16. Трунцевский Ю. В. Е-антикоррупция или е-коррупция: влияние глобальной цифровизации // Международное публичное и частное право. 2019. № 4. С. 42–48.

17. Иванова Ю. А., Сарбаев Г. М. К вопросу о киберпреступности // Цифровые трансформации экономики и права: сборник научных тезисов Национальной научно-практической конференции, Москва, 8 декабря 2021 года. Волгоград, 2022. С. 58–64.

18. Kitts D. How mobile policing technology could bring cops closer to their communities [Электронный ресурс]. – URL: https://tvo.org/article/current-affairs/how-mobile-policing-technology-could-bring-cops-closer-to-their-communiti

19. UN Guide for Anti-Corruption Policies. URL: www.unodc.org/pdf/crime/corruption/ UN_ Guide.pdf

20. Официальные интернет-ресурсы государственных органов Азербайджанской Республики. URL: https://ems.gov.az

21. Kossow N., Dykes V. Embracing Digitalisation: How to use ICT to strengthen Anti-Corruption. GIZ, 2018. URL: https://www.giz.de/de/downloads/giz2018-eng ICT-to- strengthen-Anti -Corrupti on.pdf

22. Suleiman M.M. A Review of Improving Good Governance through ICT Revitalization. 2017. URL: https://www.researchgate.net/publication/325668385

23. Adam I., Fazekas M. Are emerging technologies helping win the fight against corruption in developing countries? Pathways for Prosperity Commission Background Paper Series. No. 21. Oxford. URL: http:// www.govtransparency.eu/wp-content/ uploads/2019/02/ICT-corruption-24Feb19_ FINAL.pdf

И. А. Биккинин,
доктор юридических наук, профессор,
Уфимский юридический институт
Министерства внутренних дел Российской Федерации

МЕРЫ ПРОТИВОДЕЙСТВИЯ ТЕРРОРИСТИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ С ИСПОЛЬЗОВАНИЕМ НОВЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ (ПО МАТЕРИАЛАМ РЕСПУБЛИКИ БАШКОРТОСТАН)

Аннотация. Цифровая трансформация общества и государства должна обеспечить гражданам повышение доверия и безопасности. Работа посвящена рассмотрению вопросов противодействия террористической деятельности средствами административно-правового воздействия на операторов связи. Исследуется действующее законодательство, регулирующее деятельность операторов связи в отношении запрета на подмену абонентского номера и блокировку номеров, проводится анализ практической работы в Республике Башкортостан. На этой основе предложены меры по совершенствованию организации борьбы с правонарушениями в данной сфере.

Ключевые слова: противодействие терроризму, информационные технологии, мошенничество, оператор связи, подмена абонентского номера

MEASURES OF COUNTERING TERRORIST ACTIVITIES THROUGH THE USE OF NEW INFORMATION TECHNOLOGIES: A CASE STUDY FROM THE REPUBLIC OF BASHKORTOSTAN

Abstract. The digital transformation of society and the state aims to provide citizens with increased trust and security. This paper discusses the issue of countering terrorist activities through administrative and legal measures on telecom operators when they violate the prohibition on number substitution and refuse to block numbers. The author examines current legislation on the activities of telecommunication operators regarding the prohibition of subscriber number substitution and blocking, and analyzes practical cases in the Republic of Bashkortostan. Based on this, measures are proposed to improve law enforcement agencies' work in this area to combat offenses.

Keywords: countering terrorism, information technology, fraud, telecommunications operator, subscriber number substitution

Введение. Цифровая трансформация общества и государства включает три составляющие: данные, доверие, развитие. Для человека она должна обеспечивать снижение стоимости доверия, повышение индивидуализации, удобства и безопасности [1].

Основная часть. Согласно отчету, сделанному по итогам опроса граждан компанией КРОС в рамках определения национального индекса тревожности, в первом квартале 2024 года самой сильной была боязнь телефонных мошенников (29 субъектов Федерации). Второе место занял страх террористических актов (23 субъекта Федерации). Сразу обе боязни вошли в топ-3 в 70 регионах России. Одни из самых высоких эти показатели в Республике Башкортостан (70 юнгов) [2]. Основным источником определяется деятельность украинских спецслужб и неонацистских формирований, нацеленных на вовлечение наших граждан в подготовку и совершение диверсионно-террористических актов. Проблемой называется недостаточная компетентность должностных лиц, занимающихся противодействием терроризму [3]. Особую опасность представляет вовлечение в совершение террористических актов с использованием новых информационных технологий, возможностей, которые дают вовлекающим в преступную деятельность новые способы коммуникаций. Прежде всего это относится к установлению контакта с помощью подменных телефонных номеров.

Действенными мерами предупреждения совершения телефонных мошенничеств выступают установление и реализация ответственности операторов связи за нарушение запрета на подмену номера и отказ от блокировки абонентских номеров и, следовательно, противодействие созданию образа достоверности сведений, передаваемых мошенниками в телефонном общении. Такие звонки совершаются преступниками в целях сообщения ложных данных, информации об актах терроризма, установления помех для деятельности энергетических, инфраструктурных объектов [4]. В апреле этого года сотрудники ФСБ и следственного департамента МВД задержали пять человек, которых подозревают в организации «незаконного виртуального узла связи». Этот узел связи использовался «украинскими call-центрами для телефонного мошенничества» [5]. По актуальным данным, жалобы на мошенников стало поступать в 2–5 раз реже после того, как были

атакованы электростанции в городах Украины типа Днепра. В этих населенных пунктах располагаются колл-центры, и откуда россиянам звонят преступники.

По Башкортостану в 2023 г. жителя Уфы мошенники, используя предлог возмещения денежных средств, склонили к поджогу подразделения кредитного учреждения, а в Ишимбае местную жительницу направили совершить поджог помещения военного комиссариата [6]. Следователи ФСБ России возбудили уголовные дела в отношении двух граждан, пытавшихся под воздействием мошенников поджечь здания военкоматов в Архангельском и Зианчуринском районах [7].

Государством на сегодняшний день создан ряд IT-систем противодействия киберугрозам: ГосСОПКА, «Антифрод» (Роскомнадзор), «Антифишинг» (Минцифры), ФинЦЕРТ (Центробанк) и внутренние сервисы крупных цифровых компаний [8]. Административная ответственность операторов связи за пропуск через техническое оборудование подменных номеров, с помощью которых совершаются «телефонные преступления», определена Федеральным законом [9]. Оператор связи, участвующий в установлении телефонного соединения, должен передавать в сеть связи другого оператора в неизменном виде полученный абонентский номер [10].

Проведенный нами анализ применения установленного запрета в деятельности подразделений МВД по Республике Башкортостан показал, что в 2023 г. за неисполнение указанных требований закона по результатам проверок, в том числе по материалам уголовных дел, возбуждено 36 дел об этих правонарушениях на общую сумму 10,1 млн руб. [11].

Совершенствование взаимодействия деятельности по противодействию мошенничествам с использованием информационных технологий является важным резервом этого направления нашей работы. Об этом свидетельствуют выявленные недостатки. Так в Управление Роскомнадзора по Республике Башкортостан в 2023 г. поступил материал проверки из ОМВД России по К* району, который сопроводительным письмом от 22 марта 2023 г. возвращен начальнику ОМВД России по К* району. По аналогичным основаниям сопроводительными письмами в 2022–2023 годах возвращены более двух десятков материалов проверки [12].

Прокуратурой Республики Башкортостан проведена проверка исполнения Управлением Роскомнадзора по Республике Башкортостан законодательства об административных правонарушениях, в ходе которой выявлены факты непринятия мер по материалам, поступившим из органов полиции. В этой связи в адрес руководителя ведомства вынесено представление, одно должностное лицо привлечено к дисциплинарной ответственности.

Заключение. Подводя итог проведенному исследованию и выражая согласие с выводами проведенной прокурорской проверки, еще раз подчеркнем, что административно-правовые средства противодействия террористическим актам выступают важным юридическим инструментом этой работы. Совместная активная деятельность всех уполномоченных органов и должностных лиц, включая МВД России и Роскомнадзор, является существенным резервом в активизации борьбы с террористическими актами, которые реализуются с помощью мошеннических действий, совершаемых с использованием информационных технологий.

Список литературы

1. Голосов П. Куда ведет цифровая трансформация государства? // Сетевое издание «Ведомости». [Электронный ресурс]. – URL: https://www.vedomosti.ru/25/tsifrovoe_gosudarstvo/articles/2024/07/01/1047284-kuda-vedet-tsifrovaya-transformatsiya-gosudarstva (дата обращения: 10.07.2024).

2. Винницкая А. Мошенники страшнее смертной казни. // Газета Коммерсант. 2024. 11 мая. [Электронный ресурс]. – URL: https://www.kommersant.ru/doc/6689394 (дата обращения: 10.07.2024).

