Научная статья
Научная специальность
5.1.4 «Уголовно-правовые науки (юридические науки)»

УДК 343.727
DOI https://doi.org/10.26516/2071-8136.2025.3.101

ПРАКТИКА РЕАГИРОВАНИЯ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ НА ЗАЯВЛЕНИЯ О ТЕЛЕФОННЫХ МОШЕННИЧЕСТВАХ. ВЫБОРОЧНОЕ ИССЛЕДОВАНИЕ

© Скобликов П. А., 2025
Институт государства и права РАН, г. Москва, Россия

Рассматривается такая разновидность преступлений, совершаемых с использованием информационных технологий, как телефонные мошенничества. Отмечается, что в текущий период они получили широкое распространение в России и составляют для нашего общества острейшую криминальную проблему. Представлены результаты выборочного исследования практики рассмотрения и разрешения в правоохранительных органах заявлений о названных деяниях. Описаны типичные недостатки данной практики и нарушения процессуальных норм, с которыми могут столкнуться потерпевшие. Показаны последствия ненадлежащего реагирования на заявления о телефонных мошенничествах, предложены рекомендации для потерпевших и их представителей в уголовном процессе, нацеленные на улучшение положения потерпевших и минимизацию вреда.

Ключевые слова: телефонное мошенничество, укрытие преступлений, потерпевший, рассмотрение заявления о преступлении, информационно-коммуникационные технологии, неоконченное покушение, отказ в возбуждении уголовного дела.

PRACTICE OF LAW ENFORCEMENT RESPONSE TO REPORTS OF TELEPHONE FRAUD. A SELECTIVE STUDY

© Skoblikov P. A., 2025
Institute of State and Law Russian Academy of Sciences, Moscow, Russian Federation

The article examines telephone fraud as a type of crime committed using information technology. Currently, these crimes have become widespread in Russia and represent a critical criminal problem for our society. The paper presents the results of a selective study of how law enforcement agencies handle reports of such offenses. It describes typical shortcomings in this practice and procedural violations that victims may encounter. The consequences of inadequate response to telephone fraud reports are analyzed, and recommendations are proposed for victims and their representatives in criminal proceedings, aimed at improving victims' position and minimizing harm.

Keywords: telephone fraud, concealment of crimes, victim, consideration of crime reports, information and communication technologies, attempted offense, refusal to initiate criminal proceedings.

Введение

Пожалуй, самый резонансный криминальный феномен, который более других будоражил российское общество в 2024 г., – изощренные, масштабные и часто успешные атаки телефонных мошенников; лишь немногим удалось их избежать. Это сквозная тема года, крещендо, которое достигло пика в декабре. Напомним несколько знаковых событий конца 2024 г., чтобы через их связку обрисовывать масштаб и глубину проблемы.

В конце ноября 2024 г. руководитель аппарата Правительства РФ Д. Григоренко сообщил представителям СМИ, что в Правительстве были детально проанализированы наиболее распространенные *мошеннические схемы, включая обман через звонки и сообщения*, взломы личных кабинетов и оформление кредитов на чужие паспорта. На основе этого анализа разработаны меры для защиты граждан. В результате их реализации потенциальным потерпевшим станет доступен широкий набор инструментов, который поможет им обезопасить себя от телефонного и интернет-мошенничества[1].

[1] См., напр.: Капранов О. Кабмин разработал пакет мер по борьбе с телефонным и интернет-мошенничеством // Российская газета. 2024. 26 нояб.

19 декабря 2024 г. Президент России В. В. Путин в прямом эфире подвел итоги года и ответил на вопросы журналистов и жителей страны. При этом значительное время было уделено вопросам *противодействия телефонному и иному мошенничеству*, совершаемому с использованием информационно-коммуникационных технологий. «Объемы этого жульничества зашкаливают», – заявил глава государства[1].

20 декабря 2024 г. тема *борьбы с телефонным мошенничеством* поднималась в Совете Федерации РФ, когда в соответствии с ч. 3 ст. 129 Конституции РФ была представлена кандидатура на должность Генерального прокурора РФ. В качестве таковой Президент России на новый срок выдвинул действующего Генерального прокурора И. В. Краснова. Описывая уже предпринятые меры по борьбе с телефонным мошенничеством, последний обратил внимание сенаторов, что Генпрокуратура России добилась введения компаниями – операторами сотовой связи антифрод-систем. Кроме того, эти компании стали привлекать к ответственности за пропуск так называемого подменного трафика. В результате было пресечено более 1,2 млрд звонков телефонных мошенников. Но, безусловно, этого недостаточно, признал И. В. Краснов. С участием Генпрокуратуры приняты законодательные акты по ограничению анонимных симкарт, обманных банковских операций и по другим важным направлениям работы. «В пределах нашей компетенции мы стараемся находить новые методы борьбы с телефонным мошенничеством», – заявил Генеральный прокурор[2].

22 декабря 2024 г. информационное агентство ТАСС со ссылкой на правоохранительные органы сообщило, что в Москве и Московской области за минувшие сутки зафиксировано более 10 поджогов банкоматов и взрывов пиротехнических изделий в общественных местах. Злоумышленники, среди которых преобладают пенсионеры, действовали по заданию телефонных мошенников, от которых они же ранее финансово пострадали[3].

23 декабря 2024 г. издание «Ведомости», обобщая события нескольких предшествующих суток, сообщило, что в столице, Подмосковье и г. Санкт-Петербурге «россияне устраивали поджоги и взрывы пиротехники в общественных местах». В торговых центрах, банках и отделениях почты они бросали петарды и бутылки с зажигательной смесью, а на улицах пытались поджечь полицейские автомобили. К преступлениям граждан склонили телефонные мошенники. Зафиксировано два десятка таких случаев. Провокаторы связываются с людьми, у которых они уже похитили деньги, и обещают вернуть похищенное, если первоначальные жертвы совершат противоправные действия[4].

24 декабря 2024 г. издание «Коммерсантъ» сообщило со ссылкой на источники в операторах связи и на телеком-рынке (и эту информацию растиражировали иные СМИ), что в Минцифре[5] и Роскомнадзоре из-за роста активности мошенников в мессенджерах обсуждается введение новых ограничений. Рассматривается как полная блокировка голосовых вызовов в таких приложениях, так и частичный запрет, под который подпадут звонки из-за границы. Сейчас, по оценкам операторов связи, около 40 % вызовов в мессенджерах совершают мошенники, а среди таких звонков 70 % поступают из-за рубежа[6].

25 декабря 2024 г. председатель Госдумы Федерального собрания Российской Федерации В. В. Володин сообщил в своем телеграм-канале, что для защиты граждан от мошенников разработан и внесен в Госдуму законопроект, которым предлагается установить при выдаче кредита «период охлаждения», в течение которого не будут осуществляться финансовые операции. Это время люди смогут использовать для более тщательного анализа своих действий и, если поймут или заподозрят, что стали жертвой телефонных мошенников, смогут своевременно обратиться в полицию. Володин указал, что ранее в комментариях читатели телеграм-канала обращали внимание на необходимость решать проблему телефонного мошенничества, и пообещал, что законопроект будет рассмотрен в приоритетном порядке[7].

[1] См.: Итоги года с Владимиром Путиным // Официальный сайт Президента России. 19.12.2024. URL: http://www.kremlin.ru/events/president/transcripts/75909 (дата обращения: 01.01.2025).

[2] См.: Стенограмма 582-го заседания Совета Федерации // Официальный сайт Совета Федерации Федерального Собрания Российской Федерации. URL: http://council.gov.ru/activity/meetings/163102/transcript/ (дата обращения: 01.01.2025).

[3] См.: В Московском регионе за сутки совершили более 10 поджогов и взрывов // ТАСС. 2024. 22 дек. URL: https://tass.ru/proisshestviya/22742441 (дата обращения: 03.01.2025).

