YURISPRUDENSIYA

HUQUQIY ILMIY-AMALIY JURNALI

2026-yil 4-son

VOLUME 6 / ISSUE 4 / 2026

DOI: https://dx.doi.org/10.51788/tsul.jurisprudence.6.4.

ISSN: 2181-1938

DOI: https://dx.doi.org/10.51788/tsul.jurisprudence

MUASSIS: TOSHKENT DAVLAT YURIDIK UNIVERSITETI

"Yurisprudensiya" – "Юриспруденция" – "Jurisprudence" huquqiy ilmiy-amaliy jurnali O'zbekiston matbuot va axborot agentligi tomonidan 2020-yil 22-dekabrda 1140-sonli guvohnoma bilan davlat ro'yxatidan o'tkazilgan.

Jurnal O'zbekiston Respublikasi Fanlar akademiyasi huzuridagi Oliy attestatsiya komissiyasi jurnallari ro'yxatiga kiritilgan.

Sotuvda kelishilgan narxda.

Nashr bo'yicha mas'ul:
O. Choriyev

Muharrirlar:
E. Mustafayev, Y. Yarmolik, E. Sharipov, K. Abduvaliyeva, M. Sharifova, Sh. Beknazarova, X. Yuldasheva

Musahhih:
M. Tursunov

Texnik muharrir:
U. Sapayev

Dizayner:
D. Rajapov

Tahririyat manzili:
100047. Toshkent shahri, Sayilgoh ko'chasi, 35.
Tel.: (0371) 233-66-36 (1169)

Vebsayt: jurisprudence.tsul.uz
E-mail: lawjournal@tsul.uz

Obuna indeksi: 1387

Tasdiqnoma
№ 174625, 29.11.2023.

Jurnal 2026-yil 26-avgustda bosmaxonaga topshirildi.
Qog'oz bichimi: A4.
Shartli bosma tabog'i: 24,5
Adadi: 100. Buyurtma: № 81.

TDYU bosmaxonasida chop etildi.
Bosmaxona manzili:
100047. Toshkent shahri, Sayilgoh ko'chasi, 37.

УЧРЕДИТЕЛЬ: ТАШКЕНТСКИЙ ГОСУДАРСТВЕННЫЙ ЮРИДИЧЕСКИЙ УНИВЕРСИТЕТ

Правовой научно-практический журнал «Юриспруденция» – «Yurisprudensiya» – «Jurisprudence» зарегистрирован Агентством печати и информации Узбекистана 22 декабря 2020 года с удостоверением № 1140.

Журнал включён в перечень журналов Высшей аттестационной комиссии при Академии наук Республики Узбекистан.

Реализуется по договорной цене.

Ответственный за выпуск:
О. Чориев

Редакторы:
Э. Мустафаев, Е. Ярмолик,
Э. Шарипов, К. Абдувалиева,
М. Шарифова, Ш. Бекназарова,
Х. Юлдашева

Корректор:
М. Турсунов

Технический редактор:
У. Сапаев

Дизайнер:
Д. Ражапов

Адрес редакции:
100047. Город Ташкент,
улица Сайилгох, 35.
Тел.: (0371) 233-66-36 (1169)

Веб-сайт: jurisprudence.tsul.uz
E-mail: lawjournal@tsul.uz

Подписной индекс: 1387.

Свидетельство
от 29.11.2023 № 174625.

Журнал передан в типографию 26.08.2026.
Формат бумаги: А4.
Усл. п. л. 24,5. Тираж: 100 экз.
Номер заказа: 81.

Отпечатано в типографии Ташкентского государственного юридического университета.
100047, г. Ташкент,
ул. Сайилгох, 37.

FOUNDER: TASHKENT STATE UNIVERSITY OF LAW

"Yurisprudensiya" – "Юриспруденция" – "Jurisprudence" legal scientific and practical journal was registered by the Press and Information Agency of Uzbekistan on December 22, 2020 with certificate No. 1140.

The journal is included in the list of journals of the Higher Attestation Commission at the Academy of Sciences of the Republic of Uzbekistan.

Agreed-upon price.

Publication Officer:
O. Choriev

Editors:
E. Mustafaev, E. Yarmolik, E. Sharipov, K. Abduvalieva, M. Sharifova, Sh. Beknazarova, Kh. Yuldasheva

Proofreader:
M. Tursunov

Technical editor:
U. Sapaev

Designer:
D. Rajapov

Editorial office address:
100047. Tashkent city,
Sayilgoh street, 35.
Phone: (0371) 233-66-36 (1169)

Website: jurisprudence.tsul.uz
E-mail: lawjournal@tsul.uz

Subscription index: 1387.

Certificate
№ 174625, 29.11.2023.

The journal is submitted to the Printing house on 26.08.2026.
Paper size: A4. Cond.p.f: 24,5.
Units: 100. Order: № 81.

Published in the Printing house of Tashkent State University of Law.
100047. Tashkent city,
Sayilgoh street, 37.

