УДК 34

Международно-правовые механизмы противодействия транснациональной киберпреступности: вызовы унификации и проблемы имплементации в национальные правовые системы

Лазаренкова Ирина Юрьевна

Кандидат юридических наук,
Университет прокуратуры Российской Федерации,
123022, Российская Федерация, Москва, ул. 2-я Звенигородская, 15;
e-mail: lazarenkova99@list.ru

Аннотация

В статье представлен комплексный анализ современных международно-правовых механизмов противодействия транснациональной киберпреступности. Автор детально исследует ключевые вызовы, препятствующие эффективной унификации подходов к регулированию цифровых правонарушений на глобальном уровне. Особое внимание уделено критическому анализу Будапештской конвенции как основного инструмента международного сотрудничества, выявлению политических и юридических барьеров ее реализации, включая вопросы государственного суверенитета и различия правовых культур. Методологическую основу исследования составляет сравнительно-правовой анализ международных договоров, национального законодательства различных государств и практики правоприменения. Автор систематизирует основные проблемы правового регулирования: отсутствие единого понимания термина "киберпреступность", сложности трансграничного сбора и обмена электронными доказательствами, противоречия в вопросах экстерриториальной юрисдикции. В работе особо подчеркивается, что процесс имплементации международных норм в национальные правовые системы осложняется коллизиями законодательства, различиями правовых традиций (континентальное и общее право), а также неравномерным распределением технических ресурсов. Автор приходит к выводу, что, несмотря на осознание необходимости глобального ответа на киберугрозы, процесс унификации остается медленным из-за геополитических разногласий и различий в подходах к безопасности и защите прав человека.

Для цитирования в научных исследованиях

Лазаренкова И.Ю. Международно-правовые механизмы противодействия транснациональной киберпреступности: вызовы унификации и проблемы имплементации в национальные правовые системы // Вопросы российского и международного права. 2025. Том 15. № 2А. С. 69-83.

Ключевые слова

Киберпреступность, Будапештская конвенция, международное право, транснациональные преступления, унификация законодательства, цифровая безопасность, трансграничные доказательства, кибербезопасность, международное сотрудничество.

Введение

Киберпреступность, выходящая за национальные границы, представляет серьезную угрозу не только для отдельных государств, но и для всей системы международных отношений. Стремительное развитие информационных технологий позволяет злоумышленникам использовать глобальную сеть как инструмент незаконной деятельности, что усложняет процесс противодействия цифровым правонарушениям, имеющим транснациональный характер. Многие государства осознают, что одиночные усилия в этой сфере недостаточны, поэтому все более актуальным становится поиск эффективных международно-правовых механизмов, направленных на унификацию подходов и гармонизацию законодательства. Однако процесс согласования норм и практик сталкивается с многочисленными вызовами, прямо связанными с особенностями функционирования глобальной телекоммуникационной инфраструктуры и неоднородностью национальных правовых систем [Kambarov, Baigundinov, 2023]. При этом ни одно государство не может оставаться в стороне, поскольку киберпреступность, связанная с использованием вредоносного программного обеспечения, мошенничеством или неправомерным доступом к информационным ресурсам, угрожает как национальной безопасности, так и частным экономическим интересам.

Современные методы совершения киберпреступлений становятся все более изощренными. Если первоначально основной упор делался на получение несанкционированного доступа к отдельным информационным системам, то сегодня мы наблюдаем комплексные и скоординированные атаки, основанные на использовании ботнетов, массовой дезинформации, а также сочетании технических и социальных методов воздействия на пользователя. Применение криптотехнологий и сервисов в даркнете усложняет идентификацию преступников, позволяя им скрывать свое местоположение, истинную личность, а также получать нелегальные доходы. Данные факторы вынуждают международное сообщество формировать новые подходы к правовому регулированию, предусматривая расширение сотрудничества в сфере раскрытия, преследования и предотвращения транснациональных киберпреступлений [Костенко, Аксенова, 2020]. При этом невероятно важно обеспечить защиту основных прав и свобод человека, поскольку чрезмерное ужесточение контроля в цифровой сфере может вести к нарушениям принципов пропорциональности и необходимости.

Материалы и методы исследования

Важной вехой в формировании международно-правовых механизмов противодействия киберпреступности стала Конвенция Совета Европы о киберпреступности (Будапештская конвенция). Несмотря на то что изначально этот документ разрабатывался в формате регионального соглашения, его нормы стали де-факто универсальным стандартом для государств, стремящихся совершенствовать законодательство в сфере киберправа. Раздел о международном сотрудничестве включает ключевые положения, помогающие наладить оперативный обмен данными между компетентными органами разных стран, а также координировать действия по обнаружению и ликвидации сетевых угроз [Запорожец, Крайнова, 2023]. Однако ратификация и имплементация данного документа сталкивается с рядом политических и юридических препятствий. Некоторые страны критикуют положения Будапештской конвенции, считая их отражением интересов определенной группы государств, или указывают на потенциальное противоречие национальным конституционным принципам.

Возникает вопрос о том, насколько возможно создать по-настоящему глобальный формат соглашения, учитывающий разнообразие правовых культур и не ущемляющий суверенитет государств.

