На правах рукописи

Аббуд Руслан Ратебович

МЕЖДУНАРОДНО-ПРАВОВОЕ РЕГУЛИРОВАНИЕ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПЛЕНИЯМ

Специальность: 5.1.5. – Международно-правовые науки

АВТОРЕФЕРАТ

диссертации на соискание ученой степени

кандидата юридических наук

Москва – 2025

Работа выполнена на кафедре международного права Федерального государственного бюджетного образовательного учреждения высшего образования «Российский государственный университет правосудия им. В.М. Лебедева».

Научный руководитель: **Нешатаева Татьяна Николаевна**
доктор юридических наук, профессор, заведующий кафедрой международного права ФГБОУ ВО «Российский государственный университет правосудия им. В.М. Лебедева»

Официальные оппоненты: **Мезяев Александр Борисович**
доктор юридических наук, доцент, заведующий кафедрой конституционного и международного права УВО «Университет управления «ТИСБИ»

Скуратова Александра Юрьевна
кандидат юридических наук, доцент, доцент кафедры международного права ФГАОУ ВО «Московский государственный институт Международных отношений (университет) Министерства иностранных дел Российской Федерации»

Ведущая организация: **Федеральное государственное бюджетное Образовательное учреждение высшего образования «Саратовская государственная юридическая академия»**

Защита диссертации **состоится «24» октября 2025 года в 14 час. 00 мин.** на заседании Диссертационного совета ПДС 05.2.001.03 при ФГБОУ ВО «Дипломатическая академия МИД России» по адресу: 119021, г. Москва, ул. Остоженка, д. 53/2, стр. 1, актовый зал.

С диссертацией и авторефератом можно ознакомиться в библиотеке ФГБОУ ВО «Дипломатическая академия МИД России» по адресу: 119021, г. Москва, ул. Остоженка, д. 53/2, стр. 1 и на официальном сайте http://www.dipacademy.ru.

Автореферат разослан «___» _____ 2025 года.

Ученый секретарь
Диссертационного совета ПДС 05.2.001.03,
Кандидат юридических наук, доцент С.В. Комендантов

Общая характеристика работы

Актуальность темы диссертационного исследования. Актуальность темы исследования обуславливается рядом значимых факторов. Во-первых, киберпреступление является современным вызовом и угрозой, которая исходит от негосударственных акторов. В международном праве киберпреступление является преступлением международного характера, которое посягает как на внутригосударственный, так и на международный правопорядок. В узком смысле под киберпреступлением понимается любое противоправное деяние, осуществляемое посредством электронных операций, целью которого является преодоление защиты компьютерных систем и обрабатываемых ими данных. Киберпреступление в широком смысле означает любое противоправное деяние, совершаемое посредством или в связи с компьютерной системой или сетью, включая такие преступления, как незаконное хранение, распространение информации посредством компьютерной системы или сети. Данная проблема носит глобальный характер, которая будет возрастать по мере распространения и развития информационных технологий. В связи с этим эффективное международное сотрудничество, а также координация усилий мирового сообщества в сфере предупреждения и ликвидации последствий киберпреступлений имеет огромное значение, так как бороться с этим противоправным деянием в сфере информационно-коммуникационных технологий (далее – ИКТ) на уровне отдельного государства представляется практически невозможным.

Во-вторых, на сегодняшний день, в международном праве отсутствует консолидированный подход к пониманию термина киберпреступление. Вопрос понятийно-категориального аппарата является одним из существенных пунктов в международных договорах. Отсутствие единого подхода к пониманию самой сущности и несогласованности терминологии в международных документах, а также в доктринах свидетельствует о специфических особенностях данного криминального явления.

В-третьих, проблема киберпреступности является многогранной, требующей четкого и скоординированного принятия мер. Стоит отметить возрастание роли транснациональных и неправительственных организаций, которые превратились в важнейший инструмент по борьбе с киберпреступлениями и их расследованию. Постепенное интегрирование искусственного интеллекта, как превентивной меры, видится эффективным методом борьбы против киберпреступлений.

В-четвертых, современная множественность внутригосударственных правовых систем говорит о затруднении координации в части регулирования противодействия киберпреступлениям на национальном уровне. Сближение и унификация уголовного права, уголовно-процессуального права является неотъемлемым требованием для усовершенствования международного-правового сотрудничества в области противодействия киберпреступлениям

Таким образом, с юридической точки зрения киберпреступления являются важным объектом для изучения, а надлежащее научное обоснование, в свою очередь, помогает определить их международно-правовое регулирование. Данные положения обусловили выбор темы научного исследования.

Степень научной разработанности темы исследования.

Вопрос международной информационной безопасности, которая включает в себя международно-правовое регулирование противодействия киберпреступлениям, является одним из самых неоднозначных и дискуссионных проблем со времени появления этого феномена. Отсутствие консолидированной концепции в отношении киберпреступлений порождает определенные сложности в части международно-правового регулирования противодействия киберпреступлениям. Состояние существующего международного права в отношении борьбы с киберпреступлениями вызвано генезисом и определенными причинами развития киберпреступлений. В основу диссертационного исследования заложен анализ ряда международных

соглашений, национального законодательства, а также доктрин ученых в части киберпреступлений.

