ISSN: 2181-3906 2026

International scientific journal
«MODERN SCIENCE AND RESEARCH»
VOLUME 5 / ISSUE 4 / UIF:8.2 / MODERNSCIENCE.UZ

КИБЕРВОЙНА В СОВРЕМЕННОМ МИРЕ

Шокиров Темурбек Азизжонович
Ташкентский государственный юридический университет
Студент 2 курса факультета «Уголовное правосудие»
temursokirov036@gmail.com
https://doi.org/10.5281/zenodo.19598400

Аннотация. *Статья посвящена исследованию кибервойны как одной из ключевых форм современного межгосударственного противостояния, возникающей в условиях глобальной цифровизации. Анализируются понятие, признаки и особенности кибервойны, а также её отличие от традиционных форм вооружённых конфликтов. Особое внимание уделяется современным методам ведения кибервойн и их воздействию на критическую инфраструктуру государств. Также рассматриваются актуальные проблемы правовой квалификации кибератак и пробелы в международно-правовом регулировании данной сферы. В результате исследования обосновывается необходимость формирования эффективных международных механизмов правового регулирования и сотрудничества государств в целях противодействия киберугрозам.*

Ключевые слова: *кибервойна, киберпространство, кибератака, информационная безопасность, международное право, киберугрозы, цифровая безопасность, государственная безопасность, критическая инфраструктура, правовое регулирование.*

I. Введение

В современных условиях стремительное развитие цифровых технологий привело к тому, что киберпространство фактически признано пятой сферой ведения военных действий наряду с сушей, морем, воздушным и космическим пространством. Если ранее кибератаки рассматривались преимущественно как средство разведки или незначительного вмешательства, то в настоящее время они трансформировались в серьёзную угрозу международной безопасности, способную нарушать функционирование критической инфраструктуры, дестабилизировать государственное управление и причинять значительный экономический ущерб. Ключевая проблема заключается в том, что современная система международного права формировалась в условиях, предшествующих цифровой эпохе. В этой связи возникает вопрос о применимости традиционных правовых норм к действиям в киберпространстве: где проходит граница между обычным компьютерным инцидентом и актом вооружённой агрессии? Несмотря на то что кибероперации не находятся вне правового регулирования, международное сообщество до настоящего времени не выработало единых критериев, позволяющих однозначно квалифицировать кибератаку как применение силы. В научных и экспертных кругах, в частности среди разработчиков «Таллиннского руководства 2.0», преобладает подход, согласно которому оценка кибероперацій должна основываться не на используемых средствах, а на их последствиях и масштабе. Это предполагает возможность приравнивания кибератаки к традиционному вооружённому нападению в случаях, когда она приводит к человеческим жертвам, физическим разрушениям или длительной утрате функционирования жизненно важных систем, что, например,

наблюдалось при применении вредоносного программного обеспечения Stuxnet. Подходы различных государств к решению указанных проблем существенно различаются. Одни из них выступают за адаптацию существующих норм международного права к условиям цифровой среды, в то время как другие акцентируют внимание на концепции цифрового суверенитета и необходимости разработки новых международно-правовых инструментов, учитывающих особенности киберпространства. Цель настоящего исследования заключается в анализе современного состояния международно-правовых подходов к квалификации кибератак. В рамках работы рассматриваются критерии оценки тяжести киберинцидентов, анализируются позиции ключевых субъектов международных отношений, а также оцениваются перспективы формирования универсальной правовой базы, способной обеспечить стабильность и безопасность в условиях цифровой эпохи.

II. Методы

В данном исследовании используется качественный подход, который помогает разобраться, как классические правила международного права применимы к современным технологиям[1]. Исследование строится на нескольких основных инструментах:

Анализ документов «доктринальный метод». Посредством изучения основных правил, такие как Устав ООН, чтобы понять, можно ли считать кибератаку «применением силы». Особое внимание было уделено «Таллиннскому руководству 2.0» самому полному экспертному анализу того, как существующие законы работают в интернете[2].

Сравнение позиций стран. Мы сопоставили официальные стратегии и взгляды России, США и Китая. Это позволило увидеть, в чем страны согласны друг с другом, а в каких вопросах «например, о цифровом суверенитете» их мнения расходятся[3].

Оценка по последствиям «функциональный подход». Мы следовали логике, согласно которой кибератаку нужно оценивать не по тому, как она была проведена, а по её реальному результату. Это означает, что цифровой взлом может быть приравнен к военному нападению, если он ведет к человеческим жертвам или физическим разрушениям[4].

Изучение реальных примеров «кейс-стади». Чтобы проверить теорию на практике, мы проанализировали известные инциденты, такие как атака вируса Stuxnet, которая привела к физической поломке ядерного оборудования[5].