Одним из главных вызовов в сфере международно-правовой унификации остается проблема определения самого понятия «киберпреступление». В ряде юрисдикций даже терминология, связанная с цифровыми правонарушениями, может различаться, что создает трудности при расследовании и квалификации деяний. Некоторые государства предпочитают использовать термин «компьютерные преступления», тогда как другие — «преступления, связанные с использованием информационно-телекоммуникационных сетей» [Тетюхин, 2023]. В результате возникает фрагментарность в правовом регулировании, что, в свою очередь, осложняет последующее трансграничное взаимодействие правоохранительных органов. Нередко возникает несовпадение уровней наказания или отсутствует прямая эквивалентность составов преступления, что приводит к сложностям при выдаче подозреваемых или совместном расследовании. Международное сообщество стремится преодолеть эту проблему путем принятия руководящих документов ООН и других организаций, но на практике национальные законодательные различия сохраняют свою актуальность.

Результаты и обсуждение

Еще одним важным аспектом является обеспечение доказательной базы при расследовании транснациональных киберпреступлений. Информация очень часто хранится в облачных сервисах или на серверах, располагающихся на территории сразу нескольких государств, что требует упрощенных механизмов получения электронных доказательств. Международные договоры, предусматривающие оперативный обмен данными и взаимную правовую помощь, далеко не всегда учитывают технические особенности функционирования современных дата-центров. В некоторых случаях требуется сложная процедура запроса информации, что позволяет киберпреступникам уничтожить или изменить необходимые доказательства [Алиев, Борбат, 2020]. Такая ситуация ставит перед правоприменителями задачу ускорения взаимодействия и внедрения новых протоколов передачи данных, которые были бы признаны всеми сторонами. Однако при этом нельзя забывать о защите персональных данных, ведь передача такого рода сведений между различными юрисдикциями может приводить к злоупотреблениям и утечкам.

Одним из дискуссионных вопросов остается полномочие государственных органов в отношении проведения трансграничных оперативно-розыскных мероприятий в киберпространстве. Традиционные представления о суверенитете и территориальной юрисдикции сталкиваются с новой реальностью, в которой информация и вредоносная активность перемещаются между государствами за доли секунды [Лепешкина, 2023]. В условиях отсутствия четко регламентированных механизмов правоприменители вынуждены искать решения, иногда действуя полуофициально или выходя за рамки формальных процедур. Это порождает конфликты компетенций и недоверие между государствами. Для преодоления подобных разногласий необходимо дальнейшее развитие многосторонних соглашений, которые бы устанавливали прозрачные и универсальные нормы по проведению следственных действий в сети при соблюдении основных прав человека и национального суверенитета.

Параллельно с регулирующими документами в сфере киберпреступности набирают обороты инициативы, направленные на создание международного договора под эгидой ООН,

отражающего интересы глобального сообщества в киберпространстве [Горелик, 2021]. Этот возможный документ мог бы заложить универсальные подходы к определению киберпреступлений, закрепить принципы сотрудничества и разграничить компетенции. Тем не менее, пока что остаются существенные разногласия, связанные не только с различным видением приоритетов в сфере международной информационной безопасности, но и с политической конфронтацией, когда крупные геополитические игроки предпочитают продвигать собственные стандарты. В условиях такой сложности глобальные форматы сотрудничества формируются медленно. Странам приходится держать баланс между национальными интересами и необходимостью согласованных решений для эффективного преследования киберпреступников.

Во многих случаях решение проблем унификации осложняется вопросом правозащитных стандартов. Не все государства готовы линейно внедрять жесткие модели цифрового контроля вслед за признанными конвенциями, поскольку существуют серьезные опасения относительно возможных злоупотреблений в области электронного надзора. Если в одних правовых системах ставится превыше всего защита личных данных граждан и свободное выражение мнений, то в других — приоритет отдается государственной безопасности и недопущению экстремистской деятельности, в том числе и в интернете [Перебейносов, 2020]. Это создает риск двойных стандартов, а также затрудняет формирование единых правовых норм, которые были бы признаны всеми без исключения. Важно подчеркнуть, что международное право в сфере киберпреступности развивается на перекрестке таких принципов, как уважение к национальному суверенитету, защита основных прав человека и необходимость коллективного ответа на транснациональные угрозы.

Практическая имплементация международных норм в национальные правовые системы может идти по нескольким путям. Часть государств, желая продемонстрировать свое стремление к партнерству, первыми ратифицируют соответствующие соглашения и вносят изменения в криминальное, уголовно-процессуальное и административное законодательство. Но этот процесс далеко не всегда протекает гладко. При пересмотре норм возникают ситуации коллизий, когда, с одной стороны, нужно учесть международные требования, а с другой — не противоречить конституционным принципам и сложившимся правовым традициям [Урусова, 2024]. Кроме того, важно обеспечить достаточный уровень подготовки сотрудников правоохранительных органов, судейского корпуса и экспертов в области информационной безопасности, чтобы новые механизмы не оставались только на бумаге. Недостаток профессиональных кадров и отсутствие необходимых технических способов расследования киберпреступлений могут свести на нет все преимущества от принятия международных норм.