На сегодняшний день достаточного внимания анализу проблемы международно-правового регулирования противодействия киберпреступлениям в научной отечественной литературе должным образом не уделено, многие вопросы ее остаются открытыми. Отечественные юристы, специализирующиеся в международном праве, ограничиваются небольшими статьями в части отдельных аспектов киберпреступлений, вследствие чего актуальность научного исследования увеличивается. Большая часть монографий, посвященных особенностям международно-правового регулирования противодействия киберпреступлениям, написаны иностранными учеными. На национальном уровне существует пробел в части диссертационных исследований, посвященных объекту данной работы.

В доктрине международного права феномен киберпреступления не имеет консолидированного подхода. Ряд концепций относительно определения понятия, сущности, международно-правового противодействия и классификации киберпреступлений продолжают являться предметом научных обсуждений. Анализ международных соглашений в части киберпреступлений, а также выработка новой универсальной конвенции, которая будет регулировать киберпреступления, видятся необходимыми для решения данной проблематики.

Актуальность исследования, недостаточная разработанность выбранной темы определили цели, задачи и структуру диссертационного исследования.

Целью диссертационного исследования является проведение подробного анализа теоретических и практических вопросов, коррелирующих с международно-правовым регулированием противодействия киберпреступлениям, а также выработка конкретных предложений для решения данной проблемы.

Для достижения указанной цели ниже приведены следующие **задачи**:

– раскрыть существенные юридические характеристики понятия «киберпреступление» и дать определение этому понятию в праве с позиции автора;

– привести существующие правовые подходы в части применения термина «киберпреступление»;

– провести сравнительно-правовой анализ международных соглашений, регулирующих противодействие киберпреступлениям;

– определить классификацию киберпреступлений, которая не закреплена в международных договорах;

– проанализировать алгоритм работы систем искусственного интеллекта в качестве противодействия киберпреступлениям;

– определить институт международно-правовой ответственности государств за совершение киберпреступлений.

Объект диссертационного исследования – правоотношения, образующиеся в процессе международно-правового регулирования оснований и принципов ответственности за киберпреступления.

Предмет исследования – принципы и нормы международного права, регламентирующие основы международно-правового регулирования противодействия киберпреступлениям, а также судебная практика по данного рода преступлениям.

Методологические основы исследования.

Применены такие методы научного познания как общественные, так и социальные явления и процессы, в том числе явления правовой действительности: общенаучные и частнонаучные методы. Приведем общенаучные методы:

1) Диалектический метод. Сыграл важную роль в части подробного изучения предмета диссертации в его постоянном прогрессе с учетом корреляции с иными юридическими явлениями.
2) Метод анализа. Благодаря методу анализа были достигнуты задачи и цели, содержащиеся в диссертации.

3) Метод синтеза. Использован при определении толкований основных понятий по теме диссертации комплексному рассмотрению вопросов данной проблематики.

Далее приведем частнонаучные методы:

1) Формально-юридический метод. Данный метод был применен при формулировании конкретного смысла терминов, использованных в научном исследовании, для понимания содержания положений Протокола Конвенции ООН об использовании ИКТ в противоправных целях, а также других международных соглашений.
2) Сравнительно-правовой метод. Использовался в целях соотношения международных соглашений и норм внутригосударственного права в части киберпреступлений для выявления и анализа особенностей регулирования данной области, а также решения конкретных задач.

Теоретическую основу диссертационного исследования составили основные идеи и выводы, отображенные в работах отечественных и иностранных исследователей, в которых освещаются аспекты теории международного права, киберпрестпулений и международной информационной безопасности: А.Х. Абашидзе, П.Н. Бирюков, А.Г. Волеводз, А.Н. Вылегжанин, А.А. Ефремов, А.А. Данельян, Ю.Н. Жданов, Б.Л. Зимненко, Д.В. Красиков, А.В. Крутских, В.Д. Зорькин, М.Б. Касенова, Н.Н. Липкина, И.И. Лукашук, А.Б. Мезяев, А.В. Наумов, Т.Н. Нешатаева, А.Ю. Скуратова, Б.Р. Тузмухамедов, Г.И. Тункин, В.П. Талимончик, Т.Л. Тропина, В.Л. Толстых, Н.А. Чернядьева, А.В. Яковенко, М.Ч. Бассиуни, Томас Ж. Холт, Адам М. Босслер, Хусам аль-Таи, Самули Хаатажа, Д.Е. Деннинг, Габриэль Вейман, Мора Конвей, Али Джахангири, Д. Абрахам, Уильям А. Оуэнс, К. Уилсон, Штейн Шолберг и другие.