MUNDARIJA

12.00.01 – DAVLAT VA HUQUQ NAZARIYASI VA TARIXI. HUQUQIY TA'LIMOTLAR TARIXI

12.00.02 – KONSTITUTSIYAVIY HUQUQ. MA'MURIY HUQUQ. MOLIYA VA BOJXONA HUQUQI

12.00.03 – FUQAROLIK HUQUQI. TADBIRKORLIK HUQUQI. OILA HUQUQI. XALQARO XUSUSIY HUQUQ

СОДЕРЖАНИЕ

CONTENTS

Kelib tushgan / Получено / Received: 01.07.2026
Qabul qilingan / Принято / Accepted: 05.08.2026
Nashr etilgan / Опубликовано / Published: 26.08.2026

DOI: https://dx.doi.org/10.51788/tsul.jurisprudence.6.4./OCPY9140
UDC: 341.3:004.056(045)(575.1)

КИБЕРВОЙНА И КИБЕРОПЕРАЦИИ В МЕЖДУНАРОДНОМ ПРАВЕ: ПРОБЛЕМЫ РАЗГРАНИЧЕНИЯ И ПРАВОВОГО РЕГУЛИРОВАНИЯ

Базарбаева Шахло Рахимовна,
студентка факультета международного права
и сравнительного правоведения
Ташкентского государственного юридического университета
ORCID: https://orcid.org/0009-0006-2271-2262
e-mail: shakhlobazarbaeva070601@gmail.com

Расулов Журабек Абдусамиевич,
доктор философии по юридическим наукам,
и. о. доцента сектора международного права и прав человека
Ташкентского государственного юридического университета
ORCID: https://orcid.org/0000-0002-9235-5006
e-mail: rasulovjurabek1982@gmail.com

Аннотация. *Статья посвящена исследованию правовой природы кибератак, кибероперaций и кибервойны в международном праве. Целью исследования является разграничение указанных понятий и анализ применимости норм международного гуманитарного права к действиям в киберпространстве. Методологическую основу исследования составили теоретико-догматический, сравнительно-правовой, эмпирический и статистический методы, включая анализ практических кейсов (Stuxnet, WannaCry, NotPetya, SolarWinds, кибероперации в рамках российско-украинского конфликта), а также данных международных аналитических центров. В результате исследования установлено, что киберпространство сформировалось как самостоятельная сфера конфликтного взаимодействия, однако существующие международно-правовые нормы регулируют отношения в данной области лишь частично, что обусловливает наличие правовых пробелов и так называемой «серой зоны».*

Ключевые слова: *кибервойна, кибероперации, кибератаки, международное гуманитарное право, киберпространство, атрибуция, Таллиннское руководство 2.0, применение силы*

XALQARO HUQUQDA KIBERURUSH VA KIBEROPERATSIYALAR: FARQLASH HAMDA HUQUQIY TARTIBGA SOLISH MUAMMOLARI

Bazarbaeva Shaxlo Raximovna,
Toshkent davlat yuridik universiteti
Xalqaro huquq va qiyosiy huquqshunoslik
fakulteti talabasi

Rasulov Jurabek Abdusamiyevich,
Toshkent davlat yuridik universiteti
Xalqaro huquq va inson huquqlari sho‘basi dotsenti v.b.,
yuridik fanlar bo‘yicha falsafa doktori

Annotatsiya. *Mazkur maqola xalqaro huquq tizimida kiberhujumlar, kiberoperatsiyalar va kiberurushning huquqiy tabiatini tadqiq etishga bag‘ishlangan. Tadqiqotning maqsadi ushbu tushunchalarni o‘zaro farqlash*

hamda xalqaro gumanitar huquq normalarining kibermakondagi harakatlarga tatbiq etilishi imkoniyatlarini tahlil qilishdan iborat. Metodologik asos sifatida nazariy-dogmatik, empirik, qiyosiy-huquqiy va statistik metodlardan, jumladan, amaliy holat (Stuxnet, WannaCry, NotPetya, SolarWinds, Rossiya–Ukraina mojarosidagi kiberoperatsiya) lar hamda xalqaro tahliliy markazlar ma'lumotlari tahlilidan foydalanilgan. Tadqiqot natijasida kibermakon mojarolarning mustaqil sohasi sifatida shakllangani aniqlangan. Biroq mavjud xalqaro-huquqiy normalar ushbu sohani faqat qisman tartibga soladi. Bu esa huquqiy bo'shliqlar va "kulrang zona"ning mavjudligiga sabab bo'lmoqda.