Информационные технологии в большинстве государств регулируются комплексом правовых актов, охватывающих разные сферы — от защиты персональных данных до регулирования электронной коммерции. Любые изменения в этих областях должны учитывать риск возникновения правовых противоречий. Допустим, государство внедряет норму о блокировке интернет-ресурсов, подозреваемых в причастности к киберпреступлениям, однако получает критику со стороны правозащитных организаций за «непропорциональные меры» [Шестак, Адигамов, 2020]. Подобные конфликты могут сдерживать процесс унификации на уровне международных конвенций, так как каждая страна старается избежать компромисса, который ей кажется слишком рискованным для собственных правовых ценностей. Несмотря на это, растущее число международных киберпреступлений стимулирует поиск баланса между принципами свободы интернета и необходимостью обеспечения общественной безопасности.

Важным фактором является и то, что различные отраслевые организации, такие как IT-компании, поставщики телекоммуникационных услуг, разработчики программного обеспечения, активно вовлечены в процессы регулирования. Их позиция может оказывать серьезное влияние на формируемые международные стандарты, так как именно в их компетенции находится обеспечение технических решений, необходимых для противодействия кибератакам. Компании, предоставляющие услуги хостинга или облачной инфраструктуры, часто имеют большую рыночную силу и могут определять собственные условия предоставления данных для правоохранительных органов [Горелик, 2023]. Отсутствие четко прописанных международно-правовых норм и разный уровень корпоративной ответственности в разных юрисдикциях играют важную роль в том, насколько эффективно государствам удается добиваться правосудия. Иногда у приватного сектора есть интерес к сохранению узкого определения киберпреступлений, чтобы избежать дополнительной регулятивной нагрузки, а в иных случаях, наоборот, крупные игроки инициируют разработку единых правил, понимая, что фрагментарность законодательства усложняет ведение бизнеса.

Отсутствие четкой, согласованной на глобальном уровне политической воли также ведет к проблемам в процессе международного взаимодействия. Некоторые страны могут не спешить с присоединением к многосторонним соглашениям, опасаясь, что это ограничит их суверенное право на регулирование интернета и проведение собственных кибероперaций. В то же время другие государства настаивают на том, что в условиях глобализации именно сотрудничество является наиболее рациональным путем решения киберугроз [Горелик, 2022]. Все эти расхождения затрудняют унификацию правовых норм и создают серьезные испытания для международного права, которое призвано обеспечивать стабильность и прогнозируемость в межгосударственных отношениях. В настоящее время идет активное обсуждение необходимости реформирования систем взаимодействия, особенно в области обмена электронными доказательствами и экстрадиции обвиняемых, чтобы процесс следствия и суда по делам о киберпреступлениях проходил оперативно и с соблюдением прав человека.

Отдельного внимания заслуживают инициативы приватно-публичного партнерства в сфере борьбы с киберпреступностью. Государства не всегда обладают достаточной технической экспертизой для выяснения обстоятельств сложных компьютерных атак, а потому сотрудничают с частными компаниями, которые берут на себя аналитику инцидентов, проведение киберрасследований и разработку мер по противодействию новым угрозам [Ивлюшкин, 2023]. Такое партнерство позволяет объединить ресурсы и знания обеих сторон, однако возрастает риск того, что важная процессуальная информация станет достоянием сторонних организаций или что коммерческие интересы возобладают над принципом публичности уголовного преследования. В международно-правовых механизмах вопрос о допустимости соответствующего сотрудничества пока не получил однозначного решения, так как каждая юрисдикция самостоятельно распоряжается тем, каким образом следует регулировать доступ частных структур к материалам уголовных дел и персональным данным подозреваемых. Результатом этого является фрагментарность регулирования и дополнительные проблемы на этапе судебного рассмотрения дел о киберпреступлениях, где доказательства, собранные частными организациями, могут вызывать сомнения в допустимости.

Не менее острой проблемой становится растущее число преступлений, связанных со шпионажем, саботажем и вмешательством во внутренние дела государств через киберпространство. Широкое использование методов социальной инженерии и целенаправленных вредоносных программ, проникающих на объекты критической

инфраструктуры, приобретает значительный размах [Карпович, Ногмова, 2022]. В таких ситуациях зачастую трудно провести четкую грань между деятельностью хакеров-одиночек, организованных преступных групп и даже государственных структур, которые могут действовать через посредников, прикрываясь нелегальными формированиями. Международно-правовые механизмы, призванные преследовать преступников, не всегда учитывают геополитический контекст и сложность задач, связанных с атрибуцией атак. В результате государства пытаются продвигать идею «ответственного поведения» в киберпространстве на площадках ООН, создавая свод добровольных, но политически значимых норм. Однако это не заменяет полноценного юридического регулирования и не снимает вопроса о том, как классифицировать и карать деяния, которые направлены на подрыв критических систем безопасности.

Хотя постепенно формируется комплексный подход к регулированию, национальные особенности остаются существенным препятствием к скорейшей унификации. Каждое государство рассматривает вопросы гармонизации закона о киберпреступлениях сквозь призму собственной правовой системы, которая может основываться на континентальном праве, общей правовой традиции или исламском праве. Различия в криминализации конкретных форм поведения, а также в структурах санкций приводят к отсутствию универсального, всем понятного механизма реагирования. В результате при наличии соглашений о выдаче (экстрадиции) нередко возникают сомнения в симметричности правовых процедур, особенно если в одном государстве за конкретное киберпреступление предусмотрено серьезное наказание, а в другом — более мягкое. Правозащитные организации поднимают вопрос о соблюдении прав человека и невозможности выдачи лиц в страны, где им может грозить несоразмерно жесткое наказание или нарушение основных судебных гарантий [Давлатзода, 2023]. Подобные обстоятельства создают состояние постоянного поиска баланса, которое делает процесс унификации достаточно инертным.