Правовой основой исследования послужили: внесенный Российской Федерацией проект Конвенции ООН о противодействии использованию информационно - коммуникационных технологий в преступных целях от 27 июля 2021 года (далее – проект Конвенции ООН), Конвенция Совета Европы

о преступности в сфере компьютерной информации 2001 года (далее – Конвенция СЕ), Соглашение о сотрудничестве государств-участников СНГ в борьбе с преступлениями в сфере информационных технологий 2018 года (далее – Соглашение СНГ), Соглашение между правительствами государств – членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности 2009 года (далее – Соглашение ШОС), Директива № 2013/40/ЕС Европейского парламента и Совета Европейского Союза об атаках на информационные системы и о замене Рамочного Решения 2005/222/ПВД (далее – Директива ЕС), Конвенция Африканского союза о кибербезопасности и защите персональных данных 2014 года (далее – Конвенция АС), Конвенция Лиги Арабских Государств о борьбе с преступлениями в сфере информационных технологий 2010 года (далее – Конвенция ЛАГ), Уголовный кодекс Российской Федерации (далее – УК РФ).

Эмпирическую основу составили доклады Группы правительственных экспертов ООН, резолюции Генеральной Ассамблеи ООН в части киберпреступлений, а также судебные решения национальных и международных судов.

Научная новизна диссертационного исследования состоит в том, что впервые в отечественной юридической науке осуществлен всесторонний анализ регулирования предупреждения киберпреступлений. Диссертантом в комплексном виде осуществлен сравнительно-правовой анализ международных соглашений, регламентирующих киберпреступления. При изучении сущности киберпреступления, в диссертационном исследовании были не только выявлены характеристики данного противоправного деяния, но и сформулировано автором исследования его понятие, а также определена новая классификация киберпреступлений, не содержащаяся в международных договорах. В исследовании проанализированы институциональные и договорные формы сотрудничества между государствами в целях противодействия киберпреступлениям и аргументирована позиция в

отношении того, какие акты (*hard law vs soft law*) являются наиболее эффективными в части регулирования данной проблемы. Доказано, что нормы мягкого права, носящие рекомендательный характер, являются наиболее приоритетными, и содержатся в специальных источниках - актах органов международных организаций, стандартах, регламентах, рекомендациях, кодексах, инструкциях, разработанных в целях регулирования киберпреступлений, а также обеспечения кибербезопасности. Более того, исследование содержит анализ систем искусственного интеллекта (далее – ИИ), что позволило прийти к выводу о том, что посредством установления специального алгоритма, ИИ способен обеспечить надлежащую киберзащиту.

Проведенное исследование позволило диссертанту сформулировать и обосновать следующие основные **положения, выносимые на защиту и содержащие элементы научной новизны:**

1. Доказано, что киберпреступление является преступлением, обладающее трансграничным характером – происходит на территории двух и более государств. Трансграничность выражается в появлении иностранного элемента в правоотношениях и, как следствие, угрожает национальным правопорядкам двух или более государств. Более того, о трансграничном характере говорит то, что киберпреступление не ограничено территориальными границами одного государства. Таким образом, трансграничность киберпреступления характеризуется отсутствием каких-либо ограничений по субъектному составу и способам совершения, поскольку информационное пространство не имеет определенных границ, и его последствия выходят за пределы правопорядка отдельного государства в силу степени общественной опасности.

2. Имея ввиду отсутствие в международных соглашениях общепризнанного универсального определения киберпреступления, что связано с несогласованностью терминологии в международных документах, а также с отсутствием в доктринах единого понятия киберпреступления, предлагается определить киберпреступление – как виновно совершенный,

несанкционированный доступ к информационно-коммуникационным технологиям при помощи компьютерных устройств и иных технических средств, с целью нанесения как материального, так и нематериального ущерба и влекущее негативные последствия трансграничного характера неограниченному кругу лиц.

3. Выявлено, что в настоящий момент, учитывая стремительное развитие технологий в эпоху цифровизации, классификация киберпреступлений, содержащаяся в действующих международных соглашениях, не является исчерпывающей. В основном международные соглашения содержат перечень киберпреступлений, которые направлены против конфиденциальности, целостности и доступности компьютерных данных и систем (неправомерный доступ, перехват информации), а также, связанные с использованием компьютерных средств (мошенничество). Такие преступления в сфере информационных технологий, как криптоджекинг (противоправное использование технических средств преступниками в целях получения криптовалюты), кибербуллинг (оскорбления в сети «Интернет» с использованием цифровых технологий), дипфейк (генерация изображения или голоса с использованием нейросети), вещевой кардинг (приобретение товаров в онлайн-магазинах, посредством оплаты с чужой кредитной карты и тд.) в международных соглашениях не закреплены.

Предлагается выделить дополнительную классификацию киберпреступлений по следующему критерию объекта: «противоправное использование информационно-коммуникационных технологий в целях нарушения прав личности в части чести и достоинства, а также собственности в информационном пространстве». Из данного тезиса вытекают следующие виды киберпреступлений: а) кибербуллинг, б) дипфейк, в) криптоджекинг, г) вещевой кардинг.

4. Установлено, что борьба с киберпреступностью носит международно-правовой характер. Средством борьбы с киберпреступлениями может выступить ИИ, роль которого применимо к киберпреступлениям двойственна.

Во-первых, постепенное интегрирование искусственного интеллекта, как превентивной меры и упреждающего удара, может быть эффективным методом борьбы против киберпреступлений и обеспечения международной информационной безопасности в целом. Во-вторых, ИИ также может нести угрозу международной информационной безопасности, если системы ИИ окажутся в распоряжении умелых киберпреступников, способных взламывать базы данных, осуществлять кибератаки на инфраструктуру, критически важные объекты и при этом оставаться латентными. В исследовании делается вывод о том, что обычные нормы международного права и механизмы международно-правовых институтов в части реализации ИИ не работают.

