Дата поступления рукописи в редакцию: 23.01.2026 г.
Дата принятия рукописи в печать: 31.01.2026 г.
DOI: 10.24412/2782-3849-2026-1-167-170

КОНОПЛЯНИКОВА Марина Викторовна,
доцент кафедры государственных и гражданско-правовых дисциплин
Московского областного филиала МосУ МВД России имени В.Я. Кикотя,
кандидат педагогических наук, полковник полиции,
e-mail: Konoplyanikova-m@mail.ru

ГОНЧАРОВА Дарья Анатольевна,
доцент кафедры теории и истории права и государства
Волгоградской академии МВД России
кандидат филологических наук, капитан полиции,
e-mail: mail@law-books.ru

СОВРЕМЕННЫЕ ПОДХОДЫ И СРЕДСТВА БОРЬБЫ ГОСУДАРСТВА С КИБЕРТЕРРОРИЗМОМ В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ

Аннотация. *В рамках настоящего научного исследования проводится комплексный анализ влияния феномена информационного терроризма на уровень национальной безопасности государства. Важное значение уделяется исследованию разрушительных последствий террористических актов, осуществляемых с использованием информационных технологий, для функционирования системы национальной безопасности современного государства.*

Ключевые слова: *кибертерроризм, преступность в сети, интернет, цифровизация, борьба, методы, киберпреступность, государство, превентивные меры, технологии, безопасность страны, законодательство.*

KONOPLYANIKOVA Marina Viktorovna,
Associate Professor of the Department of State and Civil Law Disciplines
of the Moscow Regional Branch of the Moscow University
of the Ministry of Internal Affairs of Russia named after V.Ya. Kikotya,
candidate of pedagogical sciences, police colonel

GONCHAROVA Darya Anatolyevna,
Associate Professor, Department of Theory and History of Law and State
Volgograd Academy of the Ministry of Internal Affairs of Russia
Candidate of Philological Sciences, Police Captain

MODERN APPROACHES AND MEANS OF STATE COUNTERACTION TO CYBERTERRORISM IN THE INFORMATION SPACE

Annotation. *This research study provides a comprehensive analysis of the impact of the phenomenon of information terrorism on the level of national security.*

Important attention is paid to the study of the devastating consequences of terrorist attacks carried out using information technology for the functioning of the national security system of a modern state.

Key words: *cyberterrorism, online crime, internet, digitalization, combating, methods, cybercrime, state, preventive measures, technology, national security, legislation.*

Прогрессирующее развитие информационных технологий абсолютно меняет современное общество, открывая новые горизонты для их использования.

Цифровые инновационные технологии и новые возможности его применения в данной сфере сделали информацию, услуги и товары доступнее и быстрее, чем когда-либо представлялось возможным их использование.

Без сомнения актуально отметить, что данная цифровая революция создает и серьезные дилеммы, а именно, к примеру широкое распро-

странение и увеличение фактов и последствий преступлений в информационной сфере и способствует совершению киберпреступлений.

Само определение, включает в себя большое количество противоправных деяний злоумышленников, промышляющих в информационном пространстве, с использованием вредоносных программных обеспечению способствующих утечке информации и краже банковских данных потерпевших от противоправных действии злоумышленников.

В рамках прогрессирующего развития информатизации, государство обозначает приоритетной задачу обеспечения устойчивого и долгосрочного развития Российской Федерации как стратегическое направление государственной политики в противодействии преступлениям в информационной сфере.

Создание системы национальной безопасности современного государства должно реализовываться с применением современных информационных технологий.

Активное развитие информационных технологий способствует обеспечению инновации и усовершенствованию возможностей в сфере информационного пространства для современного общества.

Инновации в сфере информационно- коммуникационных технологий обеспечили доступность сведений, услуг и товаров, также упростили и ускорили процесс получения необходимой информации.

Но, вместе с тем развитие информационных технологий создали и серьезные проблемы, к примеру:

1) увеличение числа преступлений в сети Интернет;
2) преступления с использованием информационных ресурсов, среди которых: компьютерное мошенничество, фишинг, кибершантаж, кибешпионаж, вымогательство, киберджекинг и т.д.

В условиях активного развития цифровизации, государство стремится обеспечить более устойчивое развитие страны, что является актуальным приоритетным на данном этапе в сфере борьбы с преступностью в рассматриваемой сфере.

Национальная безопасность должна формироваться с использованием современных и инновационных информационных возможностей, что выделяет ее важность в обеспечении эффективного взаимодействия государственных органов в сфере информационной защиты.

В условиях осуществления противодействия преступлениям в сети Интернет, необходимо проанализировать специфические способы и методы реализуемой деятельности правоохранительных органов.

Изучение их организационной структуры поможет определить уязвимые направления в их деятельности и неэффективные способы противодействия киберпреступлениям и будет способствовать выработке новых современных и эффективных методов борьбы с преступлениями в информационной сфере и повысит качество работы структурных подразделений, специализирующихся на противодействии кибертерроризму.

Важно отметить, что основной особенностью государственной политики противодействия терроризму в информационной сфере является сама информационная среда.

Борьба в этом векторе противодействия преступности состоит в на нанесении значительного информационного ущерба, поскольку информация является главным инструментом в руках преступников.

В сложившейся ситуации информационное противодействие терроризму является критически важным элементом информационной борьбы.