Отдельное направление дискуссии связано с формальными и неформальными сетями сотрудничества правоохранителей. К формальным можно отнести такие структуры, как Интерпол, Европол и прочие региональные или международные организации, обладающие определенным мандатом на координацию усилий в сфере борьбы с киберпреступностью. Они призваны обеспечивать консолидацию усилий государств, обмен лучшими практиками и создание баз данных, включающих сведения о киберпреступной активности [Горелик, 2021]. В то же время существуют и неформальные группы экспертов, в которых представители разных стран обсуждают чувствительные проблемы, связанные с проведением оперативных операций, тайным онлайн-наблюдением и технологиями отслеживания криптовалют. Эти группы могут более гибко реагировать на новые вызовы, но их решения не имеют обязательной юридической силы, что делает процесс унификации зависимым от доброй воли участников. Такое совмещение формальных и неформальных механизмов может быть продуктивным, однако требует четких рамок ответственности, чтобы не допускать произвольных интервенций в цифровое пространство.

Правительство многих стран пытается найти оптимальную стратегию для реформирования своего правового поля, учитывая глобальные тенденции и необходимость локальной адаптации. Возникает вопрос о том, какая модель имплементации является более эффективной: жесткий автоматический перенос международных норм в национальное законодательство или же постепенное, гибкое встраивание с учетом локальных обстоятельств [Тетюхин, 2023]. Первый вариант позволяет ускорить процесс гармонизации и продемонстрировать лояльность

международному сообществу, тогда как второй предоставляет возможность выработки более сбалансированных решений, соответствующих реальной ситуации в стране. Однако и риски при этом велики. Если законодательство слишком быстро приводится к единым стандартам, может возникнуть несоответствие с уже существующими механизмами и практиками, что приведет к путанице и неопределенности. А чрезмерно медленная имплементация делает сообщество уязвимым для транснациональных киберпреступников, которые пользуются пробелами в законодательстве и отсутствии скоординированных действий между юрисдикциями.

Важную роль в развитии международно-правовых механизмов призваны играть судебные прецеденты и практика привлечения к ответственности киберпреступников в разных странах. По мере накопления опыта суды формулируют подходы к интерпретации норм, связанных со сбором электронных доказательств, а также определяют границы ответственности провайдеров и посредников в сети. Юристы и эксперты по кибербезопасности стремятся обобщать и систематизировать эту практику, чтобы сформировать единообразие. Но трудность в том, что в правовых системах, основанных на прецедентах, каждое решение суда может вносить новые оттенки в понимание правовых норм, тогда как кодексные системы нуждаются в формальных поправках законодательства [Шестак, Адигамов, 2020]. Таким образом, образуется дополнительный барьер для унификации, ведь одно государство может ссылаться на судебную практику, а другое — исключительно на букву закона. Эта разница подходов вызывает споры не только у юристов, но и у политиков, принимающих решение о том, насколько глубоко следует интегрировать международные установки в национальное право.

Комитеты, рабочие группы и экспертные сообщества, занимающиеся киберпреступностью в рамках ООН и других международных организаций, обсуждают новые проекты конвенций или протоколов к уже существующим соглашениям [Запорожец, Крайнова, 2023]. Эти дискуссии учитывают многообразие правовых культур, пытаясь найти общий знаменатель в базовых определениях и принципах. Однако раскрытие деталей, связанных с процессуальными нормами, часто вызывает противоречия. Где-то считается приемлемым использование специального программного обеспечения для удаленного обыска компьютерных систем, а в иных юрисдикциях подобные действия маркируются как противоречащие принципам неприкосновенности частной жизни граждан. Юристы пытаются найти компромиссные формулировки, но даже при их согласовании остаются вопросы о том, как именно трактовать эти нормы на практике. Многие аналитики говорят о необходимости наращивания международного диалога и формирования культуры ответственного поведения в киберпространстве, чтобы восполнять пробелы, которые пока не могут устранить конвенционные механизмы.

Особенность цифровой эпохи в том, что преступник может действовать из любой точки мира, находясь в юрисдикции, которая не желает или не может эффективно сотрудничать с другими странами. Поэтому одним из главных препятствий к устранению киберпреступности является так называемая «безпечные гавани» — государства, предоставляющие возможность безопасно компактировать инфраструктуру для атак. Такое положение дел вызывает напряженность на международной арене, ведь заинтересованные стороны готовы применять санкции и прочие меры воздействия, чтобы склонить несговорчивые страны к сотрудничеству [Карпович, Ногмова, 2022]. Но с точки зрения международного права подобные односторонние меры вызывают вопросы о правомерности и принципах невмешательства во внутренние дела государства. Дилемма усугубляется тем, что киберпреступность часто переплетается с различными формами коррупции, когда местные чиновники могут закрывать глаза на

неугодные действия хакеров. Следовательно, механизм эффективного преследования сложен и требует комплексного политико-правового решения.

