

УТЕЧКА ПЕРСОНАЛЬНЫХ ДАННЫХ И ТЕЛЕФОННОЕ МОШЕННИЧЕСТВО: ПРОБЛЕМНЫЕ ВОПРОСЫ И ПУТИ РЕШЕНИЯ

А.М. Останина, магистр

Н.В. Павлов, канд. юрид. наук, доцент

Кубанский государственный аграрный университет им. И.Т. Трубилина
(Россия, г. Краснодар)

DOI:10.24412/2500-1000-2025-1-4-151-154

Аннотация. В научной статье авторами изучены основные проблемные вопросы утечки персональных данных и телефонного мошенничества. Проанализированы мероприятия по изменению законодательства в целях недопущения нарушения конституционного права гражданина страны, связанного с неприкосновенностью частной жизни, правом на личную и семейную тайну. Приведены статистические данные, свидетельствующие о возрастающем количестве совершенных преступлений. Рассмотрены пути совершения мошеннических схем. Отмечена важность разработки и принятия мер по недопущению и пресечению утечки персональных данных, а также телефонного мошенничества. Предложены возможные пути разрешения имеющихся проблем в целях защиты и обеспечения безопасности граждан России.

Ключевые слова: персональные данные, телефонное мошенничество, контроль, безопасность, гражданин, законодательство, защита.

Утечка персональных данных, а также телефонное мошенничество остаются актуальными проблемами на сегодняшний день. Как показывают статистические данные за 2024 год Роскомнадзор зафиксировал утечку более 680 миллионов личных записей граждан Российской Федерации.

Злоумышленники разрабатывают все больше новых схем в целях завладения персональными данными других лиц. К числу сказанных относится использование фейковых сайтов (к примеру, Единого портала государственных услуг) с последующим поднятием рейтинга, подделка телефонного номера службы поддержки, а также рассылка с таких номеров текстового СМС-сообщения о якобы попытке взлома личного аккаунта, действие в социальных сетях под видом благотворительных организаций. Появилась и такая схема как похищение данных граждан через картинку-открытку. Жертва получает изображение (с расширением GIF) после нажатия на которую загружается вредоносный код, обеспечивающий утечку персональных данных владельца мобильного устройства. По информации Министерства внутренних дел Российской Федерации в преддверии новогодних праздников телефонные мошенники активизировали свою правонарушительную деятельность для расшатывания кредитно-

финансовой системы и дестабилизации обстановки на территории России. Сказанное показывает, что злоумышленники используют различные неправомерные способы в мошеннических целях. Также нельзя не отметить о доверии граждан России, которым пользуются мошенники под разными предлогами вынуждают взять в кредит внушительную сумму денег. За 2024 год путем отмеченной схемы у людей преступники похитили 250 миллиардов рублей, при этом самые уязвимые жертвы преступлений – граждане пожилого возраста.

Проблема утечки персональных данных, телефонного мошенничества вызывает мощный резонанс в обществе, который показывает то, что необходимость перемен сегодня назрела как никогда. Отмеченные вопросы поднимались в ходе прямой линии Президента России, состоявшейся 19 декабря 2024 года. При этом во многих работах ученых юристов подчеркивается необходимость борьбы и предотвращения совершения подобного рода правонарушений поскольку они подрывают основу конституционного строя Российской Федерации, гарантирующую гражданам страны неприкосновенность частной жизни, и в целом безопасности государства [1].

Абсолютно любая информация, которая прямо или косвенно относится к определенному гражданину страны составляет в сово-

купности персональные данные [2]. Как нами было отмечено выше защита сведений, которые относятся к личной жизни гражданина, имеет особое значение в соответствии с Конституцией России. Основной закон страны гарантирует каждому лицу неприкосновенность частной жизни, право на личную и семейную тайну [3]. Нарушение данных норм недопустимо. С связи с чем видится необходимость в разработке и внесение изменений в законодательство, организации более качественных и эффективных способов контрольных мероприятий за утечкой персональных данных, а также телефонным мошенничеством.

Как известно, существует два вида (типа) телефонии: традиционная и SIP или IP-телефония. Последняя в свою очередь характеризуется тем, что данный вид связи работает через интернет без подключения к мобильной сети. Данный факт не дает возможность определить принадлежность к какой-либо конкретной базовой станции, что тем самым придает виртуальный характер телефонному номеру. Сложившаяся ситуация привела к активному использованию злоумышленниками SIP или IP-телефонии в целях избежания ответственности и совершения действий мошеннического характера. Видится необходимость в запрете на законодательном уровне использования рассматриваемого типа телефонии для ограничения телефонного мошенничества. Стоит отметить, Правительство России 26 декабря 2024 года подписало постановление, которое с 1 сентября 2025 года официально запретит звонки через IP-телефонию на мобильные и стационарные телефоны.

Безопасность в государстве залог доверия и спокойной жизни граждан страны. В свою очередь в период напряженной политической обстановки участились случаи звонков из иностранных государств. В данном случае имеет место быть два варианта развития событий: телефонный звонок действительно поступает из-за границы, или мошенник совершает звонок с территории российского государства посредством использования иностранного номера телефона. Остановимся немного подробнее на первом из отмеченных случаев. Подрыв безопасности государства, дестабилизация органов власти государства,

воздействие на принятие решений указанными органами путем совершения действий террористической направленности все это преследует вербовщик из иностранного государства, который может оказаться на другой стороне телефонного звонка. Террористический акт подразумевает под собой совершение взрыва, поджога или иных действий, которые навели страх и создали опасность наступления последствий как физического характера, так и материального. Нищета, голод выступают питательной средой терроризма. Вербовщики пользуются данными рычагами воздействия разыскивая для совершения подобных действий людей с низким материальным достатком.

Сказанное с уверенностью позволяет утверждать о том, что видится необходимость в установление требований по блокировке телефонных звонков из-за границы. Уже сейчас операторы связи имеют право блокировать звонки, поступающие из иностранных государств. Однако все же этого недостаточно, следует закрепить запрет в правовых актах, на законодательном уровне. Аналогичные требования могут быть введены и в отношении мессенджеров. Как мера понуждения для них может быть использована блокировка голосового трафика в них [4]. Обратим внимание на то, что проблеме внешних атак уделяется пристальное внимание. Речь идет о спам-рассылки в органы государственной власти и местного самоуправления, которая осуществляется, как правило, посредством направления массовых обращений от заявителей, использовавших зарегистрированные в иностранной доменной зоне адреса электронной почты. Разработанном и принятом законопроекте были уточнены требования к электронному обращению гражданина, состоявшие в том, что для получения ответа или уведомления о переадресации в обращении гражданина должен быть указан электронный адрес, доменное имя которого находится в российской национальной доменной зоне. В случае, если в обращении, поступившем в государственный орган, орган местного самоуправления или должностному лицу в форме электронного документа, не будет указан адрес электронной почты, доменное имя которого находится в российской национальной доменной зоне, ответ на обращение даваться не бу-

дет [5]. На наш взгляд принятый законопроект позволит улучшить информационную безопасность, и оградит как граждан, так и государство в целом от внешних атак.

Видится важность в организации более качественных и эффективных способов контрольных мероприятий. Отметим, контроль выступает основным способом обеспечения законности в государстве [6]. Контрольные мероприятия способствуют выявлению и пресечению совершения правонарушения. Таким образом, повышение уровня контроля за утечкой персональных данных, телефонном мошенничестве послужит разрешению имеющихся на сегодняшний день пробелов.

Хотелось бы отметить тот факт, что уполномоченными органами государственной власти России разрабатываются и воплощаются различные мероприятия по изменению законодательства в целях недопущения нарушения конституционного права гражданина страны, связанного с неприкосновенностью частной жизни, права на личную и семейную тайну. Разрабатываются различные законопроекты, заключающиеся в повышении штрафов, ужесточение ответственности, предлагается установить, что согласие на обработку персональных данных должно оформляться отдельно от иных документов, которые под-

тверждает или подписывает субъект персональных данных. Чтобы оградить граждан от мошенников, разработан и внесён в Государственную Думу России законопроект, которым предлагается установить при выдаче кредита «период охлаждения», в течение которого не будут осуществляться финансовые операции: 4 часа – для сумм от 50 до 200 тысяч рублей, 48 часов – для сумм от 200 тысяч рублей. Установленное время люди смогут использовать для более тщательного анализа необходимости денежных средств, дополнительной оценки своей платежеспособности, консультаций с родственниками и друзьями. Если появятся подозрения на действия мошенников – обратиться в компетентные органы.

Подводя итог вышесказанному, отметим, утечка персональных данных и телефонное мошенничество остается наиболее актуальными проблемами в государстве. Данные проблемы требуют разработки и принятия действенных путей их разрешения. Считаем, что предложенные варианты решения будут способствовать ликвидации и недопущению утечки персональных данных граждан России, а также оградят их от телефонного мошенничества.

Библиографический список

1. Останина А.М. К вопросу о контрольной деятельности в сфере защиты персональных данных от телефонного мошенничества // Наука. Образование. Современность. – 2024. – № 1. – С. 83-86.
2. О персональных данных: Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 08.08.2024) // Собрание законодательства РФ. 2006. № 31 (1 ч.). Ст. 3451.
3. Конституция Российской Федерации (принята всенародным голосованием 12 декабря 1993 г. с изменениями, одобренными в рамках общенародного голосования 01.07.2020) // Собрание законодательства РФ. 2020. № 31. Ст. 4398.
4. Роскомнадзор: Операторы связи не должны зарабатывать на мошенническом трафике // Российская газета. – [Электронный ресурс]. – Режим доступа: <https://rg.ru>. (дата обращения: 02.01.2024).
5. Павлов Н.В., Останина А.М. Теоретико-правовые проблемы рассмотрения обращения в форме жалобы // Пробелы в российском законодательстве. – 2024. – Т. 17. № 7. – С. 32-39.
6. Останина А.М., Павлов Н.В. Контроль и надзор как основные способы обеспечения законности в административно-публичной деятельности // Евразийский юридический журнал. – 2024. – № 2 (189). – С. 187-188.

**LEAKAGE OF PERSONAL DATA AND TELEPHONE FRAUD:
PROBLEMATIC ISSUES AND SOLUTIONS**

A.M. Ostanina, *Master's Degree*

N.V. Pavlov, *Candidate of Legal Sciences, Associate Professor*

**Kuban State Agrarian University named after I.T. Trubilin
(Russia, Krasnodar)**

***Abstract.** In the scientific article, the authors studied the main problematic issues of personal data leakage and telephone fraud. The article analyzes measures to change legislation in order to prevent violations of the constitutional right of a citizen of the country related to the inviolability of private life, the right to personal and family secrets. Statistical data indicating an increasing number of crimes committed are presented. The ways of committing fraudulent schemes are considered. The importance of developing and taking measures to prevent and suppress the leakage of personal data, as well as telephone fraud, was noted. Possible ways of solving the existing problems in order to protect and ensure the safety of Russian citizens are proposed.*

***Keywords:** personal data, telephone fraud, control, security, citizen, legislation, protection.*