Прогнозирование. Мы использовали метод правового моделирования, чтобы понять, какие новые международные соглашения нужны миру для защиты от киберугроз в будущем[6].

---

[1] См.: Лазарь К. К. Квалификация кибератак как «применения силы» или «акта агрессии» в международном праве... // Правосудие/Justice. 2025. Т. 7, № 3. С. 179–192.
[2] См.: Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations / Gen. Ed. M. N. Schmitt. — Cambridge University Press, 2017.
[3] См.: Лазарь К. К. Квалификация кибератак как «применения силы» или «акта агрессии» в международном праве... // Правосудие/Justice. 2025. Т. 7, № 3. С. 179–192.
[4] См.: Лазарь К. К. Квалификация кибератак как «применения силы» или «акта агрессии» в международном праве... // Правосудие/Justice. 2025. Т. 7, № 3. С. 179–192.
[5] См.: Кибервойна // Википедия: свободная энциклопедия.
[6] См.: Рахман М. М., Дас Т. К. Противодействие кибератакам: пробелы международного права и перспективы их преодоления // Journal of Digital Technologies and Law. 2024. Т. 2, № 4. С. 973–1002.

Материалами для работы стали итоговые доклады экспертов ООН, тексты международных договоров и официальные заявления правительств разных стран.

III. Результаты

В ходе проведенного исследования было установлено, что современные кибератаки могут быть квалифицированы как «применение силы» или «акт агрессии» в тех случаях, когда они вызывают существенный ущерб, сопоставимый с последствиями традиционного вооруженного нападения. Основным критерием для такой оценки признается не технический способ совершения операции, а её масштабы и последствия: причинение физического вреда людям, человеческие жертвы или долговременное разрушение критически важной инфраструктуры. Анализ инцидента с вирусом Stuxnet наглядно подтвердил возможность причинения серьезного материального ущерба государственным объектам исключительно цифровыми средствами.

Исследование позволило выделить три уровня кибероперацій в зависимости от тяжести их последствий: действия ниже порога силы, применение силы и вооруженное нападение. Установлено, что порог, за которым кибер операция переходит в категорию применения силы, должен оцениваться комплексно по интенсивности, длительности и совокупному эффекту воздействия. При этом выявлено, что проблема атрибуции «техническая и юридическая сложность точного установления источника атаки» остается главным барьером для правомерного применения статьи 51 Устава ООН о праве на самооборону[7]. Без неопровержимых доказательств причастности конкретного государства реализация мер самозащиты в киберпространстве крайне затруднена и несет риски эскалации конфликта.

Анализ позиций ключевых международных авторов выявил существенную поляризацию подходов. США и Великобритания выступают за адаптацию действующих норм международного права к цифровой среде. В то же время Россия и Китай делают акцент на концепции кибер суверенитета и необходимости разработки новых специальных правил ответственного поведения государств[8]. Несмотря на то, что Группы правительственных экспертов ООН признали применимость международного права к киберпространству, отсутствие универсального консенсуса по конкретным правовым порогам создает опасные «серые зоны» в законодательстве[9].

Дополнительно в работе зафиксировано, что кибероперации и ответные контрмеры оказывают значительное влияние на права человека, в частности на неприкосновенность частной жизни и свободу выражения мнений. Установлено, что развитие цифровых технологий стало фактором возникновения новых угроз, таких как кибертерроризм и киберпреступность, что требует интеграции гуманитарных стандартов в национальные системы обеспечения кибербезопасности.

[7] Устав Организации Объединенных Наций (подписан в Сан-Франциско 26.06.1945).
[8] Спартак С. А. Цифровой суверенитет: основные концепции и теории в России и мире // Социально-политические науки. - 2025. - Т. 15, № 6. - С. 184–189.
[9] Рахман М. М., Дас Т. К. Противодействие кибератакам: пробелы международного права и перспективы их преодоления // Journal of Digital Technologies and Law. — 2024. — Т. 2, № 4. — С. 973–1002.

Исследование подтверждает острую необходимость разработки универсального международного договора, который смог бы более точно определить границы законного поведения государств в цифровой среде.

IV. Обсуждение

Проведенное исследование подтверждает, что киберпространство окончательно трансформировалось в «пятую сферу» ведения военных действий, где границы между миром и конфликтом становятся все более размытыми[10]. Основная научная дискуссия сегодня сосредоточена на том, как адаптировать классическое международное право «*lex lata*», созданное в доцифровую эпоху, к угрозам, которые не имеют физических границ и часто лишены явного авторства.