Эксперты подчеркивают, что одним из перспективных направлений может стать активное применение принципов экстерриториальной юрисдикции, однако такой подход несет риск подрыва международной стабильности. С одной стороны, государства хотели бы иметь возможность преследовать киберпреступников, совершивших вредоносные деяния против их граждан или инфраструктуры, даже если сами преступники находятся за границей. С другой стороны, бесконтрольное расширение юрисдикции может привести к политическим конфликтам и коллизиям, поскольку оно затрагивает суверенитет других стран [Алиев, Борбат, 2020]. Только многосторонние соглашения, детализирующие условия и порядок реализации экстерриториальных прав, могут снизить вероятность злоупотреблений. Однако достижение консенсуса в этом вопросе пока находится на начальной стадии, и многие государства выступают против подобных нововведений, опасаясь вмешательства в их внутреннюю политику.

Возникновение различных альянсов и группировок государств, объединяющихся по региональному или политическому признаку, также сказывается на темпе и качестве унификации. Внутри каждого блока могут формироваться собственные правила и стандарты борьбы с киберпреступностью, которые не всегда совместимы с уже существующими нормами, закрепленными в других регионах. Например, в одном интеграционном объединении могут делать упор на защиту прав человека и прозрачность государственных действий, а в другом — прежде всего стремиться к обеспечению кибербезопасности, даже если это предполагает дополнительные ограничения свободы выражения [Костенко, Аксенова, 2020]. Этот процесс еще сильнее фрагментирует международно-правовое поле, делая необходимым создание универсальных инструментов, которые признавались бы всеми участниками международного сообщества. Но пока такие инструменты формируются, мир сталкивается с реальными угрозами, требующими оперативного ответа. Отсюда возникает диссонанс между скоростью развития информационных технологий и темпами формирования правовых норм, что негативно сказывается на эффективности глобальной борьбы с транснациональной киберпреступностью.

Наряду с политическими и юридическими факторами следует учитывать и вопросы этического характера. В сфере противодействия киберпреступности часто затрагиваются личные права и свободы людей, особенно когда речь идет о массовом сборе данных, прослушивании коммуникаций или ограничении доступа к интернет-ресурсам. В ряде случаев государства могут оправдывать такие меры интересами национальной безопасности или борьбы с экстремистскими проявлениями, однако правозащитные организации и часть международного сообщества обвиняют их в несоблюдении принципа пропорциональности и избирательном применении норм [Лепешкина, 2023]. Налицо дилемма: чем более жесткими становятся инструменты противодействия киберпреступности, тем выше вероятность злоупотреблений и отступления от правовых стандартов. Ситуация осложняется отсутствием прозрачных механизмов надзора за деятельностью спецслужб, которые, под предлогом кибербезопасности, могут вторгаться в частную жизнь граждан.

Проблема имплементации международно-правовых механизмов затрагивает и аспект правовой культуры в целом. В странах с развитой правовой традицией и высоким доверием к институтам власти внедрение международных соглашений проходит легче, поскольку общество больше ориентировано на верховенство права. Там, где процветает правовой нигилизм, а законы не обеспечиваются должной властью судебных органов, киберпреступники чувствуют себя

более уверенно, поскольку вероятность реального наказания ниже [Горелик, 2022]. В результате образуется порочный круг: слабая правовая система делает страну «магнитом» для онлайн-преступников, а рост киберпреступности дополнительно подрывает доверие к государственным институтам и приводит к еще большему правовому хаосу. Международные организации и развитые государства помогают в формировании партнерств для укрепления правовой системы через образовательные программы и техническую поддержку, но это требует времени и значительных ресурсов.

В то же время на уровне национальных правовых систем могут возникать позитивные прецеденты, вызывающие интерес и у зарубежных партнеров. Например, государство может выработать комплексные механизмы государственно-частного взаимодействия в области противодействия кибератакам, грамотно разделить обязанности между правоохранительными органами, регулирующими органами в сфере связи и интернет-провайдерами. Если система окажется эффективной, другие страны могут заимствовать опыт, адаптируя его к собственной правовой среде. Подобный путь «локальной апробации» и последующего распространения практик позволяет продвигать идею международной гармонизации даже без формализованных соглашений [Ивлюшкин, 2023]. Тем не менее, из-за неоднородности судебных практик и политических приоритетов этот процесс продвигается фрагментарно, что затрудняет формирование единой архитектуры международного права в сфере борьбы с киберпреступностью.

Большое значение в противодействии транснациональной киберпреступности приобретает работа специализированных образовательных центров и международных программ подготовки кадров. Их цель — предоставить следователям, прокурорам, судьям и техническим экспертам современный инструментарий для выявления, документирования и преследования компьютерных преступлений [Перебейносов, 2020]. Кроме того, обмен опытом и регулярная переподготовка сотрудников правоохранительных органов помогают в унификации процессуальных подходов. Однако, несмотря на все усилия, в большинстве государств сохраняются существенные пробелы в плане технической оснащенности и финансирования. Специфика киберпреступлений такова, что они меняются и эволюционируют куда быстрее, чем традиционные формы правонарушений, поэтому образовательные программы должны находиться в состоянии постоянного обновления, что требует сотрудничества с научными организациями и высокотехнологичным бизнесом.

