Гаркуша Виктория Михайловна
аспирант, преподаватель
Игнатьев Семён Михайлович
бакалавр, студент
ФГБОУ ВО «Кубанский государственный аграрный университет им. И.Т. Трубилина»
г. Краснодар, Краснодарский край

МЕЖДУНАРОДНО-ПРАВОВЫЕ ПРОБЛЕМЫ БОРЬБЫ С КИБЕРТЕРРОРИЗМОМ: КВАЛИФИКАЦИЯ, ЮРИСДИКЦИЯ И ПРИМЕНЕНИЯ ПРАВА САМООБОРОНЫ

Аннотация: *целью исследования является анализ ключевых международно-правовых проблем противодействия кибертерроризму. В статье рассматриваются вопросы квалификации данного явления, определения юрисдикции и возможности применения права на самооборону в соответствии со статьей 51 Устава ООН в ответ на масштабные кибератаки. На основе сравнительного анализа доктринальных подходов и существующего нормативного регулирования выявляются пробелы в международном праве, в частности, отсутствие универсального определения кибертерроризма, единого механизма атрибуции атак и четких критериев отграничения от иных киберпреступлений. Особое внимание уделяется сложностям правовой оценки ущерба от кибертерроризма, который часто носит нематериальный и трудноизмеримый характер. В заключение авторы предлагают комплекс мер, направленных на совершенствование международно-правовой базы, включая разработку новой конвенции под эгидой ООН, установление универсальных стандартов атрибуции и создание глобальной системы обмена оперативной информацией.*

Ключевые слова: *кибертерроризм, международное право, квалификация преступлений, юрисдикция, право на самооборону, атрибуция, кибератака, нематериальный ущерб.*

Стремительная цифровизация глобального общества привела к формированию нового пространства для реализации противоправной деятельности. Традиционные угрозы, такие как терроризм, приобрели кибернетическое измерение, превратившись в серьезный вызов международной безопасности. По экспертным оценкам, в 2025 году только на территории России было зафиксировано свыше 105 тысяч кибератак, что почти в полтора раза превышает показатели предыдущего года [1]. Однако эффективное противодействие кибертерроризму сдерживается существенными пробелами в международном праве. Отсутствие консенсуса в определении понятия, трудности с атрибуцией атак и правовой квалификацией последствий создают «серые зоны», которыми успешно пользуются злоумышленники. Данная статья посвящена анализу этих проблем с фокусом на три ключевых аспекта: международно-правовую квалификацию кибертерроризма, вопросы юрисдикции и спорную возможность применения права на самооборону в киберпространстве.

Фундаментальной проблемой является отсутствие универсального юридического определения «кибертерроризма». В доктрине доминирует подход, согласно которому это явление представляет собой синтез цели терроризма и кибернетических средств ее достижения. Так, В.А. Голубев определяет кибертерроризм как преднамеренную атаку на информацию, компьютерные системы или сети, осуществляемую с целью дестабилизации обстановки, запугивания населения или провокации конфликта [2]. А.А. Паненков и Д. Деннинг акцентируют политический или социальный мотив, подчеркивая, что такие действия направлены на оказание давления на органы власти [3]. Таким образом, ключевыми признаками выступают: 1) использование цифровых инфраструктур в качестве средства или цели атаки; 2) наличие террористической цели (политической, идеологической, религиозной); 3) намерение вызвать страх, нанести ущерб или принудить к чему-либо государство или международную организацию.

Несмотря на доктринальные разработки, на международном уровне не закреплено единого определения, что порождает несколько правовых проблем.

1. Сложность отграничения от смежных деяний. Без четких критериев кибертерроризм сливается с кибершпионажем, хактивизмом или обычной киберпреступностью, что осложняет выбор правового режима для реагирования.

2. Проблема атрибуции и доказывания. Анонимность в сети, использование прокси-серверов и территорий третьих стран делают установление истинного источника атаки (атрибуцию) крайне сложной задачей. Отсутствие международного органа и универсальных стандартов доказательств в этой сфере вынуждает государства действовать разрозненно [4].

3. Архаичность нормативной базы. Основные действующие документы, такие как Будапештская конвенция о киберпреступности (2001 г.), были приняты в эпоху, когда современные угрозы не были столь очевидны. Они не содержат прямых положений о кибертерроризме, а попытки их адаптации, как показывает практика, часто оказываются недостаточными.

В условиях цифрового пространства, игнорирующего государственные границы, классические принципы юрисдикции (территориальный, национальный) сталкиваются с серьезными вызовами. Атака, инициированная с территории одного государства, через серверы второго, может нанести ущерб инфраструктуре третьего, что порождает конфликт юрисдикций и затрудняет расследование.

Государства вынуждены развивать национальное законодательство (как, например, Федеральный закон РФ «Об информации, информационных технологиях и о защите информации» или Концепция противодействия терроризму) и искать формы международного сотрудничества. Определенные шаги в этом направлении предпринимаются в рамках ООН. Принятые Генеральной Ассамблеей резолюции, такие как №73/27 и №73/187, закладывают основу для правил ответственного поведения государств в киберпространстве и инициируют открытый диалог по противодействию использованию ИКТ в преступных целях [5]. Однако эти документы носят рекомендательный характер, а создание обязательного к исполнению международно-правового режима по-прежнему остается предметом дискуссий.

Наиболее острую дискуссию вызывает вопрос о том, может ли масштабная кибератака, приравненная к акту кибертерроризма, рассматриваться как «вооруженное нападение», дающее право на индивидуальную или коллективную самооборону по статье 51 Устава ООН. Устав не дает расшифровки этого понятия, и его применение к цифровым атакам является правовой новеллой.

Ряд государств (США, Великобритания) в своих стратегических документах заявляют о возможности применения права на самооборону в ответ на кибератаки, последствия которых сопоставимы с традиционным вооруженным нападением. Однако эта позиция сталкивается с серьезными правовыми препятствиями:

1. Проблема порога («threshold»). Какие конкретно критерии (масштаб финансового ущерба, количество жертв, вывод из строя критической инфраструктуры) позволяют квалифицировать кибератаку как «вооруженное нападение»? Единого ответа нет.

2. Проблема соразмерности ответа. Даже если факт вооруженного нападения признан, какой ответ будет считаться соразмерным – кибернетический контрудар или применение традиционных вооруженных сил?

3. Проблема природы ущерба. Ущерб от кибертерроризма часто носит нематериальный (подрыв доверия, паника, дестабилизация) и трудноизмеримый характер, что осложняет его оценку в контексте требований статьи 51 Устава ООН.

Таблица 1

Ключевые проблемы применения права на самооборону к кибератакам

Проблема	*Суть проблемы*	*Правовое последствие*
Квалификация атаки	Отсутствие международно-признанных критериев, при которых кибератака приравнивается к «вооруженному нападению»	Риск произвольной квалификации и оправдания силовых действий под предлогом самообороны
Атрибуция	Технические и правовые сложности оперативного и неоспоримого доказательства источника атаки	Ответные меры могут быть направлены против невиновного государства, что само по себе является нарушением Устава ООН
Соразмерность ответа	Неясность, какие средства (кибернетические или кинетические) считаются допустимыми для ответа на кибератаку	Эскалация конфликта и выход ответных действий за рамки необходимой обороны

Для преодоления выявленных пробелов необходима консолидированная работа международного сообщества. Авторы статьи предлагают следующие меры.

1. Разработка под эгидой ООН новой международной конвенции по борьбе с кибертерроризмом. Этот документ должен содержать универсальное юридическое определение кибертерроризма, четкие критерии его отграничения от иных киберпреступлений и перечень составов преступлений.
2. Создание международного механизма атрибуции. Целесообразно рассмотреть возможность формирования при ООН или под ее эгидой независимой экспертной группы, которая по запросу государства-жертвы проводила бы расследование и устанавливала источник сложной кибератаки на основе единых стандартов доказательств.
3. Кодификация критериев применения права на самооборону. Необходима выработка и закрепление в международно-правовых документах (например, в виде резолюции Совета Безопасности ООН) конкретных, измеримых критериев, при которых кибератака может считаться вооруженным нападением, а также принципов соразмерного ответа.
4. Усиление оперативного сотрудничества. Развитие на постоянной основе глобальных и региональных платформ для обмена информацией об угрозах, уязвимостях и лучших практиках между национальными CERT (командами реагирования на компьютерные инциденты).

Проведенный анализ позволяет заключить, что современное международное право находится в стадии активного, но еще незавершенного поиска адекватных ответов на вызов кибертерроризма. Основные препятствия носят системный характер: от отсутствия базовых дефиниций до неопределенности с применением фундаментальных норм, таких как право на самооборону. Фрагментарность регулирования и зависимость от национальных подходов создают среду, благоприятную для злоумышленников. Решение проблемы лежит не в адаптации старых инструментов, а в создании новой, целостной международно-правовой конструкции. Ее краеугольными камнями должны стать универсальная конвенция, устраняющая терминологическую неопределенность, и создание механизмов доверия,

таких как международная атрибуция и системы обмена данными. Только на такой основе международное сообщество сможет перейти от реактивного противодействия единичным инцидентам к построению устойчивой системы коллективной безопасности в цифровую эпоху.

Список литературы

1. Данные исследовательского центра RED Security SOC. – URL: https://www.red-soc.ru/analytics (дата обращения: 30.12.2025).

2. Голубев В.А. Кибертерроризм как угроза национальной безопасности: монография / В.А. Голубев, С.С. Петров. – М.: Юрлитинформ, 2019. – 215 с.

3. Паненков А.А. Кибертерроризм как реальная угроза национальной безопасности России / А.А. Паненков // Право и кибербезопасность. – 2018. – № 1. – С. 12–19.

4. Камергоев Б.М. Кибертерроризм в глобальном информационном пространстве / Б.М. Камергоев // Государственная служба и кадры. – 2021. – №1. – С. 158–160. DOI 10.24411/2312-0444-2021-1-158-160. EDN MQPUNJ

5. Тарчоков Б.А. О противодействии угрозам кибертерроризма в глобальном информационном пространстве / Б.А. Тарчоков // Государственная служба и кадры. – 2021. – №1. – С. 148–150. DOI 10.24411/2312-0444-2021-1-148-150. EDN XGCIKL

6. Хамурзов А.Т. Кибертерроризм: новые вызовы и меры противодействия / А.Т. Хамурзов // Журнал прикладных исследований. – 2021. – Т. 2. №3. – С. 74–77. DOI 10.47576/2712-7516_2021_3_2_74. EDN ARTAJU

7. Малик Е.Н. Кибертерроризм как мировая угроза: вызовы и меры борьбы / Е.Н. Малик // Вестник Прикамского социального института. – 2020. – №1. – С. 169–173. EDN QQJHOD