Оглавление

[Введение 3](#_Toc168006952)

[Глава 1. Теоретические аспекты международного сотрудничества в области противодействия киберпреступности 7](#_Toc168006953)

[1.1. Международные документы и конвенции по борьбе с киберпреступностью (указать будапештскую и предложение по созданию новой конвенции) 7](#_Toc168006954)

[1.2. Вклад международных организаций в области противодействия киберпреступности 16](#_Toc168006955)

[1.3. Инциденты утечки данных и их влияние на международное сотрудничество 24](#_Toc168006956)

[Глава 2. Подходы России и США к противодействию киберпреступности 39](#_Toc168006957)

[2.2. Обзор развития подходов и инициатив США в сфере борьбы с киберпреступностью 48](#_Toc168006958)

[2.3. Механизмы взаимодействия России и США в контексте кибербезопасности 56](#_Toc168006959)

[Заключение 63](#_Toc168006960)

[Список источников и литературы 65](#_Toc168006961)

# **Введение**

**Актуальность.** Современный ландшафт информационных технологий теперь определяется гонкой вооружений между странами по всему миру, ситуацией, которая представляет собой вполне реальную угрозу непреднамеренной эскалации киберинцидентов. В худшем случае это может привести к вооруженному конфликту между крупными мировыми державами. Оглядываясь назад на анналы истории, становится очевидным, что всякий раз, когда технологические инновации или геополитическая динамика создавали напряженность, государства стремились создать чувство безопасности, договариваясь о мерах укрепления доверия или создавая системы контроля над вооружениями. Эти меры служат для защиты от непреднамеренного конфликта и предотвращения эскалации напряженности.

Однако в настоящее время в мире все еще отсутствуют единые, обязательные международные стандарты ведения войны и мер укрепления доверия, специально адаптированные к ответственному поведению государств в цифровой среде. Это вопиющая проблема, особенно если учесть, что не существует даже системы контроля за распространением и применением кибероружия.

По мере продвижения вперед в XXI веке информационная безопасность быстро становится решающим фактором не только в двусторонних отношениях, например, между Россией и США, но и в поддержании стратегической стабильности в глобальном масштабе. Воздействие информации является движущей силой в динамике современных войн и конфликтов, а возможность контроля и манипулирования информацией сегодня признана одним из наиболее важных компонентов совокупной власти государства.

В этих нестабильных условиях глобальная безопасность и стратегическая стабильность находятся под сильным влиянием характера отношений между российскими и американскими властями, представляющими две сверхдержавы, по вопросам международной информационной безопасности (МИБ). Это вызывает особую озабоченность, поскольку случайная или преднамеренная кибератака может спровоцировать эскалацию международной напряженности, что может привести к полномасштабному военному конфликту.

Поэтому обеспечение международной безопасности становится одним из ключевых факторов, напрямую влияющих на стратегическую стабильность в целом. Более того, в нынешнюю цифровую эпоху ни одна страна не может в одиночку защитить свою территорию от широкого спектра существующих киберугроз. Это подчеркивает важность коллективных действий и сотрудничества в сфере кибербезопасности.

**Объектом** исследования являются международные нормы противодействия киберпреступности.

**Предметом** исследования являются меры США и России по противодействию киберпреступности.

**Цель** исследования – сравнить подходы России и США в контексте противодействия киберпреступности на основе нормативных актов и международного сотрудничества.

Для достижения поставленной цели необходимо решение следующих задач:

* Определить теоретические аспекты основных международных норм и актуальной документации.
* Проанализировать работу международных акторов в аспекте противодействия киберпреступности.
* Исследовать действующие подходы и инициативы России и США.
* Проанализировать совместную работу России и США в определенных киберпроисшествиях.

**Обзор источников.** Исследование представленной темы происходило с опорой на правительственные документы Российской Федерации (РФ), которые образуют первую группу источников. В частности, в работе была использована концепция внешней политики РФ от 2023 года. Также использовалась Доктрина информационной безопасности РФ 2016 года и Концепция технологического развития до 2030 года. В данных документах обосновывается необходимость технологического развития и соблюдения норм кибербезопасности внутри государства.

Ко второй группе относятся такие международные документы по кибербезопасности как Будапештская Конвенция по кибербезопасности, Соглашение о сотрудничестве в борьбе с преступлениями в сфере компьютерной информации, в который предоставляются нормы международного сотрудничества и использования информационных сетей, а также Проект Конвенции ООН о сотрудничестве в сфере противодействия информационной преступности, предложенной РФ.

К третьей группе источников относятся научные труды таких исследователей в данной области как:

Бойко С.М., кандидат исторических наук. В своей работе «Группа правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности: взгляд из прошлого в будущее»[[1]](#footnote-1) рассматривает создание и историю Группы правительственных экспертов ООН и подчеркивает проблемы, с которыми пришлось столкнуться при достижении консенсуса.