Kalit so'zlar: *kiberurush, kiberoperatsiya, kiberhujum, xalqaro gumanitar huquq, kibermakon, atributsiya, Tallin qo'llanmasi 2.0, kuch ishlatish*

CYBERWARFARE AND CYBER OPERATIONS IN INTERNATIONAL LAW: PROBLEMS OF DELIMITATION AND LEGAL REGULATION

Bazarbaeva Shakhlo Rakhimovna,
Student at the Faculty of International Law and Comparative Law,
Tashkent State University of Law

Rasulov Jurabek Abdusamievich,
Acting Associate Professor of the Department
of International Law and Human Rights,
Tashkent State University of Law,
Doctor of Philosophy (PhD) in Law

Abstract. *The article examines the legal nature of cyberattacks, cyber operations, and cyberwarfare under international law. The aim of the study is to distinguish between these concepts and to analyze the applicability of international humanitarian law to activities conducted in cyberspace. The methodological framework of the research comprises theoretical-dogmatic, comparative legal, empirical, and statistical methods, including an analysis of practical cases such as Stuxnet, WannaCry, NotPetya, SolarWinds, and cyber operations conducted in the context of the Russia–Ukraine conflict, as well as data from international analytical centres. The study finds that cyberspace has emerged as a distinct domain of conflict; however, existing rules of international law regulate activities in this sphere only partially, resulting in legal gaps and a so-called "grey zone."*

Keywords: *cyberwarfare, cyber operations, cyberattacks, international humanitarian law, cyberspace, attribution, Tallinn Manual 2.0, use of force*

Введение

В современном мире, где обеспечение кибербезопасности становится одной из приоритетных задач многих государств, действия, совершаемые с использованием информационных технологий и цифровых устройств в киберпространстве, создают новые проблемы для применения и толкования норм международного права. В условиях трансформации традиционных форм вооружённых конфликтов киберпространство, включающее информационно-телекоммуникационные сети и компьютерные системы, приобретает всё большее значение как среда осуществления операций и межгосударственного взаимодействия (Singer & Friedman, 2014). Вместе с тем развитие цифровой среды повышает уязвимость государств перед кибератаками и создаёт новые риски для национальной и международной безопасности.

По мнению британского исследователя в области кибербезопасности Т. Рида, «кибервойны никогда не происходили в прошлом, не происходят в настоящем и крайне маловероятны в будущем», а кибератаки, по его мнению, преимущественно представляют собой современные формы шпионажа, саботажа и подрывной деятельности (*subversion*), поскольку не соответствуют предложенным им критериям войны, которая должна быть потенциально летальной, инструментальной и политической (Rid, 2012). Дискуссионность квалификации подобных действий свидетельствует о сохраняющейся неопределённости их международно-правового статуса и нали-

чии так называемой «серой зоны» правового регулирования.

Вместе с тем международное сообщество в целом исходит из применимости международного права, включая международное гуманитарное право (далее – МГП), к деятельности государств в киберпространстве. Вопросы применения существующих норм международного права к кибероперациям получили подробное доктринальное рассмотрение в Таллиннском руководстве 2.0, подготовленном международной группой экспертов под руководством М. Шмитта. Руководство рассматривает применение норм международного права к кибероперациям как в мирное время, так и в условиях вооружённого конфликта, включая вопросы *jus ad bellum* (право, регулирующее применение силы) и *jus in bello* (право, регулирующее ведение вооружённых конфликтов), однако не является юридически обязательным международно-правовым актом (Schmitt, 2017).

В настоящее время технологическое развитие значительно опережает формирование специализированных международно-правовых механизмов регулирования, что обусловливает сложности при квалификации кибероперациий, в частности при определении того, достигают ли они порога «применения силы» или «вооружённого нападения» в понимании Устава ООН, а также при разграничении кибероперациий, кибератак и кибервойны.

Научная новизна настоящего исследования заключается в комплексном анализе применимости норм и принципов международного гуманитарного права к кибероперациям, выявлении существующих пробелов международно-правового регулирования и рассмотрении особенностей соответствующей проблематики в контексте Республики Узбекистан.

Основная часть

В исследовании применены теоретико-догматический, сравнительно-правовой, эмпирический, кейс-ориентированный и статистический методы. Теоретико-догматический метод использован для анализа норм международного права, положений Устава ООН, международного гуманитарного права и Tallinn Manual 2.0. Эмпирический и кейс-ориентированный методы применены при рассмотрении практики кибероперациий, включая Stuxnet, WannaCry, NotPetya и SolarWinds. Сравнительно-правовой метод позволил сопоставить различные подходы к правовой квалификации кибероперациий в международном праве, а также международно-правовые подходы к регулированию киберпространства и законодательство Республики Узбекистан. Статистический метод применён при анализе данных международных аналитических центров (Positive Technologies, «Лаборатория Касперского»), а также официальных статистических данных Республики Узбекистан о динамике киберпреступности.

В рамках исследования разграничены понятия «кибератака», «кибероперация» и «кибервойна». Кибератака представляет собой преднамеренную попытку получить несанкционированный доступ к компьютерным системам, сетям или цифровым устройствам, нарушить их функционирование либо причинить им иной вред, в частности в целях хищения данных, шпионажа, финансового мошенничества или саботажа (Microsoft, n.d.).

