Аносов Матфей Витальевич,
магистрант
Научный руководитель
Землин Александр Игоревич,
заслуженный деятель науки Российской Федерации,
д-р юрид. наук, профессор, заведующий кафедрой

ФГБОУ ВО «Российский государственный
социальный университет»
г. Москва

ОТВЕТСТВЕННОСТЬ ЗА ЗАВЕДОМО ЛОЖНЫЕ СООБЩЕНИЯ О ТЕРРОРИСТИЧЕСКИХ АКТАХ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

Аннотация: *статья посвящена комплексному уголовно-правовому анализу ответственности за заведомо ложные сообщения об акте терроризма в условиях цифровизации общества. Актуальность обусловлена неуклонным ростом числа таких преступлений, совершаемых с использованием социальных сетей, мессенджеров и анонимных интернет-платформ, что усиливает дестабилизирующий эффект и наносит экономический ущерб. Цель – выявление системных проблем квалификации деяния по ст. 207 УК РФ и разработка предложений по совершенствованию законодательства. Предложены дифференциация ответственности за массовое распространение ложной информации, совершенствование взаимодействия правоохранительных органов с IT-компаниями и внедрение превентивных цифровых инструментов. Сделан вывод о необходимости точечной модернизации ст. 207 УК РФ для обеспечения баланса между антитеррористической безопасностью и свободой слова.*

Ключевые слова: *заведомо ложное сообщение, акт терроризма, цифровизация, статья 207 УК РФ, киберпространство, уголовная ответственность, цифровые следы.*

Одним из наиболее острых проявлений деструктивного использования информационно-телекоммуникационных сетей стало увеличение количества заведомо ложных сообщений об актах терроризма. Если ранее для распространения такой информации требовался физический звонок или письмо, то сегодня достаточно нескольких кликов в анонимном мессенджере или публикации в социальной сети.

Скорость распространения цифрового контента приводит к тому, что ложная информация о заложенном взрывном устройстве за считанные минуты охватывает огромную аудиторию, вызывая неконтролируемую панику, массовую эвакуацию объектов социальной и транспортной инфраструктуры и парализуя работу целых городов. Действующая редакция статьи 207 Уголовного кодекса Российской Федерации (далее – УК РФ), предусматривающей ответственность за заведомо ложное сообщение об акте терроризма, была принята в эпоху, когда цифровые технологии не имели такого масштаба влияния [1].

Уголовно-правовая характеристика деяния в цифровой среде.

Объектом преступления, предусмотренного ст. 207 УК РФ, является общественная безопасность, а также нормальная деятельность государственных органов, органов местного самоуправления и организаций по обеспечению безопасности населения [3, с. 45].

В условиях цифровизации факультативным объектом все чаще выступает нормальное функционирование информационно-телекоммуникационных сетей, которые используются как орудие совершения преступления [5, с. 32].

Объективная сторона выражается в действии – сообщении о готовящихся взрыве, поджоге или иных действиях, создающих опасность гибели людей. В цифровой среде способы совершения данного преступления существенно диверсифицировались.

К традиционным формам добавились: публикация постов в социальных сетях и каналах мессенджеров, рассылка электронных писем (в том числе массовая, с использованием ботнетов), размещение комментариев на форумах, а также использование сервисов анонимной отправки сообщений. Особую

криминологическую значимость приобретает признак «заведомости», который относится к субъективной стороне преступления.

Заведомость означает, что виновный достоверно знает об отсутствии реальной угрозы теракта, но умышленно создает видимость ее наличия [6, с. 23]. В цифровом пространстве доказывание этого признака усложняется. Например, лицо может утверждать, что восприняло недостоверную информацию из другого источника как истинную и действовало из ложного чувства гражданской бдительности, а не из хулиганских побуждений или желания сорвать учебный процесс.

Субъектом преступления является вменяемое физическое лицо, достигшее 14-летнего возраста. Статистика последних лет неуклонно демонстрирует «омоложение» данного вида преступности [7]. Значительная доля ложных сообщений о минировании школ и торговых центров совершается несовершеннолетними, которые, не осознавая тяжести последствий, воспринимают свои действия как «пранк» или безобидную шутку, не подпадающую под уголовную ответственность.

Проблемы квалификации и правоприменения в условиях цифровизации.

Анализ следственной и судебной практики выявляет ряд системных проблем, препятствующих эффективному противодействию рассматриваемым деяниям [3].

Во-первых, проблема идентификации личности правонарушителя. Преступники активно используют средства анонимизации: виртуальные частные сети (VPN), подменные номера телефонов (IP-телефония), одноразовые аккаунты в мессенджерах, зарегистрированные на зарубежные сим-карты. Получение информации о владельце такого аккаунта требует направления международных правовых запросов к иностранным IT-компаниям, что в текущих геополитических условиях зачастую приводит к игнорированию запросов или затягиванию сроков их исполнения на месяцы, что недопустимо при расследовании преступлений против общественной безопасности.

Во-вторых, сложность сбора и фиксации цифровых доказательств. Цифровые следы (IP-адреса, логи серверов, метаданные сообщений) обладают

свойством волатильности – они могут быть легко и бесследно удалены как самим пользователем, так и автоматически политиками конфиденциальности платформы. Нередко следственные органы сталкиваются с необходимостью проведения комплексной компьютерно-технической экспертизы для извлечения удаленных данных, что требует высокой квалификации экспертов и значительных временных затрат.