Также стоит отметить роль, которую играет кибердипломатия — новое направление внешней политики, фокусирующееся на решении вопросов, связанных с безопасностью и стабильностью в цифровом пространстве. Дипломаты, разбирающиеся в технических аспектах, могут способствовать формированию международных соглашений, учитывающих не только интересы безопасности, но и вопросы экономического развития, уважения прав человека и культурной специфики [Тетюхин, 2023]. Поддержка такого направления со стороны руководства стран создает предпосылки для более системного и комплексного подхода к вопросам унификации правовых норм в киберпространстве. Параллельно с этим одна из ключевых задач кибердипломатов — разъяснение своей национальной политики в области кибербезопасности, смягчение противоречий и достижение компромиссных решений на переговорах. Весьма вероятно, что по мере усложнения цифровых угроз значение кибердипломатии будет только возрастать, а следовательно, участие компетентных специалистов станет важным фактором для успешного продвижения международно-правовых механизмов борьбы с киберпреступностью.

Если рассматривать перспективу на ближайшие годы, то можно предположить дальнейшую активизацию работы над универсальными конвенциями или соглашениями, призванными заменить или дополнить Будапештскую конвенцию. Ускорять этот процесс будет продолжающийся рост количества киберпреступлений и ущерба, наносимого экономике и безопасности. Возможно, одним из факторов, который склонит государства к более тесной кооперации, станет масштабная кибератака, которая нанесет ущерб сразу нескольким крупным экономикам и продемонстрирует неприспособленность отдельных национальных систем. Однако и политические разногласия, и конкуренция между государствами никуда не исчезнут, поэтому нельзя рассчитывать на быстрое достижение консенсуса. Скорее, нас ожидает череда региональных инициатив, двусторонних соглашений, а также постепенная эволюция существующих международных институтов, которые в совокупности станут формировать все более плотный регулятивный каркас.

Отмечая сложности унификации на глобальном уровне, нельзя недооценивать прогресс в региональных форматах. Например, в рамках Европейского союза, Ассоциации государств Юго-Восточной Азии или Организации американских государств постепенно внедряются документы, направленные на сближение требований по кибербезопасности, обмену информацией и привлечению к ответственности правонарушителей [Урусова, 2024]. Хотя эти документы не всегда имеют прямое экстерриториальное действие, они создают мощную базу для последующего формирования единых международных правил. Региональные институты могут также функционировать как платформы для диалога и выработки механизмов быстрой реакции на киберугрозы. При этом успешные модели, опробованные в одной части мира, часто переносятся в другую, адаптируясь к локальным реалиям.

Не следует забывать и о влиянии развития квантовых вычислений, искусственного интеллекта и других передовых технологических решений на характер киберпреступности и, следовательно, на особенности правового регулирования. В ближайшем будущем может оказаться, что многие привычные методы криптографии станут уязвимы, а это значит, что концепция безопасности информационных систем должна будет перестраиваться [Kambarov, Baigundinov, 2023]. На международном уровне такая трансформация потребует согласования новых технических стандартов, обновления порядков сбора и хранения доказательств, а также пересмотра ряда юридических определений, связанных с инструментарием преступных действий в сети. Государства, обладающие финансовыми и научными ресурсами, смогут первыми адаптироваться к этим изменениям. В то же время в развивающихся странах с ограниченными ресурсами процесс будет проходить медленнее, создавая еще больший разрыв, который злоумышленники могут использовать.

Чтобы все эти вызовы не окончились для мировой системы крахом правового порядка в киберпространстве, необходима долгосрочная стратегия, в основе которой лежат принципы уважения к правам человека, международного сотрудничества и диалога культур. Повышение уровня взаимного доверия между государствами — одна из сложнейших задач, учитывая растущую геополитическую напряженность [Костенко, Аксенова, 2020]. Тем не менее, именно доверие является фундаментом, без которого любые правовые механизмы, даже самые проработанные, могут остаться на бумаге. Важнейшим элементом в этой работе станет формирование международного правосознания, ориентированного на осознание общности цифрового пространства и значимости совместного ответа на киберугрозы. И хотя до полноценной универсализации норм в сфере киберпреступности еще далеко, существующие

тенденции и создаваемые международные форматы дают основание для сдержанного оптимизма.

Серьезным стимулом для совершенствования международно-правовых механизмов становится активная позиция гражданского общества, институтов развития и научных кругов. Проводимые исследования и мониторинги ситуации в сфере киберпреступности подталкивают парламентариев к обновлению законодательства, а судебная практика расставляет акценты на пробелах правового регулирования. Различные фонды и некоммерческие организации выступают в качестве посредников между властью, бизнесом и сообществом специалистов в области информационной безопасности [Шестак, Адигамов, 2020]. Их деятельность направлена на разъяснение общественности сути международных инициатив, а также на контроль над прозрачностью принимаемых решений. Подобные механизмы обратной связи помогают корректировать политические меры, выявлять и исправлять ошибки на этапе формирования и имплементации норм. В ситуации, когда технологии развиваются стремительно, а национальные интересы часто вступают в клинч с принципами глобальной безопасности, подобный подход может оказаться спасительным.