В контексте международного гуманитарного права понятие кибератаки имеет более узкое значение. Согласно правилу 92 Tallinn Manual 2.0, кибератакой признаётся кибероперация, наступательная или оборонительная, которая, как обоснованно ожидается, причинит лицам вред здоровью или смерть либо повлечёт повреждение или уничтожение объектов (Schmitt, 2017).

Кибероперация представляет собой более широкую категорию и может охватывать различные действия в киберпространстве, в том числе действия, не достигающие порога «атаки» в смысле международного гуманитарного права. По мнению А. Рязанова, кибероперация представляет собой совокупность согласованных и взаимосвязанных кибератак, направленных на дестабилизацию системы управления противника для достижения оперативных или стратегических целей в киберпространстве. Вместе с тем такое определение отражает лишь один из возможных подходов, поскольку кибероперации не обязательно состоят из кибератак и могут вклю-

чать разведывательные, информационные, подготовительные и иные действия.

Что касается кибервойны, то данный термин широко используется в научной и экспертной литературе для характеристики масштабного противостояния, в рамках которого кибероперации применяются государствами для достижения военных, политических или иных стратегических целей. Такие операции могут быть направлены, в частности, против критической инфраструктуры, включая энергетические системы, системы водоснабжения, финансовую инфраструктуру и системы государственного управления (Madaminova, 2025; Anti-Malware.ru, n.d.).

Киберпространство также рассматривается в качестве самостоятельной операционной среды наряду с традиционными сферами ведения военных операций: сушей, морем, воздухом и космосом. П. Сингер и А. Фридман рассматривают развитие военных возможностей государств в киберпространстве, в том числе деятельность специализированных подразделений, созданных для осуществления соответствующих операций (Singer & Friedman, 2014).

Вместе с тем признание киберпространства самостоятельной операционной средой не означает признания «кибервойны» самостоятельной юридической категорией международного права. Tallinn Manual 2.0 исходит из необходимости применения существующих норм международного права к кибероперациям и рассматривает, в частности, условия, при которых такие операции могут квалифицироваться как применение силы, вооружённое нападение или атака в смысле международного гуманитарного права (Schmitt, 2017). Данный подход следует отличать от позиции Т. Рида, который, опираясь на классическое понимание войны, связанное в том числе с концепцией К. фон Клаузевица, критически относится к использованию понятия «кибервойна» применительно к большинству известных киберинцидентов (Rid, 2012).

Таким образом, кибератаки, кибероперации и кибервойна не являются взаимозаменяемыми понятиями. Кибероперация выступает наиболее широкой категорией, тогда как кибератака в контексте международного гуманитарного права представляет собой определённый вид кибероперации, отвечающий установленным критериям. Понятие «кибервойна», в свою очередь, преимущественно используется в доктринальном и политико-стратегическом дискурсе и не имеет самостоятельного общепризнанного определения в действующем международном праве.

После разграничения основных понятий представляется необходимым определить, каким образом соответствующие явления регулируются международным правом и в какой степени существующая международно-правовая база применима к различным формам кибероперций. Применимость норм международного права к деятельности в киберпространстве признается международным сообществом и соответствующими международными организациями, включая Международный комитет Красного Креста (МККК). Значительный вклад в доктринальное осмысление данного вопроса внесло Таллиннское руководство 2.0 по международному праву, применимому к кибероперациям (*Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*). Оно было подготовлено международной группой экспертов по приглашению Центра передового опыта НАТО по совместной кибероборонe (NATO Cooperative Cyber Defence Centre of Excellence – CCDCOE) в Таллине и содержит 154 правила. Руководство не имеет обязательной юридической силы и отражает позиции международной группы экспертов относительно применения существующего международного права (*lex lata*) к кибероперациям (Schmitt, 2017).

Одним из центральных вопросов является определение правовой квалификации кибероперций и установление условий, при которых они могут достигать порога «применения силы» или «вооружённого нападения» в смысле Устава ООН либо квалифицироваться как «атака» в смысле международного гуманитарного права. Данные понятия относятся к различным правовым режимам и не должны отождествляться. Согласно правилу 92 Таллиннского руководства 2.0, кибератакой в контексте международного гуманитарного права является кибероперация, наступа-

тельная или оборонительная, которая, как обоснованно ожидается, причинит лицам вред здоровью или смерть либо повлечёт повреждение или уничтожение объектов. Вместе с тем вопрос о том, может ли утрата функциональности объекта без его физического повреждения квалифицироваться как ущерб объекту и, следовательно, как атака, остаётся дискуссионным. МККК придерживается подхода, согласно которому при определённых обстоятельствах утрата функциональности объекта в результате кибероперации должна учитываться при определении наличия атаки, что обусловлено необходимостью обеспечения эффективной защиты гражданского населения и гражданских объектов (International Committee of the Red Cross, 2019).