В-третьих, проблема квалификации массового распространения (репостов). В уголовном праве дискуссионным остается вопрос о квалификации действий лиц, которые, не являясь первоисточниками ложной информации, осуществляют ее перепубликацию (репост) в своих аккаунтах с целью привлечения внимания. Если такое лицо осознает ложность информации, его действия формально содержат признаки соучастия или самостоятельного состава преступления. Однако на практике такие эпизоды редко выделяются в отдельные производства, что создает иллюзию безнаказанности и способствует вирусному распространению панических настроений.

В-четвертых, проблема разграничения преступления и административного правонарушения. В условиях информационного шума порой сложно отграничить заведомо ложное сообщение от добросовестного заблуждения или панического слуха, не имеющего конкретного адресата и деталей, что требует тщательного анализа контекста цифровой переписки [4, с. 112].

Направления совершенствования законодательства и правоприменительной практики.

Для повышения эффективности противодействия заведомо ложным сообщениям о террористических актах в цифровой среде необходим комплексный подход, включающий как законодательные, так и организационные меры [5, с. 88].

1. Модернизация диспозиции статьи 207 УК РФ. Целесообразно дополнить статью 207 УК РФ новым квалифицирующим признаком: «совершенное с использованием информационно-телекоммуникационных сетей, включая сеть «Интернет», в целях массового распространения информации». Это позволит судам назначать более строгое наказание за деяния, которые в силу цифрового охвата

причиняют существенно больший общественный вред, чем единичный телефонный звонок.

2. Совершенствование механизмов взаимодействия с IT-сектором. Необходимо законодательное закрепление обязанности для владельцев популярных мессенджеров и социальных сетей, функционирующих на территории РФ, обеспечивать хранение метаданных о фактах отправки сообщений (без содержания самой переписки, чтобы не нарушать тайну связи) в течение определенного срока и предоставлять их по мотивированному запросу следственных органов в экстренном порядке (в течение 24 часов) при поступлении сигналов о минировании в рамках исполнения норм профильного законодательства [2].

3. Внедрение превентивных цифровых технологий. Правоохранительным органам следует активнее использовать системы на базе искусственного интеллекта для мониторинга открытых источников информации на предмет наличия ключевых слов и паттернов, характерных для угроз террористического характера. Такие системы должны работать в связке с Роскомнадзором для оперативной блокировки каналов, систематически распространяющих подобного рода дезинформацию

4. Развитие правовой грамотности и профилактика среди несовершеннолетних. Учитывая высокий процент несовершеннолетних правонарушителей, необходимо внедрение в образовательные программы модулей, разъясняющих уголовно-правовые последствия «цифрового вандализма» и «своттинга». Кроме того, Верховному Суду РФ целесообразно дать дополнительные разъяснения в Постановлении Пленума о порядке оценки признака «заведомости» при совершении преступления с использованием сети Интернет, особенно в отношении лиц, не достигших 18-летнего возраста [3].

Цифровизация общества, при всех ее неоспоримых преимуществах, создала благоприятную среду для нового вида деструктивного поведения – массового и анонимного распространения заведомо ложных сообщений об актах терроризма. Действующая редакция статьи 207 УК РФ, сформированная в доцифровую эпоху, не в полной мере учитывает специфику киберпространства, что порождает

проблемы при доказывании вины, установлении личности преступника и оценке степени общественной опасности деяния [1; 4]. Проведенное исследование позволяет сделать вывод о том, что борьба с данным видом преступности не может опираться исключительно на репрессивные меры.

Необходима точечная модернизация уголовного закона путем введения квалифицирующего признака, отражающего массовый цифровой характер распространения угрозы. Параллельно с этим требуется выстраивание эффективного правового диалога с IT-компаниями для обеспечения оперативного доступа к цифровым следам, а также внедрение автоматизированных систем мониторинга [5, с. 145].

Список литературы

1. Федеральный закон «Уголовный кодекс Российской Федерации» №63-ФЗ от 13.06.1996 (ред. от 2025 г.) // Собрание законодательства РФ. – 1996. – №25. – Ст. 2954.

2. Федеральный закон «Об информации, информационных технологиях и о защите информации» №149-ФЗ от 27.07.2006 (ред. от 2025 г.) // Собрание законодательства РФ. – 2006. – №31 (ч. 1). – Ст. 3448.

3. Постановление Пленума Верховного Суда РФ «О некоторых вопросах судебной практики по делам о преступлениях террористической направленности» №47 от 29.11.2022 // Бюллетень Верховного Суда РФ. – 2023. – №2.

4. Бабий Н.А. Преступления против общественной безопасности в условиях цифровизации: монография / Н.А. Бабий. – М.: Проспект, 2023. – 288 с.

5. Землин А.И. Правовые основы противодействия терроризму в цифровой среде: учебное пособие / А.И. Землин, И.В. Мишуткин. – М.: КноРус, 2024. – 156 с. EDN WLGMVK

6. Кибальник А.Г. Проблемы субъективной стороны заведомо ложного сообщения об акте терроризма, совершенного с использованием сети Интернет / А.Г. Кибальник // Российский следователь. – 2023. – №18. – С. 22–26.

7. Судебная статистика: обзор практики рассмотрения судами дел о преступлениях против общественной безопасности за 2023–2024 годы // Судебный

департамент при Верховном Суде РФ. – URL: http://www.cdep.ru (дата обращения: 15.05.2026).