Дата поступления рукописи в редакцию: 23.01.2026 г.
Дата принятия рукописи в печать: 31.01.2026 г.
DOI: 10.24412/2782-3849-2026-1-458-461

ЯЛОВЕНКО Татьяна Васильевна,
заместитель начальника кафедры теории и истории
Волгоградской академии МВД России,
кандидат юридических наук, доцент, полковник полиции,
e-mail: mail@law-books.ru

ОСМАНОВ Мухамед Мартинович,
старший преподаватель кафедры
организации правоохранительной деятельности
Северо-Кавказского института повышения квалификации
сотрудников МВД (филиал) Краснодарского университета МВД России,
кандидат педагогических наук, подполковник полиции,
e-mail: muhamedosmanov8@gmail.com

К ВОПРОСУ О СОВЕРШЕНСТВОВАНИИ МЕТОДОЛОГИИ ПРОТИВОДЕЙСТВИЯ ИНФОРМАЦИОННОМУ ТЕРРОРИЗМУ: ПРОБЛЕМЫ ПРАВОПРИМЕНЕНИЯ И ПУТИ ИХ РЕШЕНИЯ

Аннотация. *Автором в своей научной статье проводится анализ влияния информационного терроризма на национальную безопасность государства и негативные последствия влияние террористических актов с применением информационно-коммуникационных технологий на систему национальной безопасности современного государства.*

Ключевые слова: *киберпреступность, кибертерроризм, мошенничество, компьютерные преступники, информационно- телекоммуникационные технологии, кибермошенники, информационная среда, безопасность, органы внутренних дел, противодействие, ответственность, законодательство, защита информации, государство.*

YALOVENKO Tatyana Vasilyevna,
Deputy Head of the Department of Theory and History
Volgograd Academy of the Ministry of Internal Affairs of Russia
Candidate of Law, Associate Professor, Police Colonel

OSMANOV Mukhamed Martinovich,
Senior Lecturer at the Department of Organization of Law Enforcement Activities
of the North Caucasus Institute for Advanced Training of Ministry of Internal Affairs Officers
(branch) of the Krasnodar University of the Ministry of Internal Affairs of Russia,
Candidate of Pedagogical Sciences, Police Lieutenant Colonel.

ON IMPROVING METHODOLOGIES FOR COUNTERING INFORMATION TERRORISM: LAW ENFORCEMENT CHALLENGES AND SOLUTIONS

Annotation. *In this research article, the author analyzes the impact of information terrorism on the national security of the state and the negative consequences of terrorist attacks using information and communication technologies on the national security system of a modern state.*

Key words: *cybercrime, cyberterrorism, fraud, computer criminals, information and telecommunications technologies, cyber fraudsters, information environment, security, law enforcement agencies, counteraction, liability, legislation, information protection, state.*

Российская Федерация в настоящее время сталкивается с различными вызовами, которые направлены на обеспечение внешнего и внутреннего развития. Как отмечено в первой главе одним из важнейших направлений является обеспечение национальной безопасно-

сти и совершенствование механизмом противодействия различным угрозам национальной безопасности, в том числе противодействие кибертерроризму, который является реальной угрозой национальной безопасности РФ.

Отсутствие научного и правового разъяснения понятия «информационный терроризм (кибертерроризм)» в российской системе законодательства является наиболее существенным недостатком. Четкое определение термина «информационный терроризм (кибертерроризм)» не представлено ни в одном нормативно-правовом акте.

Данное обстоятельство не предоставляет возможности выделения его структурных компонентов.

Очень важной является регламентация понятия «информационный терроризм (кибертерроризм)»

В Доктрине информационной безопасности Российской Федерации отмечается значимость совершенствования профилактических мер, направленных на повышение уровня информационной безопасности, одним из механизмов совершенствования является использование ИКТ. Данный документ является составным компонентом общей системы обеспечения информационной безопасности. Разработку доктрины следует рассматривать как нормативно-правовой механизм совершенствование мер противодействия информационному терроризму.

Следует отметить, что в системе ОВД имеются и положительные практики совершенствования в целом системы противодействия киберпреступлениям:

– в 2022 году было создано Управления по организации борьбы с противоправным использованием IT-технологий (УБК МВД России).

Структурное подразделение было создано в целях координации деятельности по борьбе с киберпреступностью в системе МВД. УБК МВД России проводит анализ данных и осуществляет взаимодействие с другими органами правоохранительной системы;

– внедрены меры мер виктимологической профилактики киберпреступлений, к примеру, это применение современных ИКТ и инновационных технологий.

Таким образом, для отдельных граждан, общества и государства информационный терроризм − это серьезная угроза и глобальная проблема современного человечества. Это обуславливает необходимость принятия комплекса мер по совершенствованию в целом системы противодействия киббертерроризму.

В целях выявления актов кибертерроризма и осуществления эффективной борьбы с ним необходимо разрабатывать эффективные стратегии и развивать технологии по выявлению киберпреступлений террористического характера, проводить активную пропагандистскую политику в целях повышения информационной грамотности населения и формирования критического мышления. Противодействие информационному терроризму в РФ является компонентом борьбы с международным терроризмом, что требует использования соответствующих механизмов противодействия.

В настоящее время можно констатировать, что законодательство не успевает адаптироваться к новым технологиям.

Основной массив законодательства, регулирующего киберпространство и цифровые технологии, был принят задолго до появления современных Интернет-сервисов и мобильных приложений, что влечет за собой правовые коллизии.

В свою очередь рассмотрим основные направления и задачи выполняемые правоохранительными органами в области борьбы с противоправными проявлениями в сети Интернет:

1) получение и предоставление подлинных сведений о мотивах и обстоятельствах, подтолкнувших к совершению преступлений и обнаружение инициаторов и участников и иных лиц за устранение выявленных факторов распространения, разработка предложений по мерам, направленным на устранение выявленных негативных факторов и условий;
2) периодически посредством использования средств массовой информации обращаться к гражданам в целях проведения профилактики терроризма и экстремизма;
3) усилить на участках обслуживаемых территорий патрулирование;
4) обеспечить эффективную защиту от возможных террористических, кибертеррористических проявлений особенно при проведении массовых мероприятий.
5) проведение оперативных действий по выявлению и пресечению деятельности транснациональных, межрегиональных организованных групп и преступных сообществ, которые совершают преступления террористического и экстремистского характера с применением информационно-коммуникационных и инновационных технологий;
6) раскрытие преступных действий, относящихся к компетенции ведомства;
7) осуществление оперативного сопровождения уголовных дел, участие в процессе следственных действий и выполнение поручений следователя;
8) разработка единых и системных механизмов в сфере пресечения, предотвращения

негативных воздействий на информационно-коммуникационные ресурсы, формирование максимально безопасной системы оборота в информационно-телекоммуникационных сетях достоверной информации, в том числе и в глобальной сети;

9) проведение мероприятий по поиску в глобальной сети потенциальных угроз, которые направлены на нарушение информационной безопасности отдельных граждан, общества и государства в целом, также поиск информации, которая под запретом к распространению в РФ;
10) принятие и реализация профилактических и эффективных мер, по устранению причин и обстоятельств обусловивших совершение преступных действий террористического и экстремистского характера;
11) принятие участия в проведении мероприятий, обеспечивающих доступ, съемку и фиксацию информации, которая хранится на специальных носителях и информационно-телекоммуникационном пространстве.

Организация деятельности органов внутренних дел Российской Федерации по противодействию преступлениям совершаемым в сети Интернет, по своей сути является весьма трудоемким процессом требующим больших усилий в организации выявления и пресечения противоправных действий и навыков в работе с интернет ресурсами в рассматриваемой сфере, требующей дальнейшей проработке способствующей эфективному противодействию киберпрестплений и по сему необходимо на постоянной основе совершенствовать навыки и новые технологии и в борьбе с информационными преступлениями, в том числе применяя методы воздействия посредствам комплексного взаимодействия между заинтересованными службами и подразделениями различных ведомств.

В заключении целесообразно отметить, что деятельность правоохранительных органов касаемо вопросов эффективного противодействия информационному терроризму связана с рядом дилемм и в результате детального разбора определены наиболее возможные причины их возникновения.

В виду чего и по результатам проведенного исследования служебной деятельности органов внутренних дел по предупреждению и пресечению преступлений в информационном пространстве, предлагаются следующие способы и методы по усовершенствованию путей противодействия:

– внесение изменения в систему нормативно-правового регулирования данной области; разработка и внедрение информационно-коммуникационных технологий, инновационных технологий при разработке механизмов противодействия информационному терроризму;
– реализация мероприятий, направленных на совершенствование технического оснащения специализированных подразделений органов внутренних дел;
– реализация мер, направленных на подготовку и повышение квалификации сотрудников, осуществляющих функции по противодействию кибертерроризму.

Реализацию выше обозначенных рекомендации необходимо выполнять в посредствам комплексного использования сил и средств территориальных органов внутренних дел в рамках внутриведомственного и в зависимости от складывающейся оперативной обстановки и рост числа преступлений в сфере информационно-коммуникационных технологий и посредством обеспечения внешнего ведомственного и межведомственного взаимодействия и международного сотрудничества, при этом учитывая и возможные факты связанные с влиянием различных внешних факторов.

Также стоит отметить, что в рамка реализации предложенных методов как путей решения и способов эффективного противодействия киберпреступлениям допустимо внесение изменений и дополнений с учетом определенных ситуаций, требующих оперативного вмешательства.

Список литературы:

[1] О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена: Указ Президента РФ от 17.03.2008 г. № 351 (ред. от 22.05.2015) // СПС «КонсультантПлюс» (дата обращения: 15.06.2025).

[2] О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы: Указ Президента РФ от 09.05.2017 г. № 203 // СПС «КонсультантПлюс» (дата обращения: 15.06.2025).

[3] О безопасности критической информационной инфраструктуры Российской Федерации: федеральный закон от 26.07.2017 № 187-ФЗ. (в ред. Федерального закона от 10.07.2023 № 312-ФЗ). // Собрание законодательства РФ. 31.07.2017 № 31 (1 ч.) ст. 4736.

[4] О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ: Указ Президента РФ

от15.01.2013 г. № 31с (ред. от 22.12.2017) // СПС «КонсультантПлюс» (дата обращения: 15.06.2025).

[5] О противодействии терроризму: федеральный закон от 06.03.2006 № 35-ФЗ (ред. 28.02.2025) // Собрание законодательства РФ от 13.03.2006 N 11 ст. 1146.

[6] О некоторых вопросах судебной практики по уголовным делам о преступлениях террористической направленности: постановление Пленума Верховного Суда РФ от 09.02.2012 № 1 (послед.ред.) // Бюллетень верховного СУДА РФ. № 4. апрель 2012.

[7] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 24.06.2025) // Собрание законодательства РФ. 17.06.1996 № 25 ст. 2954.

References:

[1] On measures to ensure information security of the Russian Federation when using information and telecommunication networks of international information exchange: Decree of the President of the Russian Federation of 17.03.2008 No. 351 (as amended by 22.05.2015) //SPS ConsultantPlus (date of reference: 15.06.2025).

[2] On the Strategy for the Development of the Information Society in the Russian Federation for 2017-2030: Decree of the President of the Russian Federation of 09.05.2017 No. 203//SPS “Consultant-Plus” (date of appeal: 15.06.2025).

[3] On the Security of the Critical Information Infrastructure of the Russian Federation: Federal Law No. 26.07.2017 of 187-FZ. (as amended by Federal Law No. 312-FZ of 10.07.2023) .//Collection of Legislation of the Russian Federation. 31.07.2017 No. 31 (1 h.) Art. 4736.

[4] On the creation of a state system for detecting, preventing and eliminating the consequences of computer attacks on information resources of the Russian Federation: Decree of the President of the Russian Federation dated January 15, 2013 No. 31c (as amended by 22.12.2017) //SPS ConsultantPlus (date of appeal: 15.06.2025).

[5] On countering terrorism: federal law of 06.03.2006 No. 35-FZ (ed. 28.02.2025) //Collection of legislation of the Russian Federation of 13.03.2006 No. 11, article 1146.

[6] On some issues of judicial practice in criminal cases of terrorist crimes: decision of the Plenum of the Supreme Court of the Russian Federation of 09.02.2012 No. 1 (last ed.)//Bulletin of the Supreme Court of the Russian Federation. № 4. April 2012.

[7] The Criminal Code of the Russian Federation of 13.06.1996 No. 63-FZ (as amended on 24.06.2025) //Collection of Legislation of the Russian Federation. 17.06.1996 No. 25 Art. 2954.