Применение международного гуманитарного права к кибероперациям в условиях вооружённого конфликта предполагает соблюдение его основных принципов, в том числе принципов различения, пропорциональности и предосторожности. Принцип различения, закреплённый, в частности, в статье 48 Дополнительного протокола I 1977 года к Женевским конвенциям 1949 года, требует от сторон вооружённого конфликта всегда проводить различие между гражданским населением и комбатантами, а также между гражданскими и военными объектами и соответственно направлять операции только против военных объектов. Применительно к кибероперациям соблюдение данного принципа может быть затруднено вследствие взаимосвязанности военных и гражданских информационных систем и возможности распространения последствий кибератак на гражданскую инфраструктуру (International Committee of the Red Cross, 2013).

В научной литературе для характеристики подобных рисков проводится аналогия между распространением вредоносного программного обеспечения и воздействием биологических агентов: вредоносное программное обеспечение способно выходить за пределы первоначально выбранной цели и воздействовать на гражданские системы. В связи с этим МККК обращает особое внимание на необходимость соблюдения принципа различения при проведении кибероперций.

Принцип пропорциональности запрещает нападения, которые, как можно ожидать, повлекут случайную гибель гражданских лиц, причинение им вреда, повреждение гражданских объектов или сочетание таких последствий, которые были бы чрезмерными по отношению к ожидаемому конкретному и непосредственному военному преимуществу. Принцип предосторожности требует принятия всех практически возможных мер предосторожности при выборе средств и методов нападения в целях предотвращения или, во всяком случае, сведения к минимуму случайной гибели гражданских лиц, причинения им вреда и повреждения гражданских объектов.

Военная необходимость также относится к фундаментальным принципам международного гуманитарного права, однако не означает, что любая атака должна лишь иметь определённую военную цель. Военная необходимость допускает только те меры, которые необходимы для достижения законной военной цели и не запрещены международным гуманитарным правом. При этом запрещается использовать насилие, основной целью которого является распространение террора среди гражданского населения.

Значительная часть межгосударственных кибероперций осуществляется ниже порогов «применения силы» и «вооружённого нападения», установленных международным правом. В научной и экспертной литературе для характеристики такой деятельности используется понятие «серой зоны». Одной из основных проблем правовой квалификации подобных операций является атрибуция поведения государству. Использование технических средств сокрытия источника кибероперации, ботнетов, скомпрометированных компьютерных систем, прокси-серверов и негосударственных субъектов может существенно затруднять установление фактического субъекта операции.

При этом необходимо разграничивать техническую атрибуцию кибероперации и юридическое присвоение поведения государству в целях установления международно-правовой ответственности. Согласно общим нормам международного права действия государственных органов присваиваются

государству. При определённых условиях государству также может быть присвоено поведение негосударственных субъектов, в частности если они действуют по указаниям либо под руководством или контролем государства. Таким образом, установление технического источника кибероперации само по себе не является достаточным для вывода о международно-правовой ответственности конкретного государства.

В зависимости от целей, характера и объектов воздействия можно выделить следующие основные формы кибероперaций (табл. 1).

Таблица 1

Основные формы кибероперaций*

Форма кибер-операции	Основная цель	Пример
Кибершпио-наж	Получение конфи-денциальной инфор-мации	SolarWinds
Киберсаботаж	Нарушение функци-онирования инфор-мационных и иных систем	Stuxnet
DDoS-атаки	Нарушение доступ-ности информаци-онных ресурсов и сервисов	DDoS-атаки на государствен-ные информаци-онные ресурсы
Киберопера-ции против критической инфраструк-туры	Нарушение функцио-нирования энергети-ческих, финансовых, транспортных и иных критически важных систем	Кибероперации против энерго-системы Укра-ины
Информаци-онно-психо-логические операции	Воздействие на об-щественное мнение и информационную среду	Дезинформаци-онные кампании

* Составлено автором на основе анализа научной литературы (Kazaryan & Belan, 2022).

Особое значение для разграничения различных видов кибероперaций и оценки масштабов современных киберугроз имеет анализ практических кейсов. Одним из наиболее показательных примеров является Stuxnet (2010) – вредоносное программное обеспечение, ставшее одним из первых широко известных примеров кибероперации, повлекшей физическое повреждение оборудования. Его воздействие привело к нарушению работы и выводу из строя значительного числа центрифуг на ядерном объекте в Натанзе (Иран), продемонстрировав возможность причинения физического ущерба посредством программного кода.

WannaCry (2017) продемонстрировал способность кибератак существенно нарушать функционирование критически важных общественных систем даже при отсутствии непосредственного физического разрушения инфраструктуры. В частности, атака оказала значительное воздействие на деятельность Национальной службы здравоохранения Великобритании (NHS), приведя к нарушениям работы медицинских учреждений и отмене значительного числа приёмов пациентов.