Также еще одной немаловажной работой Бойко С.М. является «Формирование системы международной информационной безопасности: российские подходы и инициативы»[[2]](#footnote-2), в которой он рассматривает государственную политику России в области международной информационной безопасности, определяет основные направления международного сотрудничества и дает оценку профильному двустороннему сотрудничеству

Роговский Е.А., Ведущий эксперт, Центр международной информационной безопасности и научно-технологической политики. В своей работе «Кибер-Вашингтон: глобальные амбиции»[[3]](#footnote-3) автор рассматривает глобальную борьбу США за обеспечение собственных интересов своей информационной безопасности на мировой арене, определяет наиболее уязвимые места в вопросе влияния технологий на развитие информационного общества.

Мартин С. Либики, ученый и профессор Высшей школы RAND имени Фредерика С. Парди. В свой работе «Cyberwar as a Confidence Game»[[4]](#footnote-4) автор сравнивает стратегические риски и возможности информационного оружия как ядерного, рассматривает разработки США в сохранении лидерства в вопросе кибервооружения.

**Теоретико-методологические основы исследования.** В рамках данной работы был использован сравнительно-правовой метод метод для передачи основныхмеждународныхнорм противодействия киберпреступности. Также использовалась совокупность таких методов как анализ и синтез, метод кейсов, классификация и сравнения для более глубокого исследования мер противодействия киберпреступности США и России.

# **Глава 1. Теоретические аспекты международного сотрудничества в области противодействия киберпреступности**

## **1.1. Международные документы и конвенции по борьбе с киберпреступностью**

Быстрые изменения в информационных и коммуникационных технологиях создали виртуальный домен, к которому можно подключать технологические устройства и передавать данные из любой точки мира. С развитием этого глобального киберпространства его масштабы постепенно расширялись. Все компоненты физического мира приняли участие в этом новом мире 21 века, также известном как «Век цифровых технологий». Став центром политической, экономической, социальной и военной деятельности, киберпространство рассматривается как определяющая сила настоящего и будущего международных отношений. Адаптация международных отношений к цифровой эпохе возможна посредством комплексной технологической трансформации от содержания к действующим лицам. Поэтому базовые концепции силы, безопасности, стратегии, терроризма и дипломатии в рамках международных отношений должны быть обновлены в киберпространстве. Построение порядка в новых – кибер-международных отношениях, несомненно, будет более сложным и трудным, чем в мире физических международных отношений. В этой области, где проблемы безопасности и восприятие угроз являются более неопределенными, атаки, с которыми могут столкнуться субъекты, могут иметь разрушительные последствия. Большое количество брешей в безопасности и типов атак делают эту территорию особенно привлекательной для террористических организаций. Неопределенность в отношении суверенитета государств в киберпространстве и возможности установления международных правил и норм, обязательных для всех участников, усложняет киберструктуру. Таким образом, кибердипломатия является высокоэффективной и решающей не только с точки зрения конфликтов между государствами, но и с точки зрения предлагаемых ею решений и инструментов, которые будут использоваться для решения проблем среди всех участников киберпространства.

Киберпреступность стала одной из наиболее актуальных проблем современного мира. С развитием информационных технологий и увеличением числа пользователей интернета, количество преступлений, совершаемых в виртуальном пространстве, растет с каждым годом. В связи с этим, международное сообщество активно разрабатывает различные документы и конвенции Исходя из дилеммы безопасности, анархическая структура, возникающая из-за отсутствия суверенитета в международных отношениях, также применима и к сфере киберпространства. Учитывая сложную природу киберпространства, отсутствие международных законодательных и правоприменительных органов затрудняет достижение субъектами своих целей. Конфликт между акторами, осознающими, что анархическая структура физических международных отношений более интенсивна в киберпространстве, определяется традиционной дилеммой безопасности. Нет ничего, что могло бы удержать государства от нарушения цифровых границ других государств и субъектов киберпространства. Поэтому все игроки в киберпространстве обратились к разработке как наступательных, так и защитных средств. Кибердействия стали нормальной частью построения угроз в международных отношениях. Кибероперации или другие формы кибердеятельности, которые правительства направляют друг другу, теперь считаются частью нормальных конфликтных отношений. Более того, страх перед издержками, создаваемыми киберпространством в физическом мире, преодолел теоретические барьеры. Однако радикальных изменений в традиционном понимании войны не произошло. Как отметил Лукас Келло[[5]](#footnote-5), киберреволюция не привела к кардинальным изменениям в природе войн между государствами. Это привело к возникновению важных проблем в области исследований безопасности, таких как невоенные иностранные угрозы или экономический и социальный ущерб, наносимый нетрадиционными игроками. Мощь кибероружия, сложности киберзащиты и проблемы стратегической нестабильности также интерпретируются как три основных фактора киберопасности в дискурсе международной безопасности., направленные на борьбу с киберпреступностью.