Предлагается противостоять киберпреступлениям при помощи ИИ путем разработки исходного кода внутреннего инструмента специального программного обеспечения (далее – ПО), посредством которого разработчики систем ИИ смогут находить риски и тем самым выявлять проблемы кибербезопасности.

5. Выявлено, что современная множественность национальных правовых систем свидетельствует о невозможности координации регулирования противодействия киберпреступлениям на национальном уровне. В современном мире положения правовых норм, противоречащих друг другу, приводят к коллизиям национальных законов, и как следствие, к невозможности их регулирующего действия на территории разных государств, так и реализаций наказаний за их нарушение.

Сделан вывод о том, что сближение национальных правовых систем в части криминализации во внутреннем законодательстве деяний, совершенных с использованием компьютерных технологий, а также включения в национальный уголовный процесс норм о процессуальных действиях, специфических для расследования и судебного разбирательства по делам о киберпреступлениях осуществимо через международные договоры универсального и регионального характера.

6. Установлено, что сотрудничество на региональном уровне особо значимо. На сегодняшний день в рамках Евразийского экономического союза (далее – ЕАЭС) отсутствует многостороннее соглашение в части противодействия киберпреступлениям. Сотрудничество через двусторонние международные договоры между государствами-участниками оказалось малоэффективным, так как киберпреступления нарушают правопорядок более двух государств. В целях преодоления данной проблемы видится необходимым принятия договора под эгидой ЕАЭС, который сможет обеспечить безопасность информационного пространства путем обмена информацией, взаимной помощью в части расследования киберпреступлений, а также запросах о выдаче преступников.

Вышеперечисленные механизмы взаимодействия должны обеспечить эффективность в части сотрудничества между странами-участниками ЕАЭС, а помощь их в реализации должен оказать специально созданный международный правоохранительный орган регионального характера.

7. Доказано, что принятие на универсальном уровне международного соглашения, регламентирующего усовершенствованные формы сотрудничества и усиление превентивных мер в части оказания противодействия киберпреступлениям, является актуальным. Резолюцией ГА ООН 79/243 от 24 декабря 2024 года принята Конвенция ООН против киберпреступности; Укрепление международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационно-коммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьезным преступлениям (далее – Конвенции ООН против киберпреступности), разработанная Россией. Конвенции ООН против киберпреступности предусматривает реализацию международного сотрудничества в сфере оперативно-розыскной деятельности, ареста и возврата активов. Закрепляется цифровой суверенитет государств над своим информационным пространством, в том числе

посредством наращивания международного взаимодействия между компетентными ведомствами.

Сделан вывод о важности создания в будущем международной правоохранительной организации универсального характера, наделенной компетенцией в части осуществления международной оперативно-розыскной деятельности в целях выявления, пресечения или раскрытия наиболее тяжких киберпреступлений, а также международных расследований на досудебных стадиях уголовного судопроизводства. Кроме того, в целях осуществления международного уголовного правосудия возможно создание специального трибунала ad hoc по международным киберпреступлениям.

8. Подчёркивается, что экстрадиция по-прежнему остается одним из традиционных механизмов сотрудничества в части борьбы с киберпреступлениями. Однако, как показывает практика, государства отказывают в экстрадиции со ссылками на нормы внутригосударственного законодательства. Делается вывод, что если государство по каким-либо причинам отказывается в выдаче, то оно обязано само осуществить правосудие. Тем не менее, суды подчеркивают, что государства, которые берут на себя ответственность судить преступников из другого государства, должны соблюдать основополагающие принципы справедливого судебного разбирательства, а также обеспечивать гуманное обращение к таким преступникам.

Теоретическая значимость результатов диссертационного исследования состоит в том, что данные, полученные при проведении настоящего исследования, имеют ценность в связи с тем, что они дополняют теоретические представления о правовых аспектах регулирования противодействия киберпреступлений как преступлений международного характера. Сформированные в диссертации теоретические положения могут использоваться для дальнейших исследований в области регламентации предупреждения киберпреступлений.

Практическая значимость результатов диссертационного исследования состоит в том, что полученные результаты исследования могут быть применены правоохранительными органами Российской Федерации в части уголовного преследования за совершение киберпреступлений. Более того, результаты проведенного исследования могут быть использованы в рамках разработки международного договора универсального характера под эгидой ООН или регионального международного договора ЕАЭС.

Апробация результатов диссертационного исследования. Диссертационная работа выполнена и обсуждена на кафедре международного права Федерального государственного бюджетного образовательного учреждения высшего образования «Российский государственный университет правосудия». Основные положения и выводы диссертации отражены в опубликованных научных статьях, в том числе в рецензируемых научных изданиях, рекомендованных Высшей аттестационной комиссией при Министерстве науки и высшего образования Российской Федерации, были изложены во время выступлений на международных, всероссийских и региональных научно-практических конференциях, на заседании Ученого совета ФГБОУ ВО «РГУП».