NotPetya (2017) стал примером кибератаки, последствия которой приобрели трансграничный характер и повлекли значительный экономический ущерб. Первоначально затронув преимущественно организации на территории Украины, вредоносное программное обеспечение распространилось за её пределы и нарушило деятельность крупных международных компаний. По отдельным оценкам, совокупный экономический ущерб от NotPetya превысил 10 млрд долларов США.

SolarWinds (2020) является одним из наиболее масштабных примеров компрометации цепочки поставок программного обеспечения в целях кибершпионажа. Вредоносный код был внедрён в обновления программного обеспечения SolarWinds Orion, что позволило получить скрытый доступ к информационным системам ряда государственных органов США и частных компаний.

Особое значение для исследования имеют кибероперации, проводившиеся в рамках российско-украинского вооруженного конфликта. Они продемонстрировали возможность сочетания кибероперaций с традиционными средствами и методами ведения военных действий. Кибероперации были направлены, в частности, против государственных информационных ресурсов, коммуникационных систем и объектов критической инфраструктуры. Это подтверждает возрастающую роль киберпространства как операционной среды в современных вооружённых конфликтах.

Таким образом, анализ известных практических кейсов показывает значительное

разнообразие кибероперацій по их целям, способам осуществления и последствиям. Их воздействие может варьироваться от получения несанкционированного доступа к информации и нарушения функционирования информационных систем до причинения значительного экономического ущерба и физического повреждения объектов. При этом правовая квалификация конкретной кибероперации должна осуществляться с учётом её характера и последствий, поскольку не всякая кибератака достигает порога применения силы, вооружённого нападения или атаки в смысле международного гуманитарного права.

Полученные выводы подтверждаются также статистическими данными, свидетельствующими о росте масштабов противоправной активности в киберпространстве. Вместе с тем при использовании таких данных необходимо разграничивать киберпреступность и межгосударственные кибероперации, поскольку соответствующие показатели характеризуют различные по своей правовой природе явления.

Так, согласно Всемирному индексу киберпреступности (*World Cybercrime Index*), разработанному М. Брюс и соавторами, первые позиции среди государств, связанных с наибольшей концентрацией киберпреступной активности, занимают Россия, Украина, Китай, США, Нигерия и Румыния (Bruce et al., 2024). При этом данный индекс характеризует именно географию и распространённость киберпреступности и не предназначен для определения масштабов межгосударственных кибероперацій или кибервойны. Поэтому соответствующие данные могут использоваться лишь в качестве дополнительного показателя общего масштаба противоправной активности в киберпространстве, но не в качестве доказательства интенсивности межгосударственного киберпротивостояния.

Анализ различных подходов к формированию государственной политики в киберпространстве показывает отсутствие единой универсальной модели его правового регулирования. В частности, существенные различия прослеживаются в подходах Европейского союза, США и Китайской Народной Республики.

Подход Европейского союза характеризуется значительным вниманием к нормативному регулированию цифровой среды, обеспечению кибербезопасности и защите основных прав человека. Одним из ключевых элементов правового регулирования цифровой сферы является Общий регламент по защите данных (General Data Protection Regulation – GDPR), устанавливающий требования к обработке персональных данных и механизмы защиты прав субъектов данных (European Union, 2016). Вместе с тем политика Европейского союза в киберпространстве не ограничивается защитой персональных данных и включает меры по обеспечению кибербезопасности, устойчивости информационных систем и противодействию киберугрозам.

Подход США характеризуется сочетанием нормативно-правового регулирования, обеспечения кибербезопасности и развития возможностей проведения военных операций в киберпространстве. Создание и развитие Киберкомандования США (U.S. Cyber Command) отражает признание киберпространства в качестве важной операционной среды для обеспечения национальной безопасности и достижения стратегических целей. Таким образом, государство выступает не только в качестве регулятора цифровой среды, но и как субъект, развивающий оборонительные и наступательные возможности в киберпространстве.

Подход Китайской Народной Республики характеризуется особым вниманием к государственному суверенитету и контролю в информационном пространстве. Закон КНР о кибербезопасности закрепляет ряд требований в области обеспечения безопасности сетей, защиты критической информационной инфраструктуры и регулирования деятельности операторов сетей (People's Republic of China, 2017). Существенную роль в китайской модели играет государственное регулирование трансграничных информационных потоков и доступа к цифровым ресурсам. В научной и экспертной литературе комплекс соответствующих технических и организационно-правовых механизмов часто обозначается как «Великий китайский файервол» (Great Firewall of China).

Таким образом, рассмотренные модели демонстрируют различные приоритеты государственной политики в киберпространстве: в Европейском союзе значительное внимание

уделяется нормативному регулированию цифровой среды и защите основных прав; в США – сочетанию регулирования с развитием возможностей обеспечения национальной безопасности и проведения операций в киберпространстве; в КНР – вопросам государственного суверенитета, безопасности и контроля информационного пространства. Вместе с тем указанные различия не являются абсолютными, поскольку каждая из рассмотренных моделей включает правовые, технологические, оборонные и институциональные механизмы обеспечения кибербезопасности.