3. Постановление Правительства Республики Башкортостан от 05.02.2024 № 28 «Об утверждении государственной программы «Обеспечение общественной безопасности в Республике Башкортостан» и о признании утратившими силу некоторых постановлений Правительства Республики Башкортостан». Доступ из справ.-правовой системы «КонсультантПлюс». [Электронный ресурс]. – URL: http://publication.pravo.gov.ru/document/0200202402120007?ysclid=m0s64khy5t104110170 (дата обращения: 10.07.2024).

4. Колычева А. Н. Механизм совершения мошенничества с использованием подмены телефонного номера // Современное уголовно-процессуальное право – уроки истории и проблемы дальнейшего реформирования. 2020. Т. 1, № 1(2). С. 302–308.

5. Смирнов Г. ФСБ задержала пять человек по делу об «украинских call-центрах» и ₽7 млрд // Сетевое издание «РБК». [Электронный ресурс]. – URL: https://www.rbc.ru/politics/08/04/2024/661399849a7947d8c59ee6e4?ysclid=lyu3blvelm946756084 (дата обращения: 10.07.2024).

6. Архипов Д. Число звонков от мошенников упало в 5 раз после ударов РФ по объектам на Украине // Сетевое издание «Газета.ру». [Электронный ресурс]. URL: https://www.gazeta.ru/social/news/2024/07/19/23492713.shtml (дата обращения: 10.07.2024).

7. Балыкова Н. Жители Башкирии перечислили мошенникам 2,5 млрд рублей с начала года // Сетевое издание «Коммерсантъ». [Электронный ресурс]. URL: https://www.kommersant.ru/doc/6424681?from=2_top_main_6 (дата обращения: 10.07.2024).

8. Исакова Т. Разделяй и защищай // Коммерсантъ. 2024, 24 мая. С. 7.

9. О внесении изменений в Кодекс Российской Федерации об административных правонарушениях: Федеральный закон Российской Федерации от 30 декабря 2021 г. № 480-ФЗ // Официальный интернет-портал правовой информации. [Электронный ресурс]. URL: www.pravo.gov.ru (дата обращения: 10.07.2024).

10. Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс» [Электронный ресурс]. – URL: https://www.consultant.ru/document/cons_doc_LAW_34661/?ysclid=m0s68mbuop17134260 (дата обращения: 10.07.2024).

11. По инициативе прокуроров операторы связи привлекаются к ответственности за пропуск вызова с подменного телефонного номера // Официаль-

ный сайт Прокуратуры Республики Башкортостан. 2023. 31 августа. [Электронный ресурс]. URL: https://epp.genproc.gov.ru/web/proc_02/mass-media/news/archive?item=89957211 (дата обращения: 10.07.2024).

12. Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс». [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_34661/?ysclid=m0s68mbuop17134260 (дата обращения: 10.07.2024).

13. Антонова Е. Ю. Преступления террористической направленности в эпоху цифровизации: формы деятельности и меры по противодействию. Journal of Digital Technologies and Law. 2023. № 1(1). С. 251–269. DOI: https://doi.org/10.21202/jdtl.2023.10 ; EDN: HFPMTN

Н. Н. Бойко,
кандидат юридических наук, доцент,
Уфимский университет науки и технологии,
Стерлитамакский филиал

РАССМОТРЕНИЕ ВОПРОСОВ ПРАВОВОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация. Статья посвящена исследованию проблем, связанных с обеспечением информационной безопасности. Круг исследуемых правоотношений является относительно новым явлением в российском правовом поле, в связи с чем они надлежащим образом не урегулированы нормами отечественного права. Кроме того, данные отношения развиваются стремительно, что обуславливает необходимость оперативного реагирования на новшества в сфере информационной безопасности. Необходимость в обеспечении информационной безопасности очерчена в Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы, утвержденной Президентом России. В силу того, что количество угроз в рассматриваемой сфере выросло, предлагается их классификация, что позволит выработать более эффективные меры по борьбе с данными явлениями.

Ключевые слова: право, цифровые технологии, интернет-технологии, информационное общество, информационная безопасность, угрозы информационной безопасности, кибербуллинг, несовершеннолетние, обеспечение безопасности личности

CONSIDERATION OF LEGAL SUPPORT ISSUES INFORMATION SECURITY

Abstract. The present article is devoted to the study of problems related to the provision of information security. The range of legal relations under study is a