Материалы научного исследования использованы автором в учебном процессе при подготовке и проведении лекций, а также семинарских занятий на факультете подготовки специалистов для судебной системы ФГБОУВО «Российский государственный университет правосудия» по дисциплинам «Международное право», «Международное частное право», Международное уголовное право».

Структура диссертации определена логикой исследования. Диссертация состоит из введения, двух глав, включающих в себя шесть параграфов, заключения и списка литературы.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** обоснована актуальность темы диссертационного исследования, охарактеризована степень научной разработанности темы, сформулированы цели и задачи диссертации, определены объект и предмет работы, методологическая, теоретическая, правовая, эмпирическая основы исследования, обозначена научная новизна, приведены положения и выводы, выносимые на защиту, определены теоретическая и практическая значимость результатов диссертационного исследования, приведены сведения об их апробации и структуре работы.

Первая глава исследования **«Характеристика киберпреступления в международно-правовой науке»** делится на три параграфа: **«Определение понятия киберпреступление в международном праве»**, **«Виды киберпреступлений согласно современным международно-правовым актам» и «Киберпреступление как новый вид международного преступления»**.

Первая глава исследования посвящена правовому анализу киберпреступлений с целью выявить основные признаки и черты, а также определить понятие киберпреступления в международном праве. Рассматривается подробная классификация киберпреступлений в соответствии с современными международными соглашениями, и возможность квалифицировать киберпреступление – как новый вид международного преступления.

В **первом параграфе «Определение понятия киберпреступление в международном праве»** анализируются доктринальные позиции как отечественных, так и зарубежных авторов в части определения термина «киберпреступление». Более того, исследование показало отсутствие в международных соглашениях единообразно понимаемого и применяемого нормативно-закрепленного определения понятия «киберпреступление». Тем

не менее, исходя из анализа доктринальных подходов, а также международных договоров в части регулирования киберпреступлений, выкристаллизовывается консолидированный подход в отношении того, что киберпреступление обладает трансграничным характером. Предлагается определить киберпреступление – как виновно совершенный, несанкционированный доступ к информационно-коммуникационным технологиям при помощи компьютерных устройств и иных технических средств, с целью нанесения как материального, так и нематериального ущерба и влекущее негативные последствия трансграничного характера неограниченному кругу лиц.

Во **втором параграфе «Виды киберпреступлений согласно современным международно-правовым актам»** производится классификация всех существующих видов киберпреступлений, которые закреплены в международных соглашениях. Произведен сравнительно-правовой анализ Конвенции СЕ с Директивой ЕС, Соглашением СНГ, Соглашением ШОС, Конвенцией АС, а также проектом Конвенции ООН и УК РФ. Автор приходит к выводу, что европейский опыт правового регулирования данного вопроса является наиболее наработанным и практически апробированным. Тем не менее проект Конвенции ООН является существенно прогрессивнее ныне действующих международных соглашений, так как в нем заложены эффективные механизмы сотрудничества, в частности, в вопросах выдачи и оказания правовой помощи по уголовным делам, включая выявление, арест, конфискацию и возврат активов. Кроме того, данный документ предлагает усовершенствовать форму сотрудничества. Введение меры предварительного сохранения электронной информации по запросу направлена на минимизацию рисков утечки цифровых данных. Это нововведение является важным с точки зрения расследования киберпреступлений. Более того, проект Конвенции ООН дублирует 10 видов киберпреступлений, содержащиеся в Конвенции СЕ, а также вводит новые 12 видов преступлений в сфере ИКТ, которые в Конвенции СЕ не освещены. Среди неосвещенных в Конвенции СЕ киберпреступлений можно выделить

следующие: склонение к самоубийству или доведение до его совершения, оправдание геноцида, незаконное распространение фальсифицированных лекарственных средств и медицинских изделий. Предложенный Российской Федерацией подход фактически закрепляет цифровой суверенитет государств над своим информационным пространством и открывает новую страницу в истории глобального противодействия киберпреступлениям.

Более того, автор анализирует киберпреступления, которые на сегодняшний день являются актуальными и не имеют нормативного закрепления на международном уровне. Такие преступления в сфере информационных технологий, как криптоджекинг (противоправное использование технических средств преступниками в целях получения криптовалюты), кибербуллинг (оскорбления в сети «Интернет» с использованием цифровых технологий), дипфейк (генерация изображения или голоса с использованием нейросети), вещевой кардинг (приобретение товаров в онлайн-магазинах, посредством оплаты с чужой кредитной карты) в международных соглашениях не закреплены.

В **третьем параграфе «Киберпреступление как новый вид международного преступления»** киберпреступление рассматривается с точки зрения международного преступления. Проведенный анализ международных соглашений, а также доктринальных подходов показал, что киберпреступление, направленное одним государством против другого, можно отнести к акту применения силы, если данное киберпреступление нарушает цифровой суверенитет государств и тем самым угрожает международной информационной безопасности. В практическом плане в контексте права на самооборону по ст. 51 Устава ООН международному сообществу следовало бы выработать четкие категории, позволяющие квалифицировать киберпреступление как «применение силы» или «акт агрессии», и соответственно, приравнять к международному преступлению, а также соответствующие критерии для квалификации информационно-коммуникационных технологий в качестве оружия. Кроме того, важно, чтобы

в отношении киберпреступлений было проведено расследование в соответствии с международным правом. Широкомасштабные и систематические киберугрозы будут оставаться безнаказанными без универсального международного правоохранительного органа в действии. На сегодняшний день Международная организация уголовной полиции – Интерпол координирует сотрудничество в части противодействия в отношении киберпреступлений, а его оперативно-розыскные полномочия ограничены рамками информационного содействия.