Таблица 2

Сравнительная характеристика отдельных подходов к регулированию киберпространства

Государство / объединение	Характеристика подхода	Основные приоритеты
Европейский союз	Нормативно-правовой и институциональный	Защита основных прав и персональных данных, обеспечение кибербезопасности и устойчивости цифровой инфраструктуры
США	Комплексный нормативно-правовой и военно-стратегический	Национальная безопасность, защита критической инфраструктуры, киберустойчивость, развитие оборонительных и наступательных возможностей
Китайская Народная Республика	Государственно-центричный, основанный на концепции кибersуверенитета	Государственный суверенитет и безопасность в киберпространстве, контроль информационного пространства, защита критической информационной инфраструктуры
Республика Узбекистан	Институционально-правовой	Развитие национальной системы кибербезопасности, защита информационных систем и критической информационной инфраструктуры

В отличие от международного права, в котором отсутствует общепризнанное юридически обязательное определение кибервойны, законодательство Республики Узбекистан формирует институциональные и правовые основы обеспечения кибербезопасности. Закон Республики Узбекистан от 15 апреля 2022 года № ЗРУ-764 «О кибербезопасности» составляет основу правового регулирования в данной сфере и определяет Службу государственной безопасности Республики Узбекистан в качестве уполномоченного государственного органа в области кибербезопасности. Законом также закреплены такие понятия, как «кибератака», «инцидент кибербезопасности» и «критическая информационная инфраструктура» (Republic of Uzbekistan, 2022).

Законодательством Республики Узбекистан предусмотрена юридическая ответственность за правонарушения, совершаемые с использованием информационных технологий. Соответствующие составы преступлений закреплены, в частности, в главе XX[1] Уголовного кодекса Республики Узбекистан. Рост количества преступлений, совершаемых с использованием информационных технологий, свидетельствует о необходимости дальнейшего развития комплексной системы обеспечения кибербезопасности.

Сравнительный анализ показывает, что рассмотренные модели существенно различаются по своим приоритетам. Подход Европейского союза характеризуется значительным вниманием к нормативному регулированию цифровой среды, обеспечению кибербезопасности и защите основных прав; подход США сочетает правовые и институциональные механизмы обеспечения кибербезопасности с развитием оборонительных и наступательных возможностей в киберпространстве; модель Китайской Народной Республики характеризуется особым вниманием к государственному суверенитету, безопасности и контролю информационного пространства. Указанные различия обусловлены особенностями правовых систем, национальными интересами и различными подходами к определению роли государства в обеспечении кибербезопасности.

Проведённое исследование свидетельствует о наличии ряда нерешённых вопросов международно-правового регулирования кибероперации, включая отсутствие универсального определения кибервойны, сложности атрибуции кибероперации государствам и определения условий, при которых кибероперация

достигает порога применения силы или вооружённого нападения. Вместе с тем отсутствие специальных международно-правовых норм не означает неприменимости существующего международного права к киберпространству. Нормы Устава ООН и, при наличии вооружённого конфликта, нормы международного гуманитарного права применимы к кибероперациям при соблюдении условий, предусмотренных соответствующими правовыми режимами.

Таллиннское руководство 2.0, не являясь юридически обязательным международно-правовым актом, представляет собой значимый доктринальный источник для анализа применимости существующих норм международного права к кибероперациям. Дальнейшее развитие международно-правового регулирования в данной сфере требует продолжения межгосударственного диалога по вопросам квалификации кибероперций, атрибуции поведения государствам, международной ответственности, применения норм о применении силы и самообороне, а также международного гуманитарного права.

Анализ законодательства Республики Узбекистан показывает, что национальная система кибербезопасности находится в процессе последовательного развития. Национальное законодательство закрепляет основные понятия в области кибербезопасности, определяет полномочия государственных органов и предусматривает механизмы юридической ответственности. Дальнейшее совершенствование законодательства может быть связано с развитием механизмов международного сотрудничества, обмена информацией о киберинцидентах, повышением устойчивости информационных систем и совершенствованием защиты объектов критической информационной инфраструктуры.

Таким образом, результаты проведённого исследования свидетельствуют о необходимости дальнейшего совершенствования законодательства Республики Узбекистан в сфере кибербезопасности с учётом применимых норм международного права и современных подходов к обеспечению кибербезопасности, а также развития международного сотрудничества в данной области.

Заключение

Проведённое исследование показывает, что кибероперации приобретают всё большее значение как инструмент геополитического воздействия и способны оказывать существенное влияние как на цифровую, так и на физическую инфраструктуру государств. Несмотря на отсутствие универсального международно-правового определения кибервойны, существующие нормы международного права, включая нормы МГП, применимы к кибероперациям, осуществляемым в связи с вооружённым конфликтом. Вместе с тем технические особенности кибероперацій и сложности их атрибуции затрудняют международно-правовую квалификацию соответствующих действий и способствуют сохранению правовой неопределенности. Опыт Республики Узбекистан свидетельствует о последовательном формировании институциональных и правовых основ обеспечения кибербезопасности на национальном уровне.