[4] См.: Дорофеева Е., Никольский А. В Москве и Петербурге прошла серия поджогов и взрывов банкоматов. В стране зафиксирована «самая массовая волна воздействия мошенников», отметили в МВД // Ведомости. 2024. 23 дек. URL: https://www.vedomosti.ru/society/articles/2024/12/23/1083034-rossiiskie-pensioneri-ustroili-podzhogi-i-vzrivi-bankomatov?from=copy_text (дата обращения: 03.01.2025).

[5] Министерство цифрового развития и массовых коммуникаций Российской Федерации.

[6] См.: Жабин А. Коллективная ответственность топ-мессенджеров // Коммерсантъ. 2024. 24 дек. С. 1.

[7] См.: Володин В. В. О борьбе с телефонными мошенниками // Телеграмм-канал «Вячеслав Володин». 25.12.2025. URL: https://t.me/vv_volodin/970 (дата обращения: 25.12.2025).

26 декабря 2024 г. Правительство РФ издало постановление № 1898, нацеленное на ограничение телефонного мошенничества. Именно так это постановление охарактеризовано на официальном сайте органа. Там указано, что в дальнейшем не будет выдаваться лицензия на передачу интернет-данных с наложением голосовой информации. Она давала возможность с помощью интернета выходить на связь с человеком, использующим стационарную телефонную или мобильную сети связи. Чаще всего такими технологиями пользовались мошенники, поскольку это позволяло подменять номера[1].

Итак, что следует из изложенного? Государство принимает и продолжит принимать широкий набор мер, направленных на профилактику телефонного мошенничества – путем затруднения деятельности телефонных мошенников и просвещения их потенциальных жертв, чтобы уберечь последних от неосторожных действий.

Данные меры важны и необходимы, они способны предупредить некоторую часть анализируемых здесь преступлений. Если меры хорошо продуманы, своевременны и масштабны, то *удастся предупредить значительную часть, но далеко не все такие преступления.*

Этот итог предопределен общими закономерностями противоборства. Если тот, на кого нападают, лишь защищается, уклоняясь от ударов, пытаясь смягчить их силу, но сам не наносит урон противнику, то первый обречен нести потери, а второй будет иметь больший или меньший успех (в нашем случае получать материальную выгоду) и не иметь мотивов к прекращению своей деятельности.

Вот почему необходимо устанавливать и привлекать телефонных мошенников к уголовной ответственности, назначать им эффективное наказание. Лишь в этом случае они станут нести урон, что будет способствовать не только общему, но и специальному предупреждению новых преступлений. У подвергнутых наказанию и находящихся в изоляции лиц утрачивается возможность продолжать преступную деятельность и снижается мотивация к ее возобновлению после освобождения из мест лишения свободы. Кроме того, на их удручающем примере некоторая часть других потенциальных или уже состоявшихся преступников воздержится от начала либо продолжения криминальной карьеры.

Еще одно важное обстоятельство, которое надо принять во внимание, – возбуждение уголовных дел и привлечение к уголовной ответственности телефонных мошенников создает условия для возвращения похищенных средств и (или) возмещения пострадавшим причиненного ущерба за счет имущества виновных, а также для получения страхового возмещения, если имущество пострадавших было застраховано, а хищение входит в число страховых случаев.

Основная масса телефонных мошенничеств выявляется посредством рассмотрения заявлений пострадавших. Какова же практика рассмотрения таких заявлений в правоохранительных органах? Этой теме и посвящена настоящая работа.

1. Анализ практики рассмотрения заявлений о телефонных мошенничествах на основе официальных данных

Опираясь на находящиеся в открытом доступе официальные данные, сложно составить представление о ходе и результатах рассмотрения в правоохранительных органах заявлений о телефонных мошенничествах. Это обусловлено рядом обстоятельств: ограниченностью перечня статистических данных, несовершенством учетных форм и отсутствием в открытом доступе значительной части имеющегося в правоохранительных органах массива статданных.

Сведения о количестве заявлений и других сообщений о преступлениях, поступивших в органы внутренних дел[2], учитываются там вместе со сведениями об административных правонарушениях, о происшествиях. Для их учета используется общая учетная форма – **Книга учета заявлений и сообщений о преступлениях, об административных правонарушениях, о происшествиях (КУСП)**, и дифференциация заявлений в ней при регистрации не проводится[3]. Вместе с тем до определенного времени у заинтересованных лиц имелась возможность

[1] См.: Правительство утвердило постановление для ограничения телефонного мошенничества // Официальный сайт «Правительство России». 2024. 28 дек. URL: http://government.ru/news/53879/ (дата обращения: 04.01.2025).

[2] Органы внутренних дел выявляют и расследуют подавляющее большинство всех зарегистрированных в стране преступлений. Так, в 2021 г. ими выявлено 93,2 % от общего числа зарегистрированных в России преступлений, в 2022 г. – 93,1 %; в 2023 г. – 92,8 %. Согласно ст. 151 УПК РФ основная подследственность мошенничеств отнесена к органам дознания и предварительного следствия МВД России, поэтому применительно к телефонным мошенничествам роль органов внутренних дел в их выявлении и расследовании должна быть еще более значительной.

[3] См.: Приказ МВД России от 29 авг. 2014 г. № 736 (ред. от 09.10.2019) «Об утверждении Инструкции о порядке приема, регистрации и разрешения в территориальных органах Министерства внутренних дел Российской Федерации заявлений и сообщений о преступлениях, об административных правонарушениях, о происшествиях» (далее – Инструкция о ведении КУСП).

ознакомиться со сведениями о том, сколько заявлений и других сообщений о преступлениях (в сумме) рассмотрено в порядке, предусмотренном ст. 144 УПК РФ[1].

Но и эти сведения давали весьма приблизительное представление об активности лиц, пострадавших от преступлений, поскольку, во-первых, помимо заявлений о преступлениях, поступивших от граждан и юридических лиц, поводом к возбуждению являются сообщения о преступлениях, полученные из других источников (например, из СМИ). А во-вторых, некоторые заявления о преступлениях не рассматривались (и не рассматриваются) правоохранителями в качестве таковых; соответственно, по ним не выносятся процессуальные решения, предусмотренные ст. 145 УПК РФ[2]. Такие заявления в статистике не отражаются[3], а описанные в них преступления (если заявители не ошибаются в своих оценках), по факту, укрываются.

Но и эти приблизительные данные в решении нашей задачи не могли бы помочь, потому что оставалось бы неясным, какова доля заявлений о телефонных мошенничествах в общем массиве сообщений о преступлениях, кем и в какие сроки они рассматривались, какие мероприятия и следственные действия с целью проверки заявлений предпринимались, как осуществлялось взаимодействие с заявителями, как распределялись доли принятых процессуальных решений по заявлениям, какие жалобы и кому подавали заявители, неудовлетворенные реакцией на их сообщения о преступлениях, и какие решения по таким жалобам выносились.

Описанное положение повышает ценность полевых исследований, изучения и анализа материалов, информации, которыми располагают лица, представившие в правоохранительные органы заявления о телефонных мошенничествах.

2. Описание исследования

Выборочное и углубленное исследование, проведенное нами в 2018–2024 гг., позволяет, в качестве предварительного результата, в основных чертах изложить фактический порядок реагирования органов МВД России на заявления граждан, в отношении которых неизвестные лица пытались совершить так называемые телефонные мошенничества.

Термин «телефонное мошенничество» мы используем в широком смысле, подразумевая под ним деяние, направленное на завладение чужим имуществом путем обмана или злоупотребления доверием, при совершении которого ключевую роль играет использование телефона как средства голосовой или текстовой коммуникации преступника с жертвой. Такая коммуникация упрощает вступление в контакт с жертвой, облегчает ее обман и повышает безопасность преступника, позволяет существенно оптимизировать преступную деятельность.

Прежде чем обрисовать обнаруженный порядок реагирования правоохранительных органов, уместно сделать несколько пояснений. Данное небольшое исследование проводилось путем опроса граждан, изучения предоставленных ими документов, а также посредством использования методов включенного наблюдения и правового эксперимента.

Во всех изученных случаях к пострадавшим гражданам по мобильной или фиксированной телефонной связи, через мессенджеры обращались некие лица, которые располагали более или менее полным набором персональных данных о гражданах, выдавали себя за представителей различных финансовых или коммерческих организаций, должностных лиц государственных органов либо представлялись известными в той или иной сфере деятельности персонами. Далее разыгрывались разные сценарии, направленные

[1] Эти данные приводились в сборнике «Состояние преступности в России», в разделе «Сведения о результатах разрешения заявлений, сообщений и иной информации о происшествиях в органах внутренних дел». Сборник регулярно публикуется на официальном сайте «Министерство внутренних дел Российской Федерации». Указанный раздел наличествовал в нем до 2014 г. включительно, но затем был оттуда удален. См. URL: https://xn--b1aew.xn--p1ai/reports/ (дата обращения: 05.01.2025).

[2] Процессуальный закон допускает лишь три решения по заявлению о преступлении: 1) возбудить уголовное дело; 2) отказать в возбуждении уголовного дела; 3) передать заявление по подследственности или подсудности. Однако следует иметь в виду, что практика выработала квазипроцессуальное решение четвертого вида, и оно закреплено в ведомственном нормативном акте – о приобщении заявления к материалам ранее зарегистрированного заявления о том же преступлении (подробнее см. п. 48 Инструкции о ведении КУСП). Причем органы прокуратуры и суды, несмотря на формальное противоречие процессуальному закону, поддерживают такие решения, если для них усматриваются достаточные фактические основания.

[3] Эта проблема, в частности, затронута в статье Ю. Бойцова «Административный произвол органов следствия. Метод игнорирования заявлений потерпевших СК РФ, его причины и возможности устранения», опубликованной в 2021 г. на сайте журнала «Уголовный процесс». Там описана ситуация, в которой юридическое лицо представило в подразделение МВД России заявление о преступлении. Орган дознания пришел к выводу, что деяние, описанное в заявлении, содержит признаки преступления, последственного другому ведомству – Следственному комитету РФ (СК РФ), и направил заявление с проверочным материалом для принятия решения по подследственности. Однако в подразделении СК РФ не стали рассматривать данное сообщение в порядке ст. 144 УК РФ и не приняли по нему процессуальное решение со ссылкой на то, что поступившие материалы не указывают на признаки преступления. См.: URL: https://www.ugpr.ru/article/1912-administrativnyy-proizvol-organov-sledstviya-metod-ignorirovaniya-zayavleniy-poterpevshih-sk (дата обращения: 05.01.2025).

на то, чтобы побудить граждан предоставить какие-то сведения – о себе и организации, в которой работают, совершить какие-то действия финансового и иного характера и др.

Высока вероятность, что в каждом таком случае против граждан совершено и закончено преступление, предусмотренное ч. 2 ст. 272 УК РФ[1], – неправомерный доступ к охраняемой законом компьютерной информации, поскольку деяние повлекло копирование информации и совершено с корыстной целью (это может объяснить, каким образом неизвестные завладели персональными данными граждан), и (или) другое преступление, предусмотренное ст. 137 «Нарушение неприкосновенности частной жизни» УК РФ. Кроме того, в большинстве указанных случаев усматриваются признаки покушения на мошенничество либо иные преступления, которые не были доведены до конца по не зависящим от посягающего лица обстоятельствам (ч. 3 ст. 30 УК РФ), – а следовательно, виновные должны нести уголовную ответственность, даже если не причинили материальный ущерб потерпевшим.

Кто-то из потерпевших в изученных случаях обращался в правоохранительные органы, оформив соответствующее заявление на бумаге и отправив его традиционной почтой. Иные, в целях быстроты доставления и рассмотрения, отправляли свои заявления по электронной почте или через интернет-сайт правоохранительного органа, заполнив там специальную форму. Граждане обращались с данными заявлениями в правоохранительные органы разного уровня и ведомственной принадлежности – к руководству МВД России, к руководству управлений (главных управлений) МВД России по соответствующему субъекту РФ, к руководству специализированного управления «К» МВД России и др. У заявлений была разная степень проработанности; часть из них тщательно выверялась с помощью подготовленного юриста, имеющего опыт оперативно-следственной работы. Действия злоумышленников анализировались, им давалась правовая оценка. К заявлениям прилагались копии состоявшихся переписок, аудиофайлы с речами злоумышленников, справки от мобильного оператора и провайдера об имевших место соединениях (с кем, когда, по чьей инициативе) и т. д. В резолютивной части заявлений некоторые граждане формулировали ходатайства о проведении целесообразных и неотложных, с их точки зрения, проверочных и следственных действий, оперативно-разыскных мероприятиях, об установлении иных потерпевших и сопоставлении полученных данных с тем, что изложены в заявлении и т. д.

3. Обычные результаты обращений и их негативные последствия

Все обозначенные в предыдущем разделе вариации обращений не влияли на конечный результат, он был единообразным: после прохождения длительной административной процедуры (занимавшей несколько недель) все заявления поступали в отделы полиции по месту жительства подавших заявления граждан, их рассмотрение поручалось участковым уполномоченным полиции. В свою очередь, последние оформляли письменные объяснения граждан (которые в основном дублировали сведения, изложенные в заявлениях) либо справки о том, что с гражданами не удалось связаться, а *затем по надуманным основаниям выносили постановления об отказе в возбуждении уголовного дела.* В отдельных случаях прокуроры, в рамках надзора за соблюдением установленного порядка разрешения заявлений и сообщений о совершенных и готовящихся преступлениях, инициативно отменяли постановления об отказе в возбуждении уголовного дела и назначали дополнительную проверку. Однако такая проверка выражалась, как правило, лишь в отобрании от заявителей дополнительных объяснений, затем повторно выносились постановления об отказе в возбуждении уголовного дела; о вынесении таких повторных постановлений заявители не извещались, их копии заявители не получали[2].

Это закономерный результат, поскольку участковые уполномоченные полиции не имеют необходимых познаний, умений, инструментов, полномочий и времени для доследственной проверки и расследования преступлений, тем более таких сложных, высокотехнологичных.

[1] Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (ред. от 31.07.2025) (с изм. и доп., вступ. в силу с 01.09.2025) // Гарант : справочная правовая система.

[2] Довольно давно в правоприменительной практике сложилась система приемов и уловок правоохранителей, направленных на противодействие возбуждению тех уголовных дел, которые по каким-то причинам представляются нежелательными. Среди таких приемов: нерегистрация в установленном порядке принятого заявления о преступлении; нерассмотрение принятого и зарегистрированного заявления о преступлении в установленном процессуальном порядке; неуведомление в установленном порядке заявителя о принятом процессуальном решении (о направлении заявления по подследственности либо об отказе в возбуждении уголовного дела); ненаправление или направление с большим опозданием заявителю копии постановления об отказе в возбуждении уголовного дела (что препятствует подготовке заявителем мотивированной жалобы на принятое решение) – согласно действующему закону такая копия должна быть направлена в течение 24 ч с момента вынесения соответствующего постановления, независимо от желания-нежелания заявителя. Подробнее о данных приемах см. [6].

Итак, *есть основания предполагать, что если в органы МВД России поступают заявления о преступлениях (либо покушениях на преступления), предусмотренных ст. 137, 272, 159, 159.3, 159.6 УК РФ, совершенных с использованием информационно-коммуникационных технологий, которые не причинили потерпевшим существенного материального ущерба, то работа по их проверке с привлечением оперативных работников, следователей и экспертов-криминалистов не проводится, методы оперативно-разыскной деятельности и цифровой криминалистики не применяются, следы преступлений не фиксируются, предварительное расследование не осуществляется; априори выносятся постановления об отказе в возбуждении уголовного дела.*

Описанная практика опасна не только тем, что происходит фактическое укрытие преступлений, а виновные получают возможность безнаказанно продолжать преступную деятельность (хотя это, конечно, главное). Нужно также указать на то, что участковые уполномоченные полиции отвлекаются от исполнения своих основных функций[1] и не оправдывают ожидания граждан на обслуживаемых участках. А также на то, что разъяснения прокуратуры[2] и обоснованные рекомендации специалистов[3] о том, кто и как должен расследовать киберпреступления, оказываются невостребованными – к следователям материалы попросту не попадают.

Не менее существенно то, что с высокой степенью вероятности заявители впредь не станут обращаться в правоохранительные органы за помощью, если вновь станут жертвами преступных атак, а кроме того, расскажут о своем негативном опыте родственникам и знакомым, которые сделают соответствующие выводы. Таким образом, *латентность рассматриваемых преступлений будет возрастать, равно как растут безопасность и привлекательность преступной деятельности в сфере высоких технологий. А еще увеличивается отчуждение граждан от государства, недоверие первых ко второму.*

4. Показательный пример из современной правоприменительной практики МВД России

Для более полного раскрытия темы настоящей статьи было бы полезным наглядно показать практику рассмотрения заявлений граждан о покушении на мошенничество с использованием информационно-коммуникационных технологий и о неправомерном доступе к компьютерной информации после появления в МВД России управления по организации борьбы с противоправным использованием информационно-коммуникационных технологий (УБК) МВД России, а также подразделений по борьбе с противоправным использованием информационно-коммуникационных технологий в территориальных органах МВД. Они созданы за счет штатной численности ликвидированного Управления «К»[4] Бюро специальных технических мероприятий и соответствующих подразделений на местах[5]. Это преобразование предопределено изданием Указа Президента РФ от 30 сентября 2022 г. № 688, согласно которому в структуре центрального аппарата МВД России и появилось УБК, которое отнесено к подразделениям полиции. Было разработано и принято Положение об этом Управлении[6].

УБК МВД России должно обеспечивать и осуществлять в пределах компетенции функции своего министерства *по выработке и реализации государственной политики и нормативно-правовому регулированию в области организации противодействия противоправным деяниям, совершаемым с использованием (либо в сфере) информационно-коммуникационных технологий*. В функции УБК МВД России также входит осуществление оперативно-разыскной деятельности в полном объеме, мониторинг и анализ оперативной обстановки, разработка мер по оперативному реагированию на ее изменение и мн. др.

[1] На условиях анонимности некоторые из них, проходящие службу в столичном регионе, пояснили, что в течение месяца им приходится проверять и разрешать несколько десятков заявлений о преступлениях, каждый раз вынося постановления об отказе в возбуждении уголовного дела. И это отнюдь не только и не столько заявления о киберпреступлениях; подобным образом канализируются зарегистрированные сообщения о любых преступлениях, которые по тем или иным причинам неудобны лицам, осуществляющим или контролирующим уголовно-процессуальную деятельность. Исследование о мотивах таких решений ранее было представлено в юридической литературе (см. [5]).

[2] Для примера сошлемся на материал, размещенный на официальном сайте правительства Свердловской области под заголовком «Особенности расследования уголовных дел в сфере информационных технологий. Разъясняет аппарат прокуратуры области». URL: https://midural.ru/normative_documents/100615/100629/page2/document166027/ (дата обращения: 09.10.2024).

[3] Из-за ограничений по объему настоящей статьи мы не имеем возможности назвать все публикации такого рода (их насчитываются уже сотни), но для наглядности приведем несколько [1–4; 7].

[4] Управление «К» создавалось по решению министра, в структуру центрального аппарата МВД России не входило, т. е. имело более низкий статус, нежели УБК МВД России, а также имело меньший объем функций и задач по сравнению с УБК МВД России.

[5] См.: приказ МВД России от 22 окт. 2022 г. № 812 и др.

[6] См.: Об утверждении Положения об Управлении по организации борьбы с противоправным использованием информационно-коммуникационных технологий Министерства внутренних дел Российской Федерации : приказ МВД России от 29 дек. 2022 г. № 1110.

Ну а далее представим показательный пример. Субботним утром 28 сентября 2024 г. на мобильный телефон гражданина П. поступил звонок с неизвестного ему номера с префиксом «918»[1]. Звонивший обратился к П. по имени-отчеству, а сам представился Беловым А. В., работником АО «Мосэнергосбыт». Белов (будем называть его так) известил, что в доме по месту жительства П. производится бесплатная («по федеральной программе») замена действующих индивидуальных электросчетчиков на трехтарифные. Для этого необходимо выбрать подходящий день и время, чтобы принять работника Мосэнергосбыта. Затем Белов попросил записать номер электросчетчика, который будет доставлен и подключен[2]. После этого он сообщил, что будет оформлен договор на установку электросчетчика, огласил дату рождения П. (привел ее точно)[3] и заявил, что помимо имеющихся данных гражданин должен указать свой СНИЛС. На вопрос «зачем?» Белов ответил, что новый счетчик будет оснащен сим-картой для автоматической передачи данных[4], поэтому нужны дополнительные персональные данные.

П., являющийся пенсионером МВД и имеющий опыт оперативной работы, спросил, принимает ли телефон, с которого позвонил Белов, входящие звонки. Белов ответил утвердительно и пригласил проверить. П. перезвонил, услышал голос Белова, и они ненадолго продолжили разговор. П. сказал Белову, что приезжать на адрес не следует, сначала необходимо проверить достоверность поступившей от него информации. После этого завершил разговор. П. тут же выяснил, что согласно открытым источникам номер, с которого позвонил Белов, зарегистрирован не в столичном регионе, а в Краснодарском крае. Затем П. позвонил в контактный центр АО «Мосэнергосбыт». Оператор пояснил, что на адресе П. замена электросчетчиков не проводится. Также оператор сообщил, что П. не первый, кто получил звонки от лжеработников Мосэнерогосбыта.

В тот же день П. подготовил заявление о преступлении и направил его через сайт МВД России в УБК. В заявлении описал приведенные выше факты и предположил, что дополнительные персональные данные, которые пытался выведать Белов, нужны для дальнейшей реализации преступной схемы. Например, для взлома личного кабинета жертвы на сайте «Госуслуги», последующего получения кредитов от имени жертвы и завладения полученными таким образом денежными средствами, либо завладения телефонным номером жертвы и получения посредством него доступа к банковским счетам и т. д.

В заявлении П. предложил свою правовую оценку происшедшего: имеет место совокупность двух преступлений. Первое из них – неоконченное покушение на мошенничество с целью хищения денежных средств в особо крупном размере (ч. 4 ст. 159 или ч. 4 ст. 159.3 УК РФ). Такая квалификация обоснована следующим. Исходя из обстоятельств происшедшего, умысел виновного был направлен на то, чтобы завладеть всеми денежными средствами, к которым удастся получить доступ. В таком случае деяние следует оценивать по наиболее тяжкому из возможных последствий, которые могли наступить в данном случае, но не наступили по не зависящим от виновного причинам. У потерпевшего благоприятная кредитная история, и при удачном для преступника развитии событий он мог бы оформить на потерпевшего кредит или кредиты на сумму более 1 млн руб. и завладеть кредитными средствами. Кроме того, на банковских счетах потерпевшего в сумме находилось более 1 млн руб. Поэтому виновному должно вменять-

[1] Вряд ли указанное время выбрано случайно. Если бы звонок поступил в будний день и в рабочее время, то высока вероятность, что трудоустроенный гражданин не отреагирует на звонок с незнакомого номера. Кроме того, в этот день и на следующий сотрудники правоохранительных органов отдыхают, на службе находятся лишь дежурные.

[2] Оглашение всех этих подробностей и концентрация внимания гражданина на них («запишите») призваны внушить потенциальной жертве, что действительно готовится замена электросчетчика, в то время как это лишь легенда, используемая для формирования доверия, выманивания конфиденциальной информации и побуждения жертвы к нужным мошеннику действиям.

[3] Демонстрация осведомленности о персональных данных жертвы также есть элемент подтверждения легенды мошенников по схеме, которая работает на психологическом уровне: «Вот видите, мы знаем ваши персональные данные – мы ими правомерно обладаем, ведь у нас с вами юридически значимый договор – будет нормальным эти данные уточнить и расширить их объем».

[4] Здесь следует заметить, что, действительно, в столице в рамках программы, утвержденной Департаментом экономической политики и развития г. Москвы, АО «Мосэнергосбыт» с 2019 г. совместно с подрядной организацией проводит работы по созданию системы беспроводного сбора данных показаний приборов учета электроэнергии. Однако персональный обзвон граждан в связи с этим не проводится. АО «Мосэнергосбыт» за 1–2 дня до начала работ извещает жителей домов о предстоящих работах путем расклейки объявлений в подъездах и на информационных стендах. Работники имеют при себе фирменное удостоверение и копию письма АО «Мосэнергосбыт» о проведении работ. См.: В Москве проводятся работы по установке «умных» счетчиков. Официальный сайт АО «Мосэнергосбыт». URL: https://www.mosenergosbyt.ru/individuals/news/v-moskve-provodyatsya-raboty-po-ustanovke-umnykh-schyetchikov/ (дата обращения: 29.10.2024). Чтобы выяснить эти подробности, подвергшийся мошеннической атаке гражданин должен взять паузу и заняться поиском информации. Между тем преступная схема рассчитана на то, что в ходе уже первого разговора мошенник решит намеченные задачи, а гражданин ничего не заподозрит и будет ожидать визита лжеработников АО «Мосэнергосбыт», которые якобы сделают режим потребления электроэнергии более удобным и экономным. На самом же деле личную встречу с гражданином преступная схема не предполагает.

ся покушение на мошенничество на сумму более 1 млн руб., что следует расценивать как особо крупный размер (прим. 1 к ст. 158 УК РФ).

Второе преступление окончено и предусмотрено ч. 2 ст. 277 УК РФ – неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло копирование информации и совершено с корыстной целью (только это может объяснить, откуда у мошенников обширные персональные данные о потерпевшем; возможно, преступники получили доступ к некой банковской базе данных).

П. обратил внимание правоохранителей в своем заявлении, что, по всей видимости, помимо заявителя Белов и его соучастники обзвонили ряд иных граждан, и некоторая часть из них повелась на уловки мошенников, сообщила все запрошенные данные и уже пострадала в финансовом плане либо в ближайшее время потерпит финансовый ущерб. Поэтому *следует принять незамедлительные меры к определению локации телефона, с которого звонил Белов, задержанию последнего*, закреплению цифровых и вещественных следов противоправной деятельности, установлению и опросу потенциальных потерпевших, выявлению сообщников Белова и т. д.

П. отслеживал судьбу заявления через ID, присвоенный при подаче обращения. Через два дня на сайте МВД России появилась информация, что заявление от П. 30 сентября 2024 г. зарегистрировано и находится на рассмотрении в ГУ МВД России по г. Москве. Еще через два дня появилась информация, что данное заявление зарегистрировано в КУСП.

Наконец, 14 октября 2024 г. П. позвонил сотрудник уголовного розыска из территориального отдела внутренних дел, обслуживающего район проживания заявителя. Сотрудник сообщил, что заявление поступило в указанный отдел и он отрабатывает его, поскольку находится на дежурстве. Сотрудник пригласил П. к себе для дачи объяснения. П. поинтересовался, специализируется ли сотрудник на раскрытии киберпреступлений. Последовал ответ, что принцип работы лично его и дежурной группы в целом не линейный, а территориальный, приходится разбираться с заявлениями обо всем, о грабежах, угонах, квартирных кражах и проч. После этого никаких известий для П. о результатах рассмотрения заявления о преступлении не поступало. Через четыре недели, предполагая, что принято решение об отказе в возбуждении уголовного дела и это решение скрывается (в противном случае П. был бы вызван к следователю или дознавателю на допрос или для производства иных следственных действий), он подал несколько жалоб на нарушение уголовно-процессуального законодательства[1].

Все жалобы, которые были адресованы вышестоящим руководителям, через некоторое время поступили для рассмотрения в тот территориальный отдел внутренних дел (ОВД), в котором и были допущены нарушения. А еще через месяц П. получил в ответ на эти жалобы краткое ответное письмо, подписанное начальником ОВД. В нем сообщалось: «Ваше обращение в отношении сотрудников ОВД рассмотрено и не поддержано». О чем жалоба, какие доводы приводил ее заявитель, чем они опровергнуты – информация в письме отсутствовала, т. е. оно представляет собой унифицированную отписку, которая, видимо, направляется в ответ на многие жалобы.

5. Показательный пример из современной правоприменительной практики ФСБ России

Было бы полезно сравнить практику МВД России по рассмотрению заявлений о мошенничествах, совершаемых с использованием информационно-коммуникационных технологий, с аналогичной практикой в других правоохранительных органах и получить более полное представление о фактической уголовной политике в этой сфере. В этом смысле представляет особый интерес правоприменительная практика Федеральной службы безопасности (ФСБ). Ведь согласно Положению о Федеральной службе безопасности Российской Федерации (далее – Положение о ФСБ России)[2] одной из основных задач ФСБ России является формирование и реализация в пределах своих полномочий государственной политики в области обеспечения информационной безопасности (подп. 14 п. 8). При этом в соответствии с ч. 5 ст. 151 «Подследственность» УПК РФ[3] по уголовным делам о преступлениях, предусмотренных ч. 2–7 ст. 159, ч. 2–4 ст. 159.3, ст. 272–274.1, ч. 4 ст. 327 УК РФ

[1] В ч. 2 ст. 144 УПК РФ содержится требование, чтобы о процессуальном решении по заявлению о преступлении без промедления сообщалось заявителю с разъяснением права на обжалование принятого решения. Причем в случае отказа в возбуждении уголовного дела копия соответствующего постановления в течение 24 ч с момента его вынесения направляется заявителю независимо от наличия ходатайства об этом (ч. 4 ст. 148 УПК РФ).

[2] Утверждено Указом Президента РФ от 11 авг. 2003 г. № 960, действует в актуальной редакции.

[3] Уголовно-процессуальный кодекс Российской Федерации от 18 дек. 2001 г. № 174-ФЗ (ред. от 31.07.2025) (с изм. и доп., вступ. в силу с 01.09.2025) // Гарант : справочная правовая система.

и некоторых иных, предварительное следствие может производиться также следователями органа, выявившего эти преступления, т. е. процессуальный закон допускает расследование телефонных мошенничеств следователями ФСБ России.

Однако проведение сравнительного анализа сопряжено со значительными трудностями. Во-первых, для формирования репрезентативной выборки необходимо получить доступ к эмпирическим материалам, которыми располагает ФСБ России, а это требует согласия и поддержки руководства данного ведомства. Во-вторых, это трудоемкая задача, требующая при обстоятельной работе довольно длительных усилий коллектива исследователей, а не исследователя-одиночки.

Частичным и облегченным решением данной задачи были бы нахождение и анализ показательных примеров, из которых методом неполной индукции можно вывести вероятностный вывод о том, какова практика рассмотрения в ФСБ России заявлений граждан о неправомерном доступе к компьютерной информации, а также о мошенничествах, совершаемых с использованием информационно-коммуникационных технологий и данных, полученных путем неправомерного копирования защищенной компьютерной информации. В ходе исследования нам удалось несколько таких случаев обнаружить, и один из них будет описан далее; пострадавший гражданин, обратившийся за защитой в ФСБ России, предоставил нам необходимые материалы.

3 сентября 2024 г. к гражданину А. через мессенджер «Телеграм» было направлено текстовое сообщение с аккаунта «Дмитрий П.[1]», номер его телефона был сокрыт. Обратившийся представился как Дмитрий Викторович, учредитель известного в профессиональной среде правового фонда (далее – Фонд), он же председатель совета директоров компании, которая организует работу одной из самых крупных в России информационно-справочных правовых систем.

Состоялась переписка, в ходе которой Дмитрий Викторович (будем называть его так) изложил следующую легенду. Якобы первый заместитель начальника УФСБ по г. Москве и Московской области издал приказ от 1 сентября 2024 г. о проверке Фонда. В подтверждение легенды неизвестный выслал А. через мессенджер копию приказа. Там указано, что в связи с утечкой архивных данных из Фонда и возможным влиянием иностранных спецслужб на его должностных лиц против Фонда возбуждено уголовное дело, назначается проверка (почти дословная цитата). Далее Дмитрий Викторович сообщил, что к А. обратится следователь ФСБ, у которого есть ряд вопросов. Следователь вскоре позвонит А., и надо ответить. Вероятно, Дмитрий Викторович полагал, что А. является работником Фонда (но это не так). На случай отказа от контактов со следователем, пригрозил Дмитрий Викторович, А. пришлют повестку на домашний адрес. И, чтобы не быть голословным, Дмитрий Викторович указал этот адрес (сведения оказались точными). После этого А. переписку прекратил.

Здесь надо пояснить, что Фонд является издателем довольно популярного юридического журнала, в котором в прошлые годы А. многократно печатал научные статьи. Соответственно, с ним каждый раз заключались авторские договоры, и издательство располагает персональными данными А., включая реквизиты банковского счета для перечисления гонораров. В связи с этим А. пришел к выводу, что злоумышленники получили доступ, а затем скопировали часть информации из компьютерной базы Фонда, в которой сведения об авторах отражались вместе с данными о работниках Фонда; злоумышленники по очереди «отрабатывали» этот информационный массив, не различая статус подучетных. Цель каждого такого обращения злоумышленников к лицам, фигурирующим в базе данных, вероятно, состоит в том, чтобы выведать недостающие сведения и получить доступ к банковскому счету жертв.

А. подготовил заявление о преступлении и уже 4 сентября 2024 г. направил его через веб-приемную на сайте ФСБ России в данное ведомство, а также на электронный адрес УФСБ по г. Москве и Московской области. В заявлении указал, что в содеянном неизвестными лицами, по его мнению, усматриваются признаки нескольких преступлений; это: 1) неправомерный доступ к компьютерной информации (ст. 272 УК РФ); 2) неоконченное покушение на мошенничество либо мошенничество с использованием электронных средств платежа (ч. 3 ст. 30, ст. 159 или 159.3 УК РФ); 3) подделка официального документа в целях его использования и использование заведомо подложного документа (ст. 327 УК РФ).

[1] В названии аккаунта и в переписке фигурировала довольно редкая фамилия известного предпринимателя и общественного деятеля. Мы эту фамилию не приводим здесь из этических соображений.

А. в заявлении объяснил обращение в ФСБ тем, что *преступная схема,* с которой он столкнулся, *объективно направлена на дискредитацию российских органов государственной безопасности.* Еще А. указал, что и другие авторы, сотрудничавшие с редакцией журнала, а также работники Фонда, по всей видимости, подвергаются подобным мошенническим атакам. Возможно, кто-то из них уже пострадал финансово от мошенников. Поэтому всех этих лиц желательно опросить для установления и фиксации важных подробностей происшедшего. К заявлению были прикреплены скриншоты состоявшейся переписки со злоумышленником и копия фиктивного приказа.

Через неделю А. получил письмо от 11 сентября 2024 г., из которого следует, что его заявление о преступлении в УФСБ по г. Москве и Московской области рассмотрено, «информация о возможной причастности сотрудников ФСБ России к описываемым Вами обстоятельствам своего подтверждения не нашла». Со ссылкой на ч. 3 ст. 8 Федерального закона от 2 мая 2006 г. № 59-ФЗ «О порядке рассмотрения обращений граждан в Российской Федерации»[1] заявление А. было направлено в Главное управление МВД России по г. Москве. После этого А. никаких сообщений из правоохранительных органов о судьбе своего заявления не получал.

Таким образом, есть основания полагать, что обычной практикой реагирования органов ФСБ России на заявления граждан о мошенничестве с использованием информационно-коммуникационных технологий и о неправомерном доступе к компьютерной информации является уклонение от рассмотрения их в процессуальном порядке и направление в органы МВД России. Представленный нами пример показателен тем, что имелись у сотрудников ФСБ России дополнительные резоны для того, чтобы установить и привлечь к ответственности мошенников, изготавливающих и пускающих в оборот документы, якобы подписанные высоким руководителем из данного ведомства, а также выдающих себя за сотрудников ФСБ России, но ожидания заявителя не оправдались. Этот пример подтверждает и иллюстрирует официальную статистику, в соответствии с которой органы ФСБ России выявляют лишь 0,5 % всех зарегистрированных в стране преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации[2].

Заключение

Завершая изложение, полезно сформулировать некоторые выводы и рекомендации для тех, кто пострадал или может пострадать от телефонных мошенников, а также для представителей пострадавших в уголовном процессе[3]; эти выводы и рекомендации основаны на изложенном выше материале, а также на других данных нашего исследования, которые не вошли в текст статьи из-за ограниченности ее объема.

1. Правоприменительная практика такова, что заявления о телефонном мошенничестве, поступившие в вышестоящие управления и отделы внутренних дел, как правило, перенаправляются в низовые подразделения по месту жительства заявителей. Такая же судьба ожидает заявления о телефонном мошенничестве, адресованные в УБК МВД России или подразделения по борьбе с противоправным использованием информационно-коммуникационных технологий территориальных органов МВД России.

1.1. В связи с изложенным в п. 1 рекомендуем заявление о телефонном мошенничестве адресовать в тот отдел или отделение органов внутренних дел, на территории обслуживания которых проживает пострадавший. Если имеются какие-либо доводы к тому, чтобы заявление было рассмотрено в вышестоящем органе внутренних дел или в специализированном подразделении, то можно прибегнуть к следующему тактическому приему: подготовить второе заявление на основе первого, включить туда

[1] Согласно подп. 5.1 и 5.2 п. 9 Положения о ФСБ России для решения основных задач это ведомство осуществляет такие функции, как прием, регистрация и проверка сообщений о преступлениях, поступающих в органы безопасности, а также проведение дознания и предварительного следствия по уголовным делам о преступлениях, отнесенных к ведению органов безопасности. Порядок рассмотрения сообщений о преступлениях регламентируется не Федеральным законом от 2 мая 2006 г. № 59-ФЗ«О порядке рассмотрения обращений граждан Российской Федерации», а УПК РФ. В соответствии с ним любое решение по сообщению о преступлении оформляется мотивированным постановлением; копия постановления о передаче сообщения по подследственности в течение 24 ч с момента его вынесения направляется прокурору.

[2] Так, в течение 2023 г. органы ФСБ России выявили 3497 таких преступлений, в то время как в целом в России их было зарегистрировано 668 719. В это же время следственные органы Следственного комитета РФ выявили таких преступлений еще меньше – всего 2028. См.: Состояние преступности в России за январь-декабрь 2023 года. С. 28.

[3] Здесь целесообразно отметить, что для того, чтобы представлять потерпевшего в уголовном процессе, наличие статуса адвоката не требуется. В п. 7 постановления Пленума Верховного Суда РФ от 29 июня 2010 г. № 17 «О практике применения судами норм, регламентирующих участие потерпевшего в уголовном судопроизводстве» (ред. от 16.05.2017) разъяснено следующее: по смыслу ч. 1 ст. 45 УПК РФ представителями потерпевшего могут выступать не только адвокаты, но и иные лица, способные, по мнению этих участников судопроизводства, оказать им квалифицированную юридическую помощь.

эти доводы и направить оба заявления одновременно по своим адресам. При этом следует рассматривать первое заявление как основное, второе – как дополнительное, на которое не нужно возлагать большие надежды. Однако и пренебрегать возможностью увеличить шансы на успех не стоит[1].

1.2. Если в момент совершения противоправных действий потерпевший находился вне места своего жительства (выехал за пределы своего района или населенного пункта к месту работы, в гости на выходные, в отпуск и т. д.), то изложенную выше рекомендацию модифицируем: помимо заявления, адресованного в ОВД по месту жительства, можно подготовить и направить дополнительное заявление по месту временного пребывания, и это обстоятельство (нахождение в момент совершения преступления на определенном адресе) подчеркнуть в заявлении.

1.3. Заявление, адресованное в ОВД по месту жительства, стоит доставить туда лично и быть готовым к взаимодействию с оперативным работником и со следователем, входящими в дежурную группу. Таким образом, будет обеспечено максимально быстрое реагирование на заявление о телефонном мошенничестве.

2. Тем, кто подвергся атакам телефонных мошенников, но не понес материального ущерба, или это ущерб незначителен, автор тем не менее рекомендует незамедлительно обращаться в правоохранительные органы с заявлением о преступлении и добиваться возбуждения уголовного дела. Эта рекомендация основана на нескольких соображениях.

Во-первых, таким образом пострадавшие лица исполнят свой гражданский долг, внесут посильный вклад в борьбу с новыми и опасными формами преступности.

Во-вторых, если мошенники в ходе общения с потерпевшим оперировали его персональными данными (а на их использовании обычно выстраиваются мошеннические схемы), то он объективно заинтересован в обнаружении места утечки этих данных, пресечении их дальнейшего распространения и в том, чтобы виновные лица понесли ответственность. В случае возбуждения уголовного дела и осуществления предварительного расследования, принятия надлежащих мер оперативно-разыскного характера есть вероятность обнаружить и перекрыть каналы распространения персональных данных потерпевших, изъять находящиеся в незаконном обороте электронные базы данных и т. д.

В-третьих, как показывает практика, если потерпевший проявит настойчивость в достижении указанной цели и будет пользоваться помощью грамотного юриста, то с высокой степенью вероятности возбуждения уголовного дела удастся добиться.

Есть и соображение более общего характера, выходящего за рамки заявленной темы: протестировав реакцию органов предварительного расследования на заявление о преступлении, работу контролирующих и надзирающих органов по месту своего жительства, гражданин будет лучше готов к взаимодействию с этими органами в будущем, если он или его близкие столкнутся с преступлением, которое нельзя игнорировать.

Разумеется, решение о том, втягиваться ли в соответствующий юридический процесс, должен принимать потерпевший, с учетом значимых личных обстоятельств, своих финансовых возможностей и проч.

3. Как показало наше исследование, жалобы на неизвещение заявителя о процессуальном решении, принятом по заявлению о преступлении, о ненаправлении заявителю копии постановления об отказе в возбуждении уголовного дела и на иные процессуальные нарушения, адресованные в вышестоящие органы внутренних дел, как правило, перенаправляются в тот орган, где допущены нарушения, а там в удовлетворении жалоб по надуманным мотивам либо вообще без мотивировки отказывается.

[1] Предвидим, что эта рекомендация подвергнется критике со стороны какой-то части коллег. Различные аспекты защиты прав лиц, пострадавших от тех или иных преступлений, исследуются нами уже четверть века, и в ходе опросов мы неоднократно знакомились с историями о том, как пострадавшие, при неопределенности в вопросе подследственности, подавали аналогичные заявления в разные правоохранительные органы, а затем, к своему удивлению, получали различные результаты – в одном органе в возбуждении уголовного дела отказывали, но в другом такое дело возбуждали. Если такое случится, полезно иметь в виду следующее. Согласно п. 5 ч. 1 ст. 27 УПК РФ, одним из оснований для прекращения уголовного преследования в отношении подозреваемого или обвиняемого является наличие в отношении этого лица неотмененного постановления об отказе в возбуждении уголовного дела. Однако описанные выше ситуации при буквальном толковании не подпадают под приведенное законодательное положение; пострадавший обращается с заявлением о преступлении, совершенном неизвестными, и постановление об отказе в возбуждении уголовного дела по этому заявлению выносится не в отношении конкретного лица. Следовательно, такое процессуальное решение не может препятствовать привлечению к уголовной ответственности телефонных мошенников по уголовному делу, возбужденному по другому заявлению. Но чтобы подстраховаться от расширительного толкования п. 5 ч. 1 ст. 27 УПК РФ, можно обжаловать прокурору постановление об отказе в возбуждении уголовного дела и просить его дать указание направить материал проверки заявления для приобщения к уголовному делу, возбужденному по аналогичному заявлению.

3.1. Указанные в п. 3 жалобы целесообразно направлять в органы прокуратуры в порядке ст. 124 УПК РФ, причем следует иметь в виду, что, согласно установленному порядку, обращения, решения по которым не принимали руководители нижестоящих прокуратур, направляются им для проверки изложенных доводов с установлением контроля либо без такового[1]. Поэтому для ускорения рассмотрения жалобы необходимо адресовать ее в низовую (районную или городскую) прокуратуру.

3.2. Если жалобу рассмотрел и принял по ней неудовлетворительное решение заместитель прокурора района, повторную жалобу следует направлять в ту же прокуратуру, потому что вышестоящим прокурором для заместителя будет первый заместитель, а для последнего – прокурор района.

3.3. Вместе с тем, в случае, если заявитель столкнулся с нарушениями при рассмотрении первичной жалобы (а особенно тогда, когда считает свой случай вопиющим), имеет смысл, минуя одну или несколько ступеней, обратиться в вышестоящую прокуратуру и, приведя свои доводы, просить об установлении контроля за своим обращением.

4. В тех немногих случаях, которые нам удалось изучить, – когда пострадавшие обжаловали в вышестоящий орган ФСБ России решение нижестоящего о направлении заявления о преступлении во внепроцессуальном порядке в органы внутренних дел, – наблюдалась ведомственная солидарность, вышестоящий орган поддерживал позицию нижестоящего. Однако мы не станем рекомендовать в подобных случаях обжалование в органы прокуратуры, считая его бесперспективным. По делам о мошенничестве в УПК РФ предусмотрена так называемая альтернативная подследственность (ч. 5 ст. 151); предварительное следствие может производиться следователем того органа, который выявил преступление, а значит, уголовное дело вправе возбудить и расследование провести следователь органа ФСБ России. И здесь надо обратить внимание на важный момент: вправе, но не обязан, поскольку основная подследственность таких дел – за органами внутренних дел. Если заявителю не удалось заинтересовать своим обращением органы государственной безопасности, несмотря на свои, казалось бы, веские резоны, то это надо принять, не растрачивать напрасно силы и время; добиться через прокуратуру главного – подключения к работе органов государственной безопасности – не удастся, для этого нет достаточной правовой основы.

Итак, наша рекомендация такова: подавать заявление о телефонном мошенничестве в органы ФСБ России разумно, если для этого есть конкретные доводы (иностранный или террористический след, угроза экономической безопасности и др.). Эти доводы в заявлении следует убедительно излагать, но не считать их решающими, и рассматривать такое заявление как дополнительный (неосновной) инструмент защиты.

5. Желательно не отвечать на вызовы с неизвестных номеров, при возникновении подозрения прерывать телефонное общение, а также устанавливать на мобильные телефоны программы, позволяющие в автоматическом режиме записывать все телефонные разговоры (те аудиозаписи, которые в будущем не потребуются, пользователь может периодически удалять). Такая тактика позволит в случае мошеннических атак получить образы голосов мошенников, зафиксировать все подробности состоявшихся разговоров[2], использовать записи в качестве веских улик в будущем уголовном процессе.

Рекомендация об оснащении мобильного телефона программой для записи разговоров особенно актуальна для тех, кто вынужден отвечать на вызовы с незнакомых номеров, кто часто получает звонки от мошенников, а также тех, кто уже попался на уловки телефонных мошенников, поскольку, достигнув успеха, обнаружив слабые стороны своей жертвы, они могут продолжить атаки на нее.

Конечно, в силу отличий в возрасте, образовании, профессиональном и житейском опыте, психофизиологических качествах люди имеют разную уязвимость перед атаками телефонных и иных мошенников. Тем не менее никто не застрахован от того, чтобы попасться на уловки профессиональных мошенников, особенно если в результате неудачного стечения обстоятельств стандартная мошенническая схема получит подтверждение в глазах потенциальной жертвы либо для атаки мошенники будут

[1] См. п. 3.2 Инструкции о порядке рассмотрения обращений и приема граждан в органах прокуратуры Российской Федерации (утв. приказом Генпрокурора России от 30 янв. 2013 г. № 45).

[2] В силу разных причин потерпевшие, нередко, значимые моменты разговора не запоминают или воспринимают искаженно.

использовать персонифицированную схему[1]. Поэтому никому не следует пренебрегать доступными мерами защиты.

СПИСОК ЛИТЕРАТУРЫ

1. Бастрыкин А. И. Выявление и расследование преступлений, совершенных с использованием информационно-коммуникационных технологий // Вестник Российской правовой академии. 2022. № 4. С. 88–94.

2. Киселев А. С., Горбунова К. А. Особенности тактики допроса обвиняемых при расследовании преступлений в сфере компьютерной информации // Правопорядок: история, теория, практика. 2024. № 2 (41). С. 67–74. DOI: 10.47475/2311-696X-2024-41-2-67-74

3. Романова Г. В. Информационные технологии в деятельности следователя // Вестник Волжского университета имени В. Н. Татищева. 2023. Т. 1, № 2. С. 159–169;

4. Смушкин А. Б. Криминалистические аспекты исследования даркнета в целях расследования преступлений // Актуальные проблемы российского права. 2022. № 3. С. 102–111.

5. Скобликов П. А. Мотивы необоснованных и незаконных отказов в возбуждении уголовных дел // Уголовный процесс. 2013. № 4. С. 68-74.

6. Скобликов П. А. Противодействие правоохранителей возбуждению уголовных дел: система типичных приемов и уловок // Закон. 2016. № 7. С. 92-105.

7. Янгаева М. О., Павленко Н. О. OSINT. Получение криминалистически значимой информации из сети Интернет // Алтайский юридический вестник. 2022. № 2 (38). С. 131–135.

REFERENCES

1. Bastrykin A.I. Vyyavlenie i rassledovanie prestuplenii, sovershennykh s ispolzovaniem informatsionno-kommunikatsionnykh tekhnologii [Detection and Investigation of Crimes Committed Using Information and Communication Technologies]. *Vestnik Rossiiskoi pravovoi akademii* [Bulletin of the Russian Legal Academy], 2022, no. 4, pp. 88-94. (in Russian)

2. Kiselev A.S., Gorbunova K.A. Osobennosti taktiki doprosa obvinyaemykh pri rassledovanii prestuplenii v sfere kompyuternoi informatsii [Features of Interrogation Tactics of the Accused in the Investigation of Computer Information Crimes]. *Pravoporyadok: istoriya, teoriya, praktika* [Law and Order: History, Theory, Practice], 2024, no. 2(41), pp. 67-74. DOI: 10.47475/2311-696X-2024-41-2-67-74 (in Russian)

3. Romanova G.V. Informatsionnye tekhnologii v deyatelnosti sledovatelya [Information Technologies in the Activities of an Investigator]. *Vestnik Volzhskogo universiteta imeni V.N. Tatishcheva* [Bulletin of the Volzhsky University named after V.N. Tatishchev], 2023, vol. 1, no. 2, pp. 159-169. (in Russian)

4. Smushkin A.B. Kriminalisticheskie aspekty issledovaniya darkneta v tselyakh rassledovaniya prestuplenii [Forensic Aspects of Darknet Research for Crime Investigation]. *Aktualnye problemy rossiiskogo prava* [Actual Problems of Russian Law], 2022, no. 3, pp. 102-111. (in Russian)

5. Skoblikov P.A. Motivy neobosnovannykh i nezakonnykh otkazov v vozbuzhdenii ugolovnykh del [Motives for Unfounded and Illegal Refusals to Initiate Criminal Cases]. *Ugolovnyi protsess* [Criminal Process], 2013, no. 4, pp. 68-74. (in Russian)

6. Skoblikov P.A. Protivodeistvie pravookhranitelei vozbuzhdeniyu ugolovnykh del: sistema tipichnykh priemov i ulovok [Counteraction of Law Enforcement Officers to the Initiation of Criminal Cases: A System of Typical Techniques and Tricks]. *Zakon* [Law], 2016, no. 7, pp. 92-105. (in Russian)

7. Yangaeva M.O., Pavlenko N.O. OSINT. Poluchenie kriminalisticheski znachimoi informatsii iz seti Internet [OSINT. Obtaining Forensically Significant Information from the Internet]. *Altaiskii yuridicheskii vestnik* [Altai Legal Bulletin], 2022, no. 2(38), pp. 131-135. (in Russian)

Статья поступила в редакцию 17.05.2025; одобрена после рецензирования 13.06.2025; принята к публикации 03.09.2025.

Received on 17.05.2025; approved on 13.06.2025; accepted for publication on 03.09.2025.

Скобликов Петр Александрович – доктор юридических наук, ведущий научный сотрудник сектора уголовного права, уголовного процесса и криминологии, Институт государства и права РАН (Россия, 119019, г. Москва, ул. Знаменка, 10), РИНЦ Author ID: 437024, ORCID: 0000-0001-7875-7036, e-mail: skoblikov@list.ru

Skoblikov Petr Alexandrovich – Doctor of Juridical Sciences, Leading Research Fellow of the Department of Criminal Law, Criminal Procedure and Criminology, Institute of State and Law Russian Academy of Sciences (10, Znamenka st., Moscow, 119019, Russian Federation), RSCI Author ID: 437024, ORCID: 0000-0001-7875-7036, e-mail: skoblikov@list.ru

[1] В этом смысле показателен недавний случай, когда атаке телефонных мошенников подвергся юрист-ученый, находящийся в возрасте зрелости (но не дряхлости), при этом известный в профессиональной среде как специалист по вопросам защиты банковской тайны. 50-летнему профессору пришло голосовое сообщение от бывшего коллеги по работе в столичном университете (т. е. для конкретной жертвы мошенниками был подготовлен качественный дипфейк) о том, что его разыскивает для сотрудничества заместитель руководителя Минобрнауки. Вдохновленный открывшейся перспективой профессор позвонил высокому чиновнику, но в приемной ответили, что тот на совещании (видимо, мошенники точно рассчитали время начала своей акции). Чуть позже профессору позвонил сам замминистра, но не настоящий. Он объяснил, что украинские хакеры якобы взломали сайт Минобрнауки и набрали кредитов по личным данным ученых, а деньги отсылают ВСУ. Профессору было предложено «спасти» свои средства, отправив их на «безопасный» банковский счет. Чтобы окончательно убедить жертву, ей также позвонили из «ФСБ» и «Росфинмониторинга». В итоге профессор перечислил мошенникам 6602 000 руб. См.: Миссуми Т. Телефонные аферисты развели разработчика защиты банковских данных на 6,6 млн рублей // Информационное и общественно-политическое издание «Life.ru». 2024. 13 янв. URL: https://life.ru/p/1632893 (дата обращения: 07.01.2025).