Таким образом, современные тенденции международной преступности требуют создание универсальной международной правоохранительной организации, наделенной компетенцией в части осуществления международной оперативно-розыскной деятельности в целях выявления, пресечения или раскрытия наиболее тяжких киберпреступлений, а также международных расследований на досудебных стадиях уголовного судопроизводства. Кроме того, в целях осуществления международного уголовного правосудия возможно создание специального трибунала ad hoc по международным киберпреступлениям.

Вторая глава исследования **«Международно-правовое противодействие киберпреступлениям»** делится на три параграфа: «**Международные соглашения в части противодействия киберпреступлениям», «Практика международного расследования, реализация противодействия и гармонизация национального законодательства государств», «Искусственный интеллект и кибербезопасность. Вопросы юрисдикции, экстрадиции, ответственности государств».**

Вторая глава исследования посвящена анализу международных договоров в части противодействия киберпреступлениям; соотношению норм международного и внутригосударственного уголовного права; рассмотрению обычных норм международного права и механизмов международно-правовых институтов в части реализации ИИ.

В **первом параграфе «Международные соглашения в части противодействия киберпреступлениям»** проводится подробный анализ международных соглашений в целях выявления методов международно-правового сотрудничества в сфере противодействия использованию ИКТ в преступных целях, а также выяснения, является ли регулирование данного вопроса универсальным или региональным. Более того, в рамках данного параграфа предпринимается попытка определить, акты обязательного характера или мягкого права, которые являются наиболее эффективными в части регулирования данной проблемы. Кроме того, делается вывод о том, что международное взаимодействие между государствами в части противодействия киберпреступлениям осуществляется через институциональные и договорные формы.

В основу данного параграфа заложен анализ правовых документов, разработанных в контексте 16 международных организаций. Стоит отметить, что документы различаются по юридической силе и соответствующим правовым последствиям. Исходя из критерия обязательности, данные документы разделены на две группы: обязательные и рекомендательного характера.

Так, ряд документов (Соглашение о сотрудничестве государств – участников СНГ в борьбе с преступлениями в сфере информационных технологий 2018 г., Конвенция Африканского союза о кибербезопасности и защите персональных данных 2014 г., Конвенция Лиги арабских государств о борьбе с преступлениями в области информационных технологий 2010 г., Конвенция Совета Европы о киберпреступности 2001 г. и др.) имеют характер межгосударственных соглашений, что влечет наложение определенных юридических обязательств на государство-участника в соответствии с принципом добросовестного выполнения обязательств, принятых на себя в соответствии с международным соглашением.

Другие документы (Резолюции ГА ООН, Рекомендации Организации экономического сотрудничества и развития (ОЭСР), Типовые законы

Содружества Наций о компьютерных преступлениях и электронных доказательствах 2002 г., Типовой закон о компьютерных преступлениях и киберпреступности Сообщества развития Юга Африки (САДК) 2012 г., и др.) носят рекомендательный характер и выступают в качестве общих правовых рамок и типовых моделей законодательства в сфере противодействия киберпреступности, что, в свою очередь, не предполагает установление каких-либо юридических обязательств для государств.

Автор приходит к выводу, что правовые механизмы противодействия киберпреступлениям предусмотрены преимущественно в многосторонних международных соглашениях регионального характера. Одна из причин кроется в открытом доступе к компьютерным данным государств. В основном дружественные государства идут на такой шаг сотрудничества. Однако практика показывает, что не все страны готовы поделиться информацией друг с другом и ссылаются на общие принципы международного права о невмешательстве в дела, входящие во внутреннюю компетенцию государств.

Анализ международных соглашения в части противодействия киберпреступлениям выявил следующие методы международного сотрудничества:

1) осуществление уголовного преследования по запросам иностранных государств;
2) запрос об оказании взаимной помощи;
3) выдача преступника;
4) передача лиц для отбывания наказания в государствах гражданства.

Ни международные акты обязательного характера, ни международные акты рекомендательного характера, по сути, не играют важную роль в части противодействия преступлениям в сфере ИКТ. Вышеприведенные международные акты охватывают недостаточный на сегодняшний день объем киберпреступлений. Так, например, за пределами международных соглашений оказался кибербуллинг, который представляет собой угрозы, диффамации, намеренные оскорбления и осуществляется в информационном пространстве

через информационно-коммуникационные каналы и средства ЭВМ. Кроме того, нельзя не отметить, что классические методы международного сотрудничества, включая запросы, взаимопомощь и т. д., использовавшиеся в прошлом столетии и ранее, являются неактуальными в эпоху, когда преступления могут совершаться из любой точки мира «со скоростью света». Международные соглашения в части противодействия киберпреступлениям носят фрагментарный характер и нуждаются в совершенствовании как на универсальном, так и на региональном уровне. Тем не менее, источниковая база в сфере регулирования киберпреступлений отличается преобладающей ролью норм мягкого права. Это обуславливается тем, что акты мягкого права образуют фундамент в части выработки соглашений обязательного характера.

Институциональный подход является одним из способов противодействия киберпреступлениям. Достаточно известным на сегодняшний день осуществляющим широкий круг функций в области международного правоохранительного сотрудничества является Агентство Европейского союза по сотрудничеству в правоохранительной сфере. Европол является региональным полицейским агентством, который осуществляет координацию работы правоохранительных органов государств в рамках ЕС, вправе ставить перед ними вопросы о создании совместных следственных групп, участвовать в совместных расследованиях. В рамках АС действует Механизм Африканского союза по полицейскому сотрудничеству (АФРИПОЛ), наделенный полномочиями в части обмена информацией или разведывательными данными в целях предотвращения транснациональных организованных преступлений, террористических актов, киберпреступлений и борьбы с ними. В рамках СНГ существует многостороннее соглашение в части противодействия преступлениям в сфере информационных технологий. Кроме того, в рамках данной международной организации функционирует Бюро по координации борьбы с организованной преступностью и иными опасными видами преступлений на территории государств – участников СНГ.

Таким образом, формирование и деятельность региональных международных организаций и специализированных учреждений по сотрудничеству между правоохранительными органами ныне представляет собой доминирующую тенденцию современного развития институтов международного полицейского сотрудничества. Установлено, что на сегодняшний день у ЕАЭС отсутствует многостороннее соглашение в части противодействия киберпреступлениям. Сотрудничество через двусторонние международные договоры между государствами-участниками не работает, так как киберпреступления нарушают правопорядок более двух государств. В целях преодоления данной проблемы видится необходимым принятие договора под эгидой ЕАЭС, который сможет обеспечить безопасность информационного пространства путем обмена информацией, взаимной помощью в части расследования киберпреступлений, а также запросов о выдаче преступников. Вышеперечисленные механизмы взаимодействия должны обеспечить эффективность в части сотрудничества между странами-участниками ЕАЭС, а помощь в их в реализации должен оказать специальный международный правоохранительный орган. Региональный уровень сотрудничества отличает более скоординированный и углубленный характер. В связи с этим, целесообразным является учреждение регионального международного правоохранительного органа в рамках ЕАЭС.

Во **втором параграфе «Практика международного расследования, реализация противодействия и гармонизация национального законодательства государств»** приведены позиции ученых международного права в части определения преступлений международного характера. По мнению М.Ч. Бассиуни, преступления международного характера содержат «иностранный элемент», т. е. угрожают правовым порядкам двух или более государств. Таким образом, для признания киберпреступления преступлением международного характера осложнение «иностранным элементом» должно быть выражено в форме негативных последствий правопорядкам двух или более государств. Исходя из вышеизложенного, в международном праве

киберпреступление является преступлением международного характера, которое посягает как на внутригосударственный, так и на международный правопорядок. Это противоправное деяние, которое не ограничено территориальными границами одного государства, что говорит о его трансграничном характере. Например, киберпреступление совершено в отношении конкретного физического лица, а его последствия нарушили публичный порядок. Более того, в рамках данного параграфа делается вывод, что гармонизация внутригосударственных правовых систем является позитивным шагом в целях борьбы против киберпреступлений. Сближение уголовного и уголовно - процессуального права государств в целях решения технических и юридических трудностей, связанных с нынешним международным сотрудничеством, является необходимым. В международных договорах, посвящённых киберпреступлениям, прописано, что основная роль в части реализации уголовного расследования киберпреступлений относится к внутригосударственному праву. С одной стороны, в нем должна быть прописана подробная инструкция обеспечения их предписаний, а с другой отображаться преобладающие нормы международных актов. Нормами международного права должны регулироваться общие вопросы, содержащиеся в международных договорах и направленные на противодействие киберпреступлениям будут отображены в общем виде, однако для решения казусов уголовного судопроизводства необходимо проработанное юридическое обеспечение на внутригосударственном уровне. Меры в части борьбы с киберпреступлениями, принимаемые на международном уровне, должны быть синхронно установлены и на внутригосударственном уровне. Совместные усилия как на международном, так и на внутригосударственном уровне должны связывать и дополнять друг друга в целях надлежащего обеспечения координации, а также эффективного сотрудничества в части борьбы против преступлений в сфере информационных технологий и сближения внутригосударственных законодательств.

В **третьем параграфе «Искусственный интеллект и кибербезопасность. Вопросы юрисдикции, экстрадиции, ответственности государств»** анализируются системы ИИ в части противодействия киберпреступлениям и обеспечения кибербезопасности. Обычные нормы международного права и механизмы международно-правовых институтов в части реализации ИИ не работают. Однако, делается вывод о том, для того чтобы эффективно противостоять киберпреступлениям при помощи ИИ, необходимо использовать хакерскую стратегию. Противостоять преступлениям в сфере информационных технологий при помощи нейросети возможно путем разработки исходного кода внутреннего инструмента специального ПО, посредством которого разработчики систем ИИ смогут находить риски и тем самым выявлять проблемы информационной безопасности. Сотрудники «Microsoft» создали исходный код внутреннего инструмента «PyRIT», который способен посодействовать разработчикам в обнаружении рисков в моделях нейросети. «PyRIT» автоматически генерирует тысячи состязательных запросов нейросети, с целью проверить способен ли ИИ эффективно противодействовать попыткам взлома. Алгоритм работы инструмента сгенерирован таким образом, что позволяет разработчикам добавлять разных видов ввода систем ИИ, например, голоса или изображения.

Кроме того, для преодоления киберпреступления необходимо соблюдать правила процедур взаимодействия в части противодействия данному противоправному деянию согласно принципам и нормам международного права. Экстрадиция является одним из механизмов сотрудничества в части борьбы с киберпреступлениями, однако, как показывает практика, государства нередко нарушают правовые основания в выдаче. Тем не менее, суды подчеркивают, что государства, которые берут на себя ответственность судить преступников из другого государства, должны соблюдать основополагающие принципы справедливого судебного разбирательства, а также обеспечивать гуманное обращение с такими преступниками. Если государство по каким-

либо причинам отказывается в выдаче, оно обязано само осуществить правосудие.

В параграфе также показано, что проблема в отсутствии четких правил юрисдикции порождает трудность у государств в части регулирования киберпространства. Киберпространство не имеет четких территориальных границ. Таким образом, становится затруднительно определить конкретную страну, где преступник получает доступ к сети «Интернет» или с территории какого государства отправляется конкретная компьютерная информация.

Более того, международное право позволяет одному государству привлечь к международно-правовой ответственности другое государство за совершение киберпреступления против него или нарушение международно-правового обязательства в киберпространстве. Основным источником права международной ответственности является комплекс международно-правовых обычаев, который, как это широко признано в практике государств и институтов международного правосудия, в значительной степени отражен в принятых Комиссией международного права в 2001 г. Проектах статей об ответственности государств за международно-противоправные деяния. Однако государство, которому в той или иной форме причинен вред в результате совершения киберпреступления, не всегда в состоянии самостоятельно предпринять все необходимые действия для сбора доказательств, в том числе в силу территориальной ограниченности исполнительной юрисдикции. Таким образом, несмотря на применимость норм общего права международной ответственности к отношениям в киберпространстве, существуют определённые сложности в части присвоения государствам поведения, связанного с причинением трансграничного вреда с использованием ИКТ.

В **заключении** подводятся итоги проведенного исследования и формируются основные выводы.

Основные положения диссертации опубликованы:

В рецензируемых научных изданиях, рекомендованных Высшей аттестационной комиссией при Министерстве науки и высшего образования Российской Федерации:

1. Аббуд Р.Р. Киберхалифат: новый неисследованный субъект в международном информационном пространстве // Электронное сетевое издание «Международный правовой курьер». – 2017. - № 1. – С. 61-65.
2. Аббуд Р.Р. Киберхалифат: нормативное определение и криминологическая характеристика в национальном и международном информационном праве // Вопросы российского и международного права. – 2018. - Том 8 № 8А. – С. 190-197.
3. Аббуд Р.Р. Актуальные вопросы международного права в части преступлений в сфере компьютерной информации // Евразийский юридический журнал. – 2021. - № 2 (153). – С. 43-44.
4. Аббуд Р.Р. Трансформация форм киберпреступности в условиях пандемии COVID-19 // Юридическая Наука. – 2022. - № 7. – С. 126-129.
5. Аббуд Р.Р. Международно-правовое регулирование борьбы с киберпреступлениями // Российское правосудие. – 2023. - № 4. – С. 24-30.
6. Аббуд Р.Р. Международно-правовая классификация новых киберпреступлений // Современная наука: актуальные проблемы теории и практики. Серия: Экономика и Право. – 2024. - № 8. – С. 121-124.

Публикации в сборниках научных статей / материалах конференций, индексируемых в РИНЦ:

1. Аббуд Р.Р. Актуальные проблемы международного права в части киберпреступлений – «Актуальные проблемы международных отношений и международного права», Сборник статей под редакцией Т. В. Кашириной, С. А. Агуреева, Воробьева С. В., Москва, 2021, Дипломатическая академия МИД России.

2. Аббуд Р.Р. Актуальные проблемы международного права в части преступлений в сфере компьютерной информации // Материалы Международного молодежного научного форума «ЛОМОНОСОВ-2021» / Отв. ред. И. А. Алешковский, А. В. Андриянов, Е. А. Антипов, Е. И. Зимакова. [Электронный ресурс].
3. Аббуд Р.Р. Определение термина «киберпреступность» в международном праве // Регулирование правоотношений: проблемы теории и практики: Материалы XI Всероссийской научно-практической конференции аспирантов, соискателей, магистрантов и молодых ученых в режиме видеоконференцсвязи. – М.: РГУП, 2024. – С. 20-24.
4. Аббуд Р.Р. Научные труды. Российская академия юридических наук. Труды членов Российской академии юридических наук (РАЮН) и материалы XXIV Международной научно-практической конференции. г. Москва. Издательская группа «Юрист». 2024. С. 294-303.