Однако различия в подходах государств и сохраняющиеся вопросы международно-правовой квалификации кибероперацій затрудняют формирование единообразных подходов к их регулированию. В этих условиях важными направлениями дальнейшего развития являются уточнение механизмов применения существующих норм международного права к деятельности в киберпространстве, совершенствование национального законодательства и развитие международного сотрудничества в сфере кибербезопасности.

REFERENCES

Aliev, N. (2022, November 28). *Cyber operations during the Russian invasion of Ukraine in 2022*. Riddle Russia. https://ridl.io/ru/kiberoperatsii-v-hode-rossijskogo-vtorzheniya-v-ukrainu-v-2022-godu/

Anti-Malware.ru. (n.d.). *Cyberwarfare*. https://www.anti-malware.ru/threats/cyberwarfare

Berova, D. M. (2018). Cyberattacks as a threat to information security. *Gaps in Russian Legislation, (2)*, 186–188. https://cyberleninka.ru/article/n/kiberataki-kak-ugroza-informatsionnoy-bezopasnosti

Bruce, M., Lusthaus, J., Kashyap, R., Phair, N., & Varese, F. (2024). Mapping the global geography of cybercrime with the World Cybercrime Index. *PLOS ONE, 19*(4), e0297312. https://doi.org/10.1371/journal.pone.0297312

European Parliament & Council of the European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union, L 119*, 1–88. https://eur-lex.europa.eu/eli/reg/2016/679/oj

Kazaryan, K. K., & Belan, V. V. (2022). Cyber war. *StudNet, 5*(1), 575–584. https://cyberleninka.ru/article/n/kibervoyna

Larina, E. S., & Ovchinsky, V. S. (2014). *Cyber wars of the XXI century: What Edward Snowden did not tell about*. Knizhny Mir.

Madaminova, M. (2025). Cyber wars. *Science and Technology in the Modern World, 4*(19), 91–98.

Microsoft. (n.d.). *What is a cyberattack?* Microsoft Security. https://www.microsoft.com/ru-ru/security/business/security-101/what-is-a-cyberattack

People's Republic of China. (2016). *Cybersecurity Law of the People's Republic of China*. National People's Congress of the People's Republic of China.

Rid, T. (2012). Cyber war will not take place. *Journal of Strategic Studies, 35*(1), 5–32. https://doi.org/10.1080/01402390.2011.608939

Ryazanov, A. A. (2021). Cyber operations as an instrument of interstate military-economic competition. *Bulletin of S. Y. Witte Moscow University. Series 1: Economics and Management, (2)*, 15–21. https://doi.org/10.21777/2587-554X-2021-2-15-21

Sebekin, S. A., & Kostrov, A. V. (2019). Chinese military philosophy and cyber warfare: Traditional conceptual foundations for non-traditional operations. *International Relations, (3)*, 66–81. https://doi.org/10.7256/2454-0641.2019.3.30872

Segal, A. (2016). *The hacked world order: How nations fight, trade, maneuver, and manipulate in the digital age*. PublicAffairs.

Singer, P. W., & Friedman, A. (2014). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford University Press.

Urmanova, M. (2025). Cyber warfare in international humanitarian law: Application of IHL guiding principles. *Society and Innovations, (SI3)*, 426–439.

United Nations. (1977, June 8). *Protocol additional to the Geneva Conventions of 12 August 1949, and relating to the protection of victims of international armed conflicts (Protocol I).* https://www.ohchr.org/en/instruments-mechanisms/instruments/protocol-additional-geneva-conventions-12-august-1949-and

Schmitt, M. N. (Ed.). (2017). *Tallinn manual 2.0 on the international law applicable to cyber operations*. Cambridge University Press.

International Committee of the Red Cross. (2013, June 28). *What limits does the law of war impose on cyber attacks?* https://www.icrc.org/en/doc/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm

International Committee of the Red Cross. (2019, November). *International humanitarian law and cyber operations during armed conflicts: Position paper*. ICRC position paper

Republic of Uzbekistan. (2022, April 15). *On cybersecurity (Law No. LRU-764)*. Lex.uz. https://lex.uz/ru/docs/5960609

Vyatkina, A., & Osipova, A. (2025, August 28). *Current cyber threats: Q1–Q2 2025*. Positive Technologies. https://ptsecurity.com/research/analytics/aktual-nye-kiberugrozy-i-ii-kvartaly-2025-goda/

YURISPRUDENSIYA

HUQUQIY ILMIY-AMALIY JURNALI

2026-YIL 4-SON

VOLUME 6 / ISSUE 4 / 2026

DOI: https://dx.doi.org10.51788/tsul.jurisprudence.6.4.

DOI: https://dx.doi.org/10.51788/tsul.jurisprudence