В ходе дальнейшей эволюции международных институтов уже не будет достаточно полагаться на традиционные дипломатические каналы. Интерактивный диалог с привлечением международных экспертных сообществ, публичных форумов и платформ для обмена опытом станет неотъемлемой частью процесса. Такой формат позволит учитывать мнения всех заинтересованных сторон, включая частный сектор и профессиональные ассоциации, которые обладают уникальными знаниями о тенденциях в мире информационных технологий. Хотя это усложнит и затянет процесс принятия решений, только открытость и многосторонний подход способны обеспечить достаточный уровень легитимности и поддержки новых правил [Алиев, Борбат, 2020]. Сегодня уже очевидно, что силовое давление или односторонние требования не сработают в цифровой сфере, где все страны взаимосвязаны и любая попытка «автаркии в интернете» обречена на провал.

Многие инициативы предлагают расширить компетенции существующих международных организаций, таких как Интерпол, предоставив им более широкий мандат на координацию глобального взаимодействия при расследовании дел о киберпреступлениях. Другие эксперты считают, что следует создавать специализированные структуры со своими полномочиями и сетями взаимодействия. Но формат, при котором несколько организаций с пересекающимися сферами деятельности пытаются выработать общую повестку, тоже не всегда эффективен. Существует риск дублирования функций, конкуренции за ресурсы и политического влияния, что не ведет к реальной консолидации усилий [Горелик, 2021]. Поэтому многие аналитики указывают, что выработка единых правил возможно лишь при четкой институциональной архитектуре, которая должна учитывать опыт как глобального сотрудничества, так и региональных объединений.

Отдельно стоит упомянуть развитие научных исследований, посвященных проблемам социологических и психологических аспектов киберпреступности. Понимание мотивации злоумышленников, социальных факторов, способствующих вовлечению в преступную деятельность, и возможных путей ресоциализации является важным компонентом комплексного подхода. Международно-правовые механизмы не могут ограничиваться одними лишь карательными мерами, поскольку превенция и просвещение общества в области цифровой гигиены дают неизмеримо больший долгосрочный эффект [Ивлюшкин, 2023]. Усиление

ответственности интернет-компаний и провайдеров за пропаганду безопасного поведения в сети, а также сотрудничество с образовательными учреждениями поможет снизить риски вовлечения молодежи в онлайн-преступность.

Заключение

Таким образом, противодействие транснациональной киберпреступности — это многогранная задача, для решения которой необходимо взаимодействие на разных уровнях: от локального правоохранительного и законодательного до международного дипломатического. Сложность цифрового пространства, скорость технологических изменений и разный уровень экономического развития государств делают процесс унификации правовых норм чрезвычайно трудоемким [Карпович, Ногмова, 2022]. Более того, наличие специфических политических интересов и идеологических разногласий способно затормозить любой многосторонний диалог. Однако, несмотря на все противоречия, международное сообщество постепенно движется к осознанию безальтернативности сотрудничества. Расширение договорной базы, создание новых форматов экспертизы и обмена информацией, укрепление региональных институтов — все это в совокупности формирует предпосылки для появления более согласованного и эффективного механизма борьбы с киберпреступностью на глобальном уровне.

Дальнейшее развитие международно-правовых механизмов будет зависеть от того, насколько государства сумеют преодолеть барьеры недоверия и разделить общую ответственность за состояние цифровой среды. Речь идет не только о криминальном преследовании, но и о создании открытосетевых инфраструктур, где каждая сторона занята поиском совместных решений [Урусова, 2024]. Достичь же полной гармонизации в обозримом будущем вряд ли удастся, однако последовательное внедрение согласованных правил и обмен практическим опытом уже сейчас существенно снижает риски, связанные с киберпреступностью. В итоге можем заключить, что формирование единых правовых стандартов — длительный процесс, который постепенно набирает обороты, опираясь на растущую потребность в глобальном партнерстве и осмысление того, что трансграничные угрозы невозможно эффективно сдерживать в одностороннем порядке.

Библиография

1. Горелик И. Б. Формирование международно-правовой системы противодействия киберпреступности: от терминологии до проекта универсальной конвенции // Международное право. 2022. № 4. С. 60-71.
2. Горелик И. Б. Международно-правовое противодействие киберпреступности: процесс формирования и проблемы управления // Вестник Дипломатической академии МИД России. Международное право. 2021. № 1 (12). С. 87-104.
3. Урусова Л. Х. Противодействие использованию информационно-коммуникационных технологий в преступных целях // Право и управление. 2024. № 7. С. 325-329.
4. Карпович О. Г., Ногмова А. Ш. Международно-правовые проблемы противодействия киберпреступности // Международное публичное и частное право. 2022. № 1. С. 21-26.
5. Шестак В. А., Адигамов А. И. Современные походы в законодательстве стран-членов ЕС к уголовной ответственности за преступления в киберпространстве // Образование и право. 2020. № 8. С. 277-282.
6. Костенко М. А., Аксенова Е. А. Глобальное и национальное регулирование киберпреступлений и кибертерроризма как угроз международной безопасности // Управление в экономических и социальных системах. 2020. № 3 (5). С. 27-34.
7. Алиев Н. Т. О., Борбат А. В. Транснациональная организованная преступная деятельность в эпоху глобализации // Всероссийский криминологический журнал. 2020. Т. 14. № 3. С. 431-440.
8. Перебейносов М. С. Борьба с киберпреступностью как новым проявлением транснациональной организованной преступности // Дневник науки. 2020. № 6 (42). С. 55.