Это связано с тем, что субъекты таких действий стремятся оказать управляющее информационное воздействие на выбранные цели, используя деструктивную информацию.

В политологии существует множество подходов к анализу факторов, которые формируют приоритеты государственной политики и определяют ее развитие.

Российская Федерация, в соответствии со своей Конституцией, обязуется защищать личность, общество и государство от различного рода проявлений преступлений террористического характера, в том числе и в информационном пространстве

Начальствующий субъект различных федеральных органов исполнительной власти являются представителями Национального антитеррористического комитета, которые непосредственно занимаются обеспечением антитеррористической защиты и безопасности на уровне решения важных государственных вопросов, связанных с обеспечением безопасности общества и государства в том числе и противодействию преступлениям террористического и криминального характера в том числе в информационной сфере.

Такого рода методика национальной безопасности способствует объединению возможностей всех органов исполнительной власти, на всех уровнях и в пределах компетенции и способствует обеспечению применения комплекса усилий и задействовать различных представителей определенных структур власти и управления в стране.

Зачастую, сотрудникам органов внутренних дел и иным заинтересованным службам трудно вычислить каналы финансирования, спонсирующие преступников для реализации противоправных действий террористического характера, и данная дилемма создает затруднения в завершении расследований и доведения дел до судебного разбирательства.

В связи с чем, очень важно проработать качественный и эффективный способ воздействия на данную ситуацию и способствовал бы решению данного вопроса.

Кибертеррористы активно применяют разнообразные методы атак для осуществления своих преступных замыслов.

Крайне необходимо осознавать, что используемые ими инструменты дают им возможность получать доступ к различным типам данных, перехватывать информацию и нарушать нормальное функционирование сетевых коммуникаций.

Безусловно, экономическое положение страны напрямую влияет на уровень преступности, включая распространение преступлений в сети Интернет.

Складывающиеся в современном обществе негативные экономические явления, зачастую и становятся своего рода мотиваторами и причиной увеличения преступности в том числе и в рассматриваемой сфере и способствуют дальнейшему развитию киберпреступлений.

Важно выделить отметить, что такого рода обстоятельство, бытующее в обществе, является объектом разбирательства не только лишь в правоохранительной сфере, но и носит транснациональный характер, что в свою очередь обуславливает применение комплексного подхода для разрешения данного вопроса по профилактике и противодействию преступлениям в данной сфере и на международном уровне посредствам сотрудничества с заинтересованными службами и подразделений.

Актуально отметить, что информационно-коммуникационные ресурсы и специализированное программное обеспечение являются основным инструментом для киберпреступников.

Преступления террористического характера в данной сфере носят и международный характер, потому что географические границы безграничны, в результате чего злоумышленники могут совершать киберпреступлентя находясь на территории одной страны и осуществлять посягательство и реализовывать свой преступления в отношении определенных объектов, находящихся на территории другого государства.

Стоит отметить, что противодействие преступления террористического характера должно реализовываться с непосредственным применением информационных технологий, а не только лишь применение нормативно-правовых актов, поскольку это будет способствовать использованию навыков специалистов в данной сфере и модернизации существующих, а также созданию новых технологий для оперативного выявления и нейтрализации несанкционированных вторжений в информационные системы, а подготовка специалистов высокого уровня является фундаментальным аспектом в совершенствовании стратегий противодействия кибертерроризму.

Также необходимо внедрение более строгих процедур профессионального отбора, предполагающих конкурсный принцип формирования кадрового состава.

В продолжении отметим, что поскольку разрушительное влияние оказывается на систему национальной безопасности и влечет за собой крайне негативные последствия, вплоть до нарушения территориальной целостности государства и дестабилизации общественных устоев.

Неоднократно проводились исследования влияния информационного терроризма на систему информационной безопасности как составной части национальной безопасности.

На основании вышеуказанного и в заключении проведенного исследования необходимо отметить, что государство реализует комплексную политику в сфере противодействия терроризму и его разновидностям, а деятельность правоохранительных органов осуществляется в соответствии с установленными государством приоритетами.

Противодействие кибертерроризму предполагает использование передовых информационных инструментов и инновационных технологий.

Совершенствование существующих и разработка новых инструментов для борьбы с кибертерроризмом требует применения исключительно научного подхода.

Список литературы:

[1] Об утверждении Доктрины информационной безопасности Российской Федерации: Указ Президента РФ от 5.12.2016 г. № 646 // СПС «КонсультантПлюс» (дата обращения: 15.06.2025).

[2] 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).

[3] Об информации, информационных технологиях и о защите информации: федеральный закон от 27.07.2006 № 149-ФЗ. (ред. от 01.04.2025) // Собрание законодательства РФ. 31.07.2006 № 31 (1 ч.) ст. 3448.

[4] 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).

[5] 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.

References:

[1] On approval of the Information Security Doctrine of the Russian Federation: Decree of the President of the Russian Federation of 5.12.2016 No. 646//SPS “ConsultantPlus” (date of appeal: 15.06.2025).

[2] 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).

[3] On Information, Information Technology and Information Protection: Federal Law No. 27.07.2006 of 149-FZ. (as amended by 01.04.2025) //Collection of Legislation of the Russian Federation. 31.07.2006 No. 31 (1 h.) Art. 3448.

[4] 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).

[5] 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.