

2. О противодействии терроризму : федеральный закон от 6 марта 2006 г. № 35-ФЗ. Доступ из справочно-правовой системы «Гарант.ру».

3. Остапенко А. А. Виды цифровых доказательств в административном судопроизводстве // StudNent. 2021. № 5.

4. Куликова Я. А. Цифровые технологии в процессе доказывания в производстве по делам об административных правонарушениях // Административное и муниципальное право. 2024. № 6. С. 81–99.

5. Соколов А. Ю. Правовая политика в области использования цифровых технологий в производстве по делам об административных правонарушениях // Вестник СГЮА. 2023. № 1 (150). С. 118–121.

© Терехов М. Г., 2026

УДК 340.1

Тулбаева Д. Т. – доцент кафедры административно-правовых дисциплин Карагандинской академии МВД Республики Казахстан имени Б. Бейсенова (Республика Казахстан, г. Караганда)

ИНФОРМАЦИОННЫЙ ТЕРРОРИЗМ КАК СОВРЕМЕННАЯ УГРОЗА НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ: ПРОБЛЕМЫ, ПУТИ РЕШЕНИЯ

INFORMATION TERRORISM AS A MODERN THREAT TO NATIONAL SECURITY: PROBLEMS AND SOLUTIONS

Аннотация. В статье рассматривается информационный терроризм как одна из наиболее опасных форм современных угроз в условиях глобализации и цифровизации. Выделяются ключевые проблемы противодействия, предлагаются комплексные пути их решения и анализируются возможные последствия как при эффективной реализации мер, так и при их отсутствии.

Ключевые слова: информационный терроризм, киберинциденты, глобализация, киберугроза.

Abstract. The article examines information terrorism as one of the most dangerous forms of modern threats in the context of globalization and digitalization. The key problems of counteraction are highlighted, comprehensive ways of their solution are proposed, and possible consequences are analyzed both in case of effective implementation of measures and in case of their absence.

Keywords: information terrorism, cyber incidents, globalization, cyber threat.

Современный мир переживает период глубинных трансформаций. С усилением геополитической напряженности в мире происходит перераспределение влияния, нарастает гонка вооружений, а также формируются новые формы угроз безопасности мирового сообщества, которые часто носят скрытый и неочевидный характер. Словосочетание «Холодная война» стало не просто термином, так как уровень напряженности в мире нарастает, что не может не отразиться на ходе «Часов судного дня». Мировое научное сообщество предполагает (Bulletin of Atomic Scientists), что угрозы мировой информационной безопасности представляют совпадение сразу нескольких факторов, таких как ослабевание международной системы безопасности, развитие информационных технологий, опережающее формирование системы упреждающего контроля. На этом фоне цифровые технологии стали не просто инструментом развития, а новым «полем боя» в обеспечении национальной безопасности государства и общества.

Согласно отчету глобального индекса терроризма в 2025 году число террористических атак достигло 2944, при этом от рук террористов погибло 5 582 человека [1], по сравнению с 2024 годом произошло количественное снижение, при этом на фоне заметного снижения числа атак наблюдается усложнение тактики, фрагментация факторов и рост значимости технологических инструментов, используемых террористами, а именно: активное использование беспилотных летательных аппаратов (БПЛА) в конфликтах, удары по инфраструктуре. Целью становится не захват территорий, а дестабилизация экономики. Из анализа данных можно сделать вывод, что информационный терроризм выступает в роли перспективного негативного тренда, который с годами будет набирать обороты и оказывать все большее неблагоприятное воздействие на мировое сообщество.

Сегодня невозможно представить устойчивое развитие ни в одной сфере без информационно-коммуникационных технологий. Государственное управление, финансовая система, правоохранительная деятельность, здравоохранение, образование – все ключевые сферы зависят от цифровой инфраструктуры. Однако вместе с возможностями растут и угрозы. Одной из самых опасных из них является информационный терроризм.

Информационный терроризм в современных условиях представляет собой качественно новую форму террористической деятельности, которая возникла в результате развития информационно-коммуникационных технологий и трансформации традиционной формы угрозы национальной безопасности. Несмотря на то, что сам термин был введен в научный оборот еще в 1980-х годах, его содержательное наполнение до настоящего времени остается дискуссионным, что обусловлено быстрыми темпами внедрения цифровых технологий в жизнь общества и многообразием форм противоправного поведения в информационном пространстве.

В общепринятом представлении информационный терроризм можно рассматривать как преднамеренное использование информационных тех-

нологий для совершения атак, направленных на достижение террористических целей, включая дестабилизацию общественных отношений, подрыв функционирования государственных институтов, оказание давления на органы власти, а также формирование атмосферы страха и неопределенности в обществе.

В отличие от иных форм киберпреступности, информационный терроризм имеет ярко выраженную политико-идеологическую направленность, основной целью которого является дисбаланс общественного порядка и причинение стратегических последствий. Особую опасность представляет то, что такие атаки могут быть направлены на объекты жизнеобеспечения общества – энергетику, транспорт, здравоохранение, оборонные системы.

В доктринальном плане информационный терроризм следует рассматривать не только как совокупность отдельных противоправных деяний, но как сложное социально-правовое явление, обладающее системными признаками. Особого внимания заслуживает проблема разграничения информационного терроризма, киберпреступности и актов кибервойны. В юридической плоскости данное разграничение осложняется совпадением объективной стороны деяний (например, несанкционированный доступ к информационным системам) при различии их субъективных целей и последствий. В этой связи ключевым критерием квалификации информационного терроризма выступает именно террористическая направленность – стремление к устрашению населения, воздействию на принятие решений органами государственной власти либо дестабилизации общественного порядка.

К числу специфических признаков информационного терроризма следует отнести его транснациональный характер, анонимность субъектов, высокую латентность и асимметричность воздействия. В отличие от традиционных форм терроризма, информационная террористическая атака может быть осуществлена дистанционно с минимальными ресурсными затратами, но при этом иметь последствия, сопоставимые с масштабными техногенными или даже военными угрозами.

Информационный терроризм следует квалифицировать как комплексное, многоуровневое явление, обладающее высокой степенью общественной опасности и требующее адекватного правового осмысления. Его исследование и нормативное закрепление должны осуществляться с учетом междисциплинарного подхода, объединяющего достижения юридической науки, информационных технологий и теории безопасности.

При определении подходов противодействия информационному терроризму необходимо формировать комплексную и внутренне согласованную систему мер, ориентированную на адекватное реагирование на вызовы цифровой эпохи. При этом речь должна идти не о фрагментарном совер-

шенствовании отдельных элементов, а о выработке целостной концепции, интегрирующей правовые, институциональные и технологические механизмы обеспечения безопасности.

В первую очередь приоритетным направлением выступает совершенствование нормативно-правовой базы. Представляется обоснованным формирование четкого и научно выверенного определения информационного терроризма, закреплённого на законодательном уровне. Такое определение должно учитывать как технологическую специфику деяния, так и его целевую направленность, связанную с террористическим воздействием на общество и государство. Кроме того, необходима гармонизация национального законодательства с международными правовыми стандартами, что позволит обеспечить единообразие подходов к квалификации и преследованию соответствующих деяний.

Не менее значимым направлением является институциональное укрепление механизмов противодействия. В современных условиях особую роль приобретает создание специализированных подразделений и межведомственных центров, обеспечивающих мониторинг, предупреждение и оперативное реагирование на информационные угрозы. Эффективность их деятельности во многом зависит от уровня синергии между государственными органами, включая правоохранительные структуры, органы национальной безопасности и регуляторов в сфере информационных технологий.

С учетом транснационального характера информационного терроризма принципиальное значение приобретает развитие международного сотрудничества. Представляется необходимым активизировать участие государств в многосторонних соглашениях, направленных на противодействие информационным угрозам, а также совершенствовать механизмы обмена информацией и проведения совместных операций. В данном контексте особую актуальность приобретает формирование единых стандартов и процедур взаимодействия, способных обеспечить оперативность и эффективность реагирования.

Отдельного внимания требует обеспечение безопасности критической инфраструктуры. В условиях возрастающей зависимости государства от цифровых систем приоритетной задачей становится внедрение современных технологий защиты, регулярное проведение аудита информационных систем, а также разработка сценариев реагирования на возможные киберинциденты. Важным элементом является также формирование механизмов резервирования и устойчивости систем, способных минимизировать последствия возможных атак.

Существенную роль в повышении эффективности противодействия информационному терроризму играет развитие кадрового потенциала. Подготовка высококвалифицированных специалистов в области информационной безопасности, повышение квалификации сотрудников правоохрани-

нительных органов, а также развитие научных исследований в данной сфере должны рассматриваться как стратегическое направление государственной политики. В условиях постоянного усложнения технологий именно человеческий фактор во многом определяет способность системы безопасности адекватно реагировать на угрозы.

Наряду с этим необходимо уделять внимание формированию культуры информационной безопасности в обществе. Повышение уровня цифровой грамотности населения, развитие навыков безопасного поведения в информационной среде и осознание рисков, связанных с использованием цифровых технологий, способны существенно снизить уязвимость общества перед киберугрозами.

Таким образом, эффективное противодействие информационному терроризму возможно лишь при условии реализации комплексного подхода, предполагающего одновременное развитие правовых, организационных, технологических и образовательных мер.

Решение обозначенных проблем требует комплексного подхода. В первую очередь необходимо совершенствовать законодательство. Это включает разработку четкого определения информационного терроризма, устранение правовых пробелов и приведения в соответствие национальных норм с международными стандартами.

Важнейшим направлением является развитие международного сотрудничества. Эффективная борьба с транснациональными угрозами невозможна без обмена информацией, совместных операций и согласованных стратегий.

Особое внимание должно уделяться защите критической инфраструктуры. Регулярный аудит систем, внедрение современных средств киберзащиты и создание механизмов оперативного реагирования способны существенно снизить риски.

Не менее значима подготовка кадров. Формирование профессионального сообщества специалистов по информационной безопасности, развитие научных исследований и повышение квалификации сотрудников правоохранительных органов являются ключевыми условиями успеха.

Кроме того, необходимо повышать цифровую грамотность населения. Человеческий фактор остается одним из самых уязвимых элементов системы безопасности.

Реализация предложенных мер способна привести к существенному укреплению национальной безопасности. Снижение количества кибератак, повышение устойчивости инфраструктуры и рост доверия к государственным институтам создадут условия для стабильного развития цифровой экономики.

В то же время игнорирование проблемы может иметь крайне негативные последствия. Кибератаки способны парализовать работу государ-

ственных органов, разрушить экономические связи, вызвать массовую панику и подорвать социальную стабильность. Утечка конфиденциальной информации и воздействие на стратегические объекты могут привести к долгосрочным кризисам.

Информационный терроризм – это не гипотетическая угроза будущего, а реальность настоящего. Эффективное противодействие возможно только при условии системного подхода, объединяющего правовые, технологические и организационные меры. В противном случае киберпространство рискует превратиться в ключевую арену деструктивного воздействия на безопасность государств и общества.

Библиографический список

1. Global terrorism index 2026. URL: <https://www.visionofhumanity.org/wp-content/uploads/2026/03/Global-Terrorism-Index-2026-Report.pdf> (дата обращения: 05.04.2026).
2. О противодействии терроризму : закон Республики Казахстан от 13 июля 1999 г. URL: https://adilet.zan.kz/rus/docs/Z990000416_ (дата обращения: 05.04.2026).
3. О национальной безопасности : закон Республики Казахстан от 6 января 2012 г. URL: <https://adilet.zan.kz/rus/docs/Z1200000527/z1200527.htm> (дата обращения: 05.04.2026).
4. Коркмазов А. В. Современные тенденции цифрового экстремизма и терроризма // Пробелы в российском законодательстве. 2023. Т. 16 № 4. С. 208–211.

© Тулебаева Д. Т., 2026