9. Запорожец С. А., Крайнова Н. А. К вопросу о противодействии киберпреступности в условиях новой геополитической реальности // Ученые записки Крымского федерального университета имени В. И. Вернадского. Юридические науки. 2023. Т. 9 (75). № 3. С. 448-456.
10. Kambarov A. K., Baigundinov E. N. International cooperation in combating criminal offences in the field of informatization and communications // Вестник Академии правоохранительных органов при Генеральной прокуратуре Республики Казахстан. 2023. № 2 (28). С. 74-80.
11. Горелик И. Б. Возможные направления развития международно-правовых институтов в области обеспечения глобальной кибербезопасности // Международное право. 2023. № 2. С. 33-44.
12. Ивлюшкин А. С. Применимость норм международного публичного права к обеспечению безопасности в киберпространстве: позиция НАТО // Международное сотрудничество евразийских государств: политика, экономика, право. 2023. № 4. С. 32-39.
13. Лепешкина О. И. Международное сотрудничество государств СНГ по противодействию киберпреступности // Евразийская интеграция: экономика, право, политика. 2023. Т. 17. № 4 (46). С. 82-91.
14. Тетюхин В. В. Оценка эффективности мер Российской Федерации по нейтрализации угроз транснациональной преступности // Социально-гуманитарные знания. 2023. № 3. С. 152-156.
15. Давлатзода К. Д. Аҳаммияти санадҳои байналмилалӣ дар муқовимат бо киберҷиноятҳо // Паёми Донишгоҳи миллии Тоҷикистон. Бахши илмҳои ичтимоӣ-иқтисодӣ ва ҷамъиятӣ. 2023. № 2. С. 221-229. [Давлатзода К.Д. Значение международных документов в борьбе с киберпреступностью // Вестник Таджикского национального университета. Кафедра социально-экономических и общественных наук. 2023. № 2. С. 221-229.]

International Legal Mechanisms for Combating Transnational Cybercrime: Challenges of Harmonization and Implementation into National Legal Systems

Irina Yu. Lazarenkova

PhD in Law,
Prosecutor General's Office University of the Russian Federation,
123022, 15, 2-ya Zvenigorodskaya str., Moscow, Russian Federation;
e-mail: lazarenkova99@list.ru

Abstract

The article provides a comprehensive analysis of contemporary international legal mechanisms for combating transnational cybercrime. The author examines key challenges hindering effective harmonization of approaches to regulating digital offenses at the global level, with particular focus on a critical analysis of the Budapest Convention as the primary instrument of international cooperation. The study identifies political and legal barriers to its implementation, including issues of state sovereignty and differences in legal cultures. The methodological framework combines comparative legal analysis of international treaties, national legislation of various states, and law enforcement practices. The author systematizes core problems in legal regulation: lack of a unified definition of "cybercrime," difficulties in cross-border collection and exchange of electronic evidence, and contradictions regarding extraterritorial jurisdiction. The research emphasizes that implementing international norms into national legal systems is complicated by legislative conflicts, differences between legal traditions (civil law vs. common law), and uneven distribution of technical resources. The study concludes that despite recognizing the need for a global response to cyber threats, harmonization progresses slowly due to geopolitical disagreements and divergent approaches to security and human rights protection.

For citation

Lazarenkova I.Yu. (2025) Mezhdunarodno-pravovye mekhanizmy protivodeystviya transnatsionalnoy kiberprestupnosti: vyzovy unifikatsii i problemy implementatsii v natsionalnye pravovye sistemy [International Legal Mechanisms for Combating Transnational Cybercrime: Challenges of Harmonization and Implementation into National Legal Systems]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 15 (2A), pp. 69-83.

Keywords

Cybercrime, Budapest Convention, international law, transnational crimes, legal harmonization, digital security, cross-border evidence, cybersecurity, international cooperation

References

1. Gorelik I.B. (2022) "Formirovanie mezhdunarodno-pravovoy sistemy protivodeystviya kiberprestupnosti: ot terminologii do proekta universalnoy konventsii" [Formation of the international legal system for combating cybercrime: from terminology to the draft universal convention]. Mezhdunarodnoe pravo [International Law], no. 4, pp. 60-71.
2. Gorelik I.B. (2021) "Mezhdunarodno-pravovoe protivodeystvie kiberprestupnosti: protsess formirovaniya i problemy upravleniya" [International legal counteraction to cybercrime: formation process and management problems]. Vestnik Diplomaticheskoy akademii MID Rossii. Mezhdunarodnoe pravo [Bulletin of the Diplomatic Academy of the Russian Foreign Ministry. International Law], no. 1(12), pp. 87-104.
3. Urusova L.Kh. (2024) "Protivodeystvie ispolzovaniyu informatsionno-kommunikatsionnykh tekhnologiy v prestupnykh tselyakh" [Countering the use of information and communication technologies for criminal purposes]. Pravo i upravlenie [Law and Governance], no. 7, pp. 325-329.
4. Karpovich O.G., Nogmova A.Sh. (2022) "Mezhdunarodno-pravovye problemy protivodeystviya kiberprestupnosti" [International legal problems of combating cybercrime]. Mezhdunarodnoe publichnoe i chastnoe pravo [International Public and Private Law], no. 1, pp. 21-26.
5. