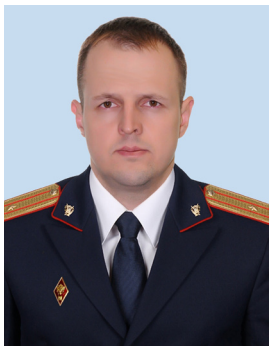
Научная статья
УДК 343
https://doi.org/10.36511/2078-5356-2024-1-92-96



Отдельные проблемы противодействия преступлениям против общественной безопасности, совершаемым посредством распространения заведомо ложной информации с использованием средств сетевой телекоммуникации

Гущев Максим Евгеньевич[1], Летёлкин Николай Владимирович[2]
[1, 2]Нижегородский филиал Санкт-Петербургской академии Следственного комитета Российской Федерации, Нижний Новгород, Россия
[1]gushchev.me@skspba.ru
[2]letyolkin.nv@skspba.ru

Аннотация. В статье рассматриваются актуальные проблемы противодействия преступлениям против общественной безопасности, совершаемым посредством распространения заведомо ложной информации с использованием средств сетевой телекоммуникации. Приводятся новые способы совершения таких деяний с применением технологий *IP*-телефонии. Предлагаются меры по совершенствованию отечественного законодательства в указанной сфере.

Ключевые слова: информация, заведомо ложные сведения, преступления против общественной безопасности, проблемы расследования, *IP*-телефония

Для цитирования: Гущев М. Е., Летёлкин Н. В. Отдельные проблемы противодействия преступлениям против общественной безопасности, совершаемым посредством распространения заведомо ложной информации с использованием средств сетевой телекоммуникации // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2024. № 1 (65). С. 92–96. https://doi.org/10.36511/2078-5356-2024-1-92-96.

Original article

Selected problems of countering crimes against public safety committed through the dissemination of deliberately false information using network telecommunications

Maxim E. Gushchev[1], Nikolay V. Letelkin[2]
[1, 2]Nizhny Novgorod branch of the St. Petersburg Academy of the Investigative Committee, Nizhny Novgorod, Russian Federation
[1]gushchev.me@skspba.ru
[2]letyolkin.nv@skspba.ru

Abstract. The article discusses current problems of countering crimes against public safety committed through the dissemination of deliberately false information using network telecommunications. New ways of committing such acts using IP-telephony are given. Measures are proposed to improve domestic legislation in this area.

Keywords: information, deliberately false information, crimes against public safety, investigation problems, IP-telephony

For citation: Gushchev M. E., Letelkin N. V. Selected problems of countering crimes against public safety committed through the dissemination of deliberately false information using network telecommunications. *Legal Science and Practice: Journal of the Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia*, 2024, no. 1 (65). pp. 92–96. (In Russ.). https://doi.org/10.36511/2078-5356-2024-1-92-96.

Двадцать первый век — век информации и компьютерных технологий. В последнее время этот тезис получил очередной виток своей актуальности. Пандемия новой короновирусной инфекции *Covid-19*, усложнившаяся на почве различных вооруженных конфликтов, международная обстановка серьезно влияют как на отдельных людей, государства, так и международное сообщество [1, с. 6–7].

Сложная геополитическая ситуация, попытки сохранения устаревшей модели однополярного мироустройства привели к тому, что устоявшиеся основополагающие принципы международного сотрудничества, морали и нравственности уходят на второй план, а средства массовой коммуникации, информационно-телекоммуникационные сети и другие технологии становятся средствами гибридной войны в отношении России.

Более семи лет назад на восьмом совещании послов и постоянных представителей Российской Федерации, состоявшемся в Министерстве иностранных дел России, Президент Российской Федерации В. В. Путин очень точно дал установку на необходимость и важность защиты информационного поля: «Мы живем в информационную эпоху, и афоризм “кто владеет информацией, тот владеет миром” отражает реальности сегодняшнего дня».

И действительно, сущность сегодняшнего дня такова, что информация может выступать средством посягательства на самые различные общественные отношения и ценности: интересы личности, экономики, общественной безопасности и общественного порядка, государственной власти, военной службы, мира и безопасности человечества, то есть всей системы отечественного уголовного закона.

Вместе с тем наибольшую угрозу представляет информация, посягающая на интересы общественной безопасности. Этот тезис подтверждается событиями, произошедшими в 2022–2023 годах, в том числе в городе Буча, где была осуществлена хорошо прорежиссированная провокация, направленная на причинение репутационного вреда Российской Федерации [2], в Дагестане, где массовые беспорядки были инспирированы посредством сетевых телекоммуникаций с территории Украины [3] и т. д.

Следует признать, что отечественный законодатель пытается адекватно реагировать на подобные вызовы, в том числе посредством криминализации ряда норм об ответственности за публичное распространение заведомо ложной информации (ст. 207[1]–207[3] УК РФ) и пенализации, осуществленной применительно к статье 207 УК РФ [4].

В то же время расследование указанных преступлений представляет особую сложность, что обосновывается:

— во-первых, неустоявшейся следственно-судебной практикой применения рассматриваемых норм, вызванной сравнительно небольшим сроком их действия (применительно к ст. 207[1]–207[3] УК РФ);

— во-вторых, проблемами расследования, сопряженными с трансграничным характером таких деяний, в том числе совершенных посредством информационно-телекоммуникационных сетей.

С целью выявления и решения обозначенных проблем в 2023 году на базе Нижегородского филиала Санкт-Петербургской академии Следственного комитета Российской Федерации проведено комплексное исследование практики противодействия преступлениям, сопряженным с публичным распространением заведомо ложной информации [5]. Ранее с целью научной апробации полученных результатов указанного исследования в научной литературе рассматривались вопросы подтверждения факта ложности распространяемых сведений при проведении предварительного расследования [6]. Вместе с тем обозначенная проблема, уже ставшая предметом научной дискуссии, не является единственной.

Так, следует отметить, что значительное число рассматриваемых деяний совершается с использованием средств *IP*-телефонии и методов анонимизации личности в виртуальном пространстве, в том числе и с территории иностранных государств.

Изначально при проведении предварительной проверки сообщения о преступлении, звонок, совершенный с использованием средств *IP*-телефонии, воспринимается как осуществленный с территории Российской Федерации, так как визуализируется номер отечественного

сегмента телефонной связи. Этот номер зарегистрирован на конкретное лицо, которое не причастно к совершению рассматриваемых преступлений, то есть фактически является подставным, что в дальнейшем устанавливается посредством проведения допросов, а при необходимости и выемки с дальнейшим осмотром аппарата связи указанного лица.

Все дело в том, что при использовании технологий *IP (SIP)*-телефонии при совершении соединения злоумышленник использует средства компьютерной техники, а сигнал передается в цифровом виде посредством информационно-телекоммуникационных сетей (например, через «Интернет»). Переход на номерную емкость отечественного сегмента связи «+7…» может быть осуществлен двумя способами, с использованием технологии подмены номера либо применением специализированного оборудования (коммутаторов).

Следует последовательно изучить природу каждого из представленных методов.

Технология подмены номера реализуются посредством замены идентификатора — *Caller ID*. Указанный идентификатор может быть изменен при использовании специализированного программного обеспечения (в том числе, и находящегося в свободном доступе), либо программно-аппаратных средств. Кроме того, такая услуга может быть предоставлена и оператором связи (в том числе и иностранным).

Опасность применения технологий подмены номера в полной мере осознана и отечественным законодателем, который в 2021 году предпринял попытку пресечения возможности использования изменений *Caller ID*. Так, 2 июля 2021 года были внесены существенные изменения в Федеральный закон №-28 «О связи» [7], в соответствии с которыми с 1 января 2023 года на отечественных операторов связи возложена обязанность по передаче в сеть других операторов, участвующих в конкретном соединении абонентского номера (или идентифицирующего кода) в неизменном виде. Эта новелла фактически исключает использование рассматриваемой технологии при совершении звонков на территории Российской Федерации с измененным идентификатором *Caller ID*.

Что касается подмены номера, осуществляемой за пределами Российской Федерации, то при таком соединении на отечественного оператора связи возложена обязанность его блокирования, в том числе посредством внедрения различных технологий, действующих по типу «Антифрод» [8].

Следует признать, что предпринятые законодательные меры реагирования можно признать действующими. В настоящее время количество преступлений, совершаемых с использованием описанной технологии подмены номера, существенно сокращается ввиду использования других алгоритмов проведения соединения, поступающего с территории иностранного государства.

Указанные алгоритмы заключаются ***в применении различного оборудования,*** установленного на территории Российской Федерации, ***выполняющего роль коммутатора,*** который преобразовывает цифровой сигнал, проходящий по протоколу *“IP”* в сигнал телефонной связи с присвоением соответствующего номера. Таким образом, представляется, что оператор связи не может осуществить мероприятия по проверке достоверности сведений о пользователе (абоненте), а изменения Федерального закона «О связи», принятые Федеральным законом от 2 июля 2021 года № 319-ФЗ, не могут быть реализованы по техническим причинам.

В рассматриваемых случаях операторы связи заключают с юридическими и физическими лицами договоры об оказании услуг связи, в рамках которых передают последним определенное количество номерных емкостей в виде физических или электронных *Sim*-карт в корпоративное пользование. Кроме того, могут заключаться дополнительные соглашения о возможности самостоятельного управления услугами связи со стороны третьих лиц.

В конечном итоге полученные емкости загружаются в специализированное оборудование, свободно доступное к приобретению, выполняющее роль коммутатора.

Такое оборудование (например «Симбокс» или *“sim pool*”), принимая цифровой сигнал, поступающий, в том числе с территории иностранного государства, переводит его на *Sim*-карту отечественного оператора связи (загруженную в оборудование). В дальнейшем звонок происходит и поступает адресату как телефонное соединение с определением российского номера телефона.

Проблемы расследования преступлений, совершаемых с использованием описанного алгоритма подмены номера, состоят в том, что:

во-первых, коммутаторное оборудование может находиться не по юридическому адресу, установленному в договоре с оператором связи;

во-вторых, в соответствии с соглашениями о самостоятельном управлении операторы связи не несут ответственности за проведенное соединение;

в-третьих, лица, использующие оборудование, как правило, не посвящены в вопросы преступной деятельности, а фактически — оказывают услуги по переводу сетевого трафика из протокола "*IP*" в "*GSM*";

в-четвертых, ввиду использования технологий анонимизации личности в рассматриваемых условиях зачастую невозможно установить местонахождение реального преступника.

Следует отметить, что в эпоху, когда информация является средством, а зачастую и орудием гибридной войны против национальной безопасности Российской Федерации, совершаемой, в том числе и с использованием возможностей зарубежных правительственных центров информационных технологий и систем обороны или информационно-психологических операций (например, ЦИПсО Сил специальных операций Украины), необходимо осуществлять жесткий контроль оборота такой информации и средств ее передачи.

С этой целью назревает необходимость совершенствования законодательства в названной сфере. В частности, следует рассмотреть следующие вопросы:

во-первых, о запрете делегирования операторами связи полномочий и ответственности за управление соединениями;

во-вторых, о введении контроля оборота оборудования по типу «Симбокс» (*"sim pool*").

Между тем проблемы противодействия преступлениям против общественной безопасности, совершаемым посредством распространения заведомо ложной информации с использованием средств сетевой телекоммуникации, существуют не только в прикладном, но и в практическом сегменте. В частности, с позиции уголовно-правового противодействия следует поставить вопрос о необходимости дополнения квалифицирующего (особо квалифицирующего) признака, позволяющего учитывать при квалификации подобных деяний факт использования информационно-телекоммуникационных сетей (включая сеть «Интернет»), так как научно обоснованно, что использование таких технологий существенно влияет на общественную опасность содеянного.

Список источников

1. Уголовно-правовое противодействие преступлениям, совершаемым с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет»): монография / отв. ред. А. В. Петрянин. Москва: Проспект, 2020. 176 с.

2. Ильина В. Песков: В Буче произошел чудовищный подлог // Российская газета. URL: https://rg.ru/2022/04/05/peskov-v-buche-proizoshel-chudovishchnyj-podlog.html (дата обращения: 01.02.2024).

3. Копорушкин М. Следователи возбудили дело после массовых беспорядков в аэропорту Махачкалы // Российская газета. URL: https://rg.ru/2023/10/29/sledovateli-vozbudili-delo-po-besporiadkam-v-aeroportu-mahachkaly.html (дата обращения: 01.02.2024).

4. Уголовный кодекс Российской Федерации от 13 июня 1996 года № 63-ФЗ: принят Государственной Думой Российской Федерации 24 мая 1996 года // Собрание законодательства РФ. 1996. № 25, ст. 2954.

5. Особенности расследования преступлений, предусмотренных статьями 207[1]–207[3] УК РФ: учебное пособие. Санкт-Петербург: Санкт-Петербургская академия Следственного комитета, 2024. 126 с.

6. Емельянова Е. В., Летёлкин Н. В., Пшеничнов И. М. О практике применения норм об ответственности за преступления против общественной безопасности, сопряжённые с публичным распространением заведомо ложной информации (в том числе посредством использования информационно-телекоммуникационных сетей) // Расследование преступлений: проблемы и пути их решения. 2023. № 4. С. 104–110.

7. О связи: федеральный закон от 7 июля 2003 года № 126-ФЗ // Собрание законодательства РФ. 2003. № 28, ст. 2895.

8. О внесении изменений в Федеральный закон «О связи»: федеральный закон от 2 июля 2021 года № 319-ФЗ // Собрание законодательства РФ. 2021. № 27. Ч. I, ст. 5147.

References

1. Criminal legal counteraction to crimes committed using information and telecommunication networks (including the Internet): monograph / ed. by A. V. Petryanin. Moscow: Prospect Publ., 2020. 176 p. (In Russ.)

2. Ilyina V. Peskov: A monstrous forgery occurred in Bucha. *Rossiyskaya Gazeta*. URL: https://rg.ru/2022/04/05/peskov-v-buche-proizoshel-chudovishchnyj-podlog.html (accessed 01.02.2024). (In Russ.)

3. Koporushkin M. Investigators opened a case after riots at the Makhachkala airport. *Rossiyskaya Gazeta*. URL: https://rg.ru/2023/10/29/sledovateli-vozbudili-delo-po-besporiadkam-v-aeroportu-mahachkaly.html (accessed 01.02.2024). (In Russ.)

4. Criminal Code of the Russian Federation: federal law no. 63-FZ of June 13, 1996: adopted by the State Duma of the Russian Federation of May 24, 1996. *Collection of legislative acts of the RF,* 1996, no. 25, art. 2954. (In Russ.)

5. Features of the investigation of crimes provided for in Articles 2071–2073 of the Criminal Code of the RF: training manual. St. Petersburg: St. Petersburg Academy of the Investigative Committee Publ., 2024, 126 p. (In Russ.)

Legal Science and Practice: Journal of Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia, 2024, no. 1 (65)

6. Emelyanova E. V., Letyolkin N. V., Pshenichnov I. M. On the practice of applying the rules on liability for crimes against public safety associated with the public dissemination of knowingly false information (including through the use of information and telecommunication networks). *Investigation of crimes: problems and ways to solve them*, 2023, no. 4, pp. 104–110. (In Russ.)

7. On communications: federal law no. 126-FZ of Jule 7, 2003. *Collection of legislative acts of the RF*, 2003, no. 28, art. 2895. (In Russ.)

8. On amendments to the federal law "On Communications": federal law no. 319-FZ of February 7, 2021. *Collection of legislative acts of the RF*, 2021, no. 27, part I, art. 5147. (In Russ.)

Информация об авторах

М. Е. Гущев — кандидат юридических наук, доцент, заведующий кафедры криминалистики;
Н. В. Летёлкин — кандидат юридических наук, доцент, доцент кафедры криминалистики.

Information about the authors

M. E. Gushchev — Candidate of Sciences (Law), Associate Professor, Head of the Department of Criminalistics;
N. V. Letelkin — Candidate of Sciences (Law), Associate Professor, Associate Professor of the Department of Criminalistics.

Статья поступила в редакцию 07.02.2024; одобрена после рецензирования 26.02.2024; принята к публикации 05.03.2024.

The article was submitted 07.02.2024; approved after reviewing 26.02.2024; accepted for publication 05.03.2024.