Доминирующей силой, формирующей мир в XXI веке, несомненно, является Интернет. Включение Интернета в физический мир ускорило переход в сферу киберпространства и облегчило получение данных от различных субъектов в этой области. На государствах и институтах лежит большая ответственность в этом вопросе. Потому что это их обязанность защищать как отдельных людей, так и социальную структуру от всякого рода вреда. Хотя сеть Интернет имеет гибкую и модульную структуру, она полна пробелов в безопасности. По этой причине баланс сил в киберпространстве складывается в пользу злоумышленников. Самые сложные препятствия или наступательно-защитные стратегии в этой области, хотя и не впечатляют в физической среде, кажутся вполне логичными и новаторскими в виртуальной среде. Национальные границы участников киберпространства физически и виртуально пересекаются. Таким образом, внутренняя среда безопасности пересекается с дилеммой международной безопасности, и существует необходимость развития агрессивно-оборонительного киберпотенциала. Усилия действующих лиц по увеличению своих кибер-возможностей, с одной стороны, и защите своей кибер-слабости, с другой, создают цикл нестабильности в сфере киберпространства. Конечно, влияние Интернета на формирование этого цикла велико. Сеть Интернет также стерла многие классические различия в международных отношениях и исследованиях безопасности. Например, о резких различиях между индивидуальными и коллективными взглядами на безопасность в киберпространстве уже нельзя упоминать. В дополнение к этому, в сфере киберпространства подходы к гражданской, военной и политической безопасности стали пересекаться. С другой стороны, дилемма кибербезопасности гораздо больше, чем любая другая дилемма межгосударственной безопасности. Дискурсы по кибербезопасности связаны с различными формами угроз, включая базовые компьютерные вирусы, киберпреступность и кибершпионаж. Сложная структура киберпространства, создаваемая множеством акторов, приводит к прямому влиянию мер безопасности, предпринимаемых государствами в этой области, на жизнь людей.

С другой стороны, большое количество участников и разнообразие в киберпространстве затрудняют сдерживание. В общем, цель сдерживания – изменить восприятие и планы нападающего. Сдерживание навязывает убеждение, что действия, направленные против угроз, не будут успешными или что стоимость действий превысит рассчитанную сумму выгод. В отсутствие применимых соглашений меры сотрудничества могут обеспечить международный мир и стабильность. Для поддержания порядка в международной системе необходимы приемлемые нормы и принципы ответственного поведения. То же самое относится и к киберпространству, и установление порядка в киберпространстве зависит от способности субъектов домена устанавливать приемлемые нормы и правила. Будапештская конвенция о киберпреступности стала важным документом, подтверждающим насущную необходимость международного сотрудничества для эффективной борьбы с киберугрозами. Она обеспечивает всеобъемлющую основу для борьбы с киберпреступностью на мировом уровне.

Основные цели Будапештской конвенции о киберпреступности заключаются в повышении эффективности международного сотрудничества в борьбе с киберпреступностью, содействии гармонизации национального законодательства и содействии разработке надежных мер кибербезопасности. Устанавливая общую правовую базу и способствуя трансграничному сотрудничеству, конвенция направлена на смягчение вызовов, создаваемых киберугрозами, при одновременном соблюдении основных прав человека и верховенства закона.

Существует несколько причин, по которым Будапештская конвенция о киберпреступности имеет важное значение. Прежде всего, поскольку киберпространство является глобальной средой, традиционные границы юрисдикции больше не имеют значения, и страны должны сотрудничать в расследовании и судебном преследовании киберпреступлений, которые пересекают национальные границы. Крайне необходимы скоординированные международные ответные меры, о чем свидетельствует рост числа киберугроз, таких как кибератаки, онлайн-мошенничество, кража личных данных и эксплуатация детей. Кроме того, отсутствие единообразных правовых рамок и процессуальных процедур затрудняет успешную борьбу с киберпреступностью, что подчеркивает важность согласования правовых рамок между странами.

Будапештская конвенция о киберпреступности предоставляет государствам-членам многочисленные возможности для укрепления их потенциала в области кибербезопасности и более эффективной борьбы с киберугрозами. Содействие обмену информацией и сотрудничеству между правоохранительными органами является одним из основных потенциальных возможностей, поскольку позволяет быстрее проводить расследования киберпреступлений и привлекать виновных к ответственности. Кроме того, конференция предоставляет площадку для проведения мероприятий, направленных на расширение потенциала, технической поддержки и образовательных возможностей, с тем чтобы страны-участницы могли создавать надежные структуры кибербезопасности и правовые системы. Соблюдение конвенции также укрепляет международный авторитет и уверенность в себе, что поощряет сотрудничество и партнерские отношения между государствами в борьбе с общими киберугрозами.

1. Бойко С. Группа правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности: взгляд из прошлого в будущее // Международная жизнь. 2016. N. 8. С. 53-71. [↑](#footnote-ref-1)
2. Бойко С. Формирование системы международной информационной безопасности: российские подходы и инициативы // Международная жизнь. 2018. N. 5. С. 100-110. [↑](#footnote-ref-2)
3. Роговский Е. Кибер-Вашингтон: глобальные амбиции. М.: Международные отношения. 2014. 846 с. [↑](#footnote-ref-3)
4. Libicki М. Cyberwar as a Confidence Game. / M. Libicki // Strategic Studies Quaterly. Vol. 5, N. 1. Spring 2011. [↑](#footnote-ref-4)
5. Lucas Kello The Meaning of the Cyber Revolution: Perils to Theory and Statecraft // International Security. - 2013. - №Vol. 38, No. 2. - С. 7-40. [↑](#footnote-ref-5)