 (262). С. 218–221.

<sup>8</sup> Яковлева М. А. Органы внутренних дел как один из субъектов в системе профилактики преступности : дис. ... канд. юрид. наук. СПб., 2019. С. 77.

Вместе с тем преступления, связанные с дистанционными мошенничествами, должны и далее «профилактироваться» ОВД РФ, поскольку «дистанционные мошенники» постоянно совершенствуют свои криминальные как «навыки», так и «способы» их осуществление.

### Библиографический список

*Efremova M. A.* Computer fraud // European Science Review. 2015. № 1/2. P. 126–128.

Интервью Бондарева А. С. // МК на Кубани. URL: <https://yandex.ru/turbo/kuban.mk.ru/s/social/2021/01/25/polkovnik-bondarev-rasskazal-kak-ne-poddatsya-gipnozu-distancionnykh-moshennikov.html?prefetch=1>

*Кудрявцев Р. В.* Организация деятельности по раскрытию дистанционных мошенничеств // Молодой ученый. 2019. № 24 (262). С. 218–221.

*Яковлева М. А.* Органы внутренних дел как один из субъектов в системе профилактики преступности : дис. ... канд. юрид. наук. СПб., 2019.

### References

*Efremova M. A.* Computer fraud // European Science Review. 2015. № 1/2. P. 126–128.

Interview with Bondarev A. S. // МК на Kubani. URL: <https://yandex.ru/turbo/kuban.mk.ru/s/social/2021/01/25/polkovnik-bondarev-rasskazal-kak-ne-poddatsya-gipnozu-distancionnykh-moshennikov.html?prefetch=1>

*Kudryavtsev R. V.* Organization of activities for the disclosure of remote fraud // Young scientist. 2019. No. 24 (262). P. 218–221.

*Yakovleva M. A.* Internal affairs bodies as one of the subjects in the system of crime prevention : dissertation ... Candidate of Legal Sciences. SPb., 2019.

*Филиал Кубанского государственного университета (г. Тихорецк)*

*Сирик М. С., кандидат юридических наук, доцент, заведующая кафедрой уголовного права, процесса и криминалистики*

*E-mail: sirik-marina@yandex.ru*

*Branch of the Kuban State University (Tikhoretsk)*

*Sirik M. S., Candidate of Legal Sciences, Associate Professor, Head of the Criminal Law, Process and Criminalistics Department*

*E-mail: sirik-marina@yandex.ru*

---

246

*Отдел МВД России по Тихорецкому району, филиал Кубанского государственного университета (г. Тихорецк)*

*Озерская А. Г., старший дознаватель, старший преподаватель кафедры уголовного права, процесса и криминалистики*

*E-mail: oz.ali@bk.ru*

*Department of the Russian Ministry of Internal Affairs for the Tikhoretsky District, Branch of the Kuban State University (Tikhoretsk)*

*Ozerskaya A. G., Senior Investigator, Senior Lecturer of the Criminal Law, Process and Criminalistics Department*

*E-mail: oz.ali@bk.ru*