Критерии квалификации и «пороги» ущерба Центральным элементом обсуждения остается подход, заложенный в «Таллиннском руководстве 2.0», который предлагает оценивать кибероперации не по используемым инструментам, а по их масштабам и последствиям. Однако на практике определение точного «порога» применения силы остается субъективным. Если случай с вирусом Stuxnet, повлекшим физическое разрушение оборудования, однозначно интерпретируется как применение силы, то квалификация операций, вызывающих системный экономический хаос или паралич государственных сервисов «как в случаях с атаками на критическую инфраструктуру», до сих пор вызывает споры. Эксперты указывают на необходимость учета не только прямого физического вреда, но и функционального ущерба, когда инфраструктура перестает работать без механических разрушений.

Проблема атрибуции и право на самооборону Важнейшим барьером для реализации статьи 51 Устава ООН является техническая и юридическая сложность атрибуции. Анонимность интернета позволяет государствам использовать прокси-группы и негосударственных акторов для проведения атак, сохраняя при этом «правдоподобное отрицание». Это создает опасную ситуацию, когда государство-жертва не может юридически обосновать применение силы в порядке самообороны из-за отсутствия неопровержимых доказательств причастности другого государства. Более того, поспешная или ошибочная атрибуция может привести к неоправданной эскалации конфликта.

Поляризация национальных подходов сравнительный анализ выявил глубокий идеологический раскол между ведущими мировыми державами. США, Великобритания и их союзники настаивают на универсальности существующих норм, полагая, что кибератаки на критическую инфраструктуру уже сейчас могут считаться «*casus belli*». В противовес этому, Россия и Китай активно продвигают концепцию цифрового суверенитета, утверждая, что государства должны обладать полным контролем над своим национальным сегментом интернета. Российская доктрина идет дальше, предполагая, что даже кибероперации, подрывающие политическую стабильность или суверенитет без физических жертв, могут квалифицироваться как акты агрессии.

[10] Кибервойна // Википедия: свободная энциклопедия.

Вызовы международного гуманитарного права «МГП» применение принципов МГП в киберпространстве сталкивается с проблемой объектов двойного назначения «*dual-use*».

Большинство серверов, каналов связи и облачных платформ одновременно используются как военными, так и гражданскими лицами. Это делает практически невозможным соблюдение принципа различения, когда атака на военный узел связи неизбежно выводит из строя больницы, школы и банковские системы, что нарушает требования соразмерности и гуманизма[11].

Институциональный кризис и роль ООН Несмотря на многолетнюю работу групп правительственных экспертов «ГПЭ» и Открытых рабочих групп «ОРГ» ООН, процесс формирования обязательных норм идет медленно из-за требования консенсуса. В настоящее время регулирование остается фрагментарным и опирается на добровольные правила поведения. В доктрине все чаще звучат призывы к разработке универсальной конвенции ООН по кибербезопасности, которая бы закрепила четкие определения «кибернетического вооруженного конфликта» и установила международный механизм атрибуции.

Социально-правовые последствия. Нельзя игнорировать и гуманитарный аспект: усиление мер кибербезопасности и ответные контрмеры часто вступают в конфликт с правами человека, такими как право на неприкосновенность частной жизни и свободу выражения мнений. Милитаризация информационного пространства создает риск тотальной слежки и цензуры под предлогом защиты национальной безопасности[12].

Таким образом, обсуждение показывает, что текущее состояние международного права характеризуется наличием значительных «серых зон». Для предотвращения глобальной кибервойны необходимо достижение политического компромисса, который позволит перейти от декларативных заявлений к созданию юридически обязывающего режима регулирования цифровой сферы[13].

V. Заключение

Проведенное исследование подтверждает, что в условиях глобальной цифровой трансформации киберпространство окончательно закрепилось в статусе «пятой сферы» ведения военных действий наряду с сушей, морем, воздухом и космосом. Современные киберугрозы перестали быть исключительно инструментом шпионажа и превратились в фактор, способный подрывать национальную безопасность, дестабилизировать работу государственных институтов и разрушать критически важную инфраструктуру. Основными итогами работы являются следующие выводы:

Проблема реализации права на самооборону. Главным барьером для правомерного применения статьи 51 Устава ООН остается техническая и юридическая сложность атрибуции.

[11] Рахман М. М., Дас Т. К. Противодействие кибератакам: пробелы международного права и перспективы их преодоления // Journal of Digital Technologies and Law. — 2024. — Т. 2, № 4. — С. 973–1002.
[12] Хамдамова Ф. У. Цифровые технологии как фактор угроз международной безопасности... // in Library. 2024. — Т. 1, № 1. — С. 110–117.
[13] См.: Лазарь К. К. Квалификация кибератак как «применения силы» или «акта агрессии» в международном праве... // Правосудие/Justice. 2025. Т. 7, № 3. С. 179–192.

Анонимность цифровой среды и использование негосударственных прокси-групп позволяют агрессорам сохранять «правдоподобное отрицание», что делает практически невозможным быстрое и доказанное установление источника атаки. Без решения вопроса атрибуции принятие ответных силовых мер несет в себе критические риски неконтролируемой эскалации международного конфликта[14].

Правовой статус кибероперaций. Международное сообщество признает, что киберпространство не является «юридическим вакуумом», и к нему применимо существующее международное право, включая Устав ООН. Квалификация кибератаки как «применения силы» или «вооруженного нападения» основывается на принципе нейтральности средств: определяющими факторами являются масштабы и последствия инцидента [15] . Если цифровая операция приводит к физическим разрушениям, человеческим жертвам или системному экономическому коллапсу, она может рассматриваться как эквивалент традиционного военного удара. Инцидент с вирусом Stuxnet служит историческим прецедентом, доказавшим возможность нанесения серьезного материального ущерба исключительно программными методами.

Геополитическая поляризация. Исследование выявило концептуальный раскол в подходах ведущих мировых держав. США и Великобритания делают ставку на адаптацию действующих норм к новым реалиям. В противовес им, Россия и Китай продвигают доктрину цифрового суверенитета, настаивая на том, что государства должны обладать полным контролем над своим национальным сегментом интернета и защищать его от внешнего вмешательства[16].

Институциональные и гуманитарные вызовы. Текущая деятельность групп правительственных экспертов «ГПЭ» и открытых рабочих групп «ОРГ» ООН по выработке норм ответственного поведения замедляется из-за необходимости достижения консенсуса в условиях высокого недоверия между субъектами международного права.

Параллельно с этим милитаризация ИКТ-среды создает прямые угрозы для прав человека, включая право на неприкосновенность частной жизни и свободу выражения мнений, что требует разработки дополнительных защитных механизмов.

Рекомендации по совершенствованию ситуации: для обеспечения глобальной стабильности необходимо инициировать переговоры по созданию универсальной международной конвенции под эгидой ООН, которая четко определит правовые «пороги» кибератак и введет единые стандарты ответственности государств за вредоносную деятельность, исходящую с их территории. Перспективным решением представляется учреждение международного механизма атрибуции, основанного на независимой технической экспертизе, что позволит минимизировать риск политизированных и ошибочных обвинений.

[14] Антипов, А. Кибервойна: Понимание современной угрозы в цифровую эру // Security Lab. – 2023. – 8 мая.
[15] Определение агрессии: Резолюция 3314 (XXIX) Генеральной Ассамблеи ООН от 14 декабря 1974 г.
[16] Кибератаки на критическую информационную инфраструктуру // TAdviser : [портал]. – 2025. – 28 июля

Только через равноправный диалог и поиск компромисса между концепциями безопасности и цифрового суверенитета международное сообщество сможет предотвратить превращение интернета в театр глобальной кибервойны[17].

Список литературы

1. См.: Лазарь К. К. Квалификация кибератак как «применения силы» или «акта агрессии» в международном праве... // Правосудие/Justice. 2025. Т. 7, № 3. С. 179–192.
2. См.: Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations / Gen. Ed. M. N. Schmitt. — Cambridge University Press, 2017.
3. См.: Кибервойна // Википедия: свободная энциклопедия.
4. См.: Рахман М. М., Дас Т. К. Противодействие кибератакам: пробелы международного права и перспективы их преодоления // Journal of Digital Technologies and Law. 2024. Т. 2, № 4. С. 973–1002.
5. Антипов, А. Кибервойна: Понимание современной угрозы в цифровую эру // Security Lab. – 2023. – 8 мая.
6. Определение агрессии: Резолюция 3314 (XXIX) Генеральной Ассамблеи ООН от 14 декабря 1974 г.
7. Кибератаки на критическую информационную инфраструктуру // TAdviser : [портал]. – 2025. – 28 июля.
8. Хамдамова Ф. У. Цифровые технологии как фактор угроз международной безопасности... // in Library. 2024. — Т. 1, № 1. — С. 110–117.
9. Спартак, С. А. Цифровой суверенитет: основные концепции и теории в России и мире // Социально-политические науки. – 2025. – Т. 15, № 6. – С. 184–189.
10. Кибератаки на критическую информационную инфраструктуру // TAdviser : [портал]. – 2025. – 28 июля.
11. Кебец, В. В. Роль ООН в формировании правового обеспечения международной информационной безопасности / В. В. Кебец, А. А. Орлова // Сборник студенческих работ БГУ. – Минск, 2022. – С. 78–80.
12. Гаркуша-Божко, С. Ю. Определение вооруженного конфликта в киберпространстве // Вестник Санкт-Петербургского университета. Право. – 2023. – Т. 14, вып. 1. – С. 194–210.

[17] Спартак, С. А. Цифровой суверенитет: основные концепции и теории в России и мире // Социально политические науки. – 2025. – Т. 15, № 6. – С. 184–189