(cc) BY

Андрианова Елена Олеговна,
магистрант
ФГБОУ ВО «Российский государственный
социальный университет»
г. Москва

ПРАВОВАЯ КВАЛИФИКАЦИЯ КИБЕРТЕРРОРИЗМА В РОССИЙСКОЙ ФЕДЕРАЦИИ: ПРОБЛЕМЫ ДЕФИНИЦИИ И РАЗГРАНИЧЕНИЯ СМЕЖНЫХ СОСТАВОВ ПРЕСТУПЛЕНИЙ

Аннотация: *статья посвящена теоретико-правовому анализу кибертерроризма и дефектам его регламентации в Федеральном законе №35-ФЗ, порождающим латентные правоприменительные коллизии. Автор предлагает разграничительные маркеры для квалификации посягательств на стыке статей 205 и 274.1 УК РФ, доказывая приоритет политико-идеологического мотива над техническими признаками вредоносного воздействия. По итогам исследования разработаны проекты законодательных новелл для синхронизации антитеррористических норм с законодательством о безопасности критической информационной инфраструктуры.*

Ключевые слова: *кибертерроризм, противодействие терроризму, информационная безопасность, критическая информационная инфраструктура, квалификация преступлений, субъективная сторона, идеология насилия, уголовная ответственность, правовая определенность, правоприменительный дефект.*

Динамичное развитие глобальной информационной инфраструктуры и сквозное внедрение цифровых технологий во все сферы жизнеобеспечения коренным образом изменили архитектонику угроз национальной безопасности Российской Федерации. Тотальная цифровизация сформировала высокоуязвимую среду, ставшую объектом деструктивных устремлений радикальных транснациональных сообществ. В результате смещения вектора агрессии в кибернетическое пространство традиционный терроризм, исторически опиравшийся на

Content is licensed under the Creative Commons Attribution 4.0 license (CC-BY 4.0)

физическое насилие и линейные методы воздействия, претерпел глубокую эволюционную трансформацию, что привело к кристаллизации феномена кибертерроризма.

Несмотря на очевидную практическую опасность технологических угроз, отечественное законодательство и правоприменительная практика обнаруживают концептуальный дефицит. В Федеральном законе от 6 марта 2006 года №35-ФЗ «О противодействии терроризму» до сих пор отсутствует легальное определение кибертерроризма, а его понятийный аппарат ориентирован преимущественно на аналоговые формы контроля. В свою очередь, Особенная часть Уголовного кодекса РФ не содержит самостоятельной нормы, криминализирующей террористические акты в виртуальном пространстве, что порождает нормативный вакуум и правоприменительные коллизии.

В практической плоскости органы следствия и суды сталкиваются с трудностями при разграничении террористического акта (ст. 205 УК РФ), совершенного с использованием компьютерных технологий, и смежных составов – неправомерного воздействия на критическую информационную инфраструктуру (ст. 274.1 УК РФ), создания вредоносных программ (ст. 273 УК РФ) или диверсий (ст. 281 УК РФ). Отсутствие доктринально выверенных разграничительных маркеров по элементам состава (прежде всего по мотиву, целям и объекту посягательства) ведет к системным ошибкам квалификации, размыванию следственной юрисдикции и снижению эффективности Общегосударственной системы противодействия терроризму (ОГСПТ).

Развитие концепции кибертерроризма в международной и отечественной доктрине долгое время сопровождалось дискуссией между сторонниками широкого и узкого подходов. Широкий подход предлагал включать в этот контур любую деструктивную деятельность радикальных групп в сети (пропаганду, вербовку, финансирование через криптоактивы). Однако в академической науке возобладал узкий (функциональный) подход, согласно которому подлинный кибертерроризм обладает уникальным, самостоятельным способом совершения преступления – непосредственным использованием программно-аппаратного кода в

Содержимое доступно по лицензии Creative Commons Attribution 4.0 license (CC-BY 4.0)

качестве основного поражающего элемента для удаленного деструктивного воздействия на критические узлы инфраструктуры.

Современные исследователи констатируют, что ОГСПТ, созданная на базе силовой парадигмы пресечения аналоговых атак, сталкивается с феноменом платформенной уязвимости, когда защищенные физическими барьерами объекты остаются проницаемыми через цифровые системы управления (SCADA, АСУ ТП). Настоящее исследование направлено на восполнение указанных доктринальных пробелов и выработку системных предложений по модернизации антитеррористического и уголовного законодательства. Четкое нормативное конструирование дефиниций и преодоление стагнации понятийного аппарата статьи 3 Федерального закона №35-ФЗ выступают безальтернативными условиями для защиты государственных институтов в цифровую эпоху.

Список литературы

1. О противодействии терроризму : Федеральный закон от 6 марта 2006 г. №35-ФЗ : в ред : от 25.05.2026 // Официальный интернет-портал правовой информации. – URL: http://pravo.gov.ru (дата обращения: 08.09.2026). – Текст : электронный.

2. О безопасности критической информационной инфраструктуры Российской Федерации : Федеральный закон от 26 июля 2017 г. №187-ФЗ : в ред : от 08.08.2024 // СПС КонсультантПлюс : сайт. – URL: consultant.ru (дата обращения: 08.09.2026). – Текст : электронный.

3. О судебной практике по делам о преступлениях террористической направленности : Постановление Пленума Верховного Суда Российской Федерации от 9 февраля 2012 г. №1 : (в редакции от 03.11.2016) // СПС КонсультантПлюс : сайт. – URL: consultant.ru (дата обращения: 08.09.2026). – Текст : электронный.

4. Веселовский, С. С. Многостороннее сотрудничество в борьбе с транснациональным терроризмом : монография / С. С. Веселовский. – Москва : Навона, 2009. – 272 с. – ISBN 978-5-91798-005-4.

Content is licensed under the Creative Commons Attribution 4.0 license (CC-BY 4.0)

5. Горбунов, Ю. С. Терроризм и правовое регулирование противодействия ему : монография / Ю. С. Горбунов. – Москва : Молодая гвардия, 2012. – 460 с. – ISBN 978-5-235-03513-3.

6. Емельянов, В. П. Терроризм и преступления с признаками терроризирования : уголовно-правовое исследование / В. П. Емельянов. – Санкт-Петербург : Юридический центр Пресс, 2002. – 289 с. – ISBN 5-94201-052-1 // Библиотечно-издательский комплекс СФУ : сайт. – URL: sfu-kras.ru (дата обращения: 08.09.2026).

Содержимое доступно по лицензии Creative Commons Attribution 4.0 license (CC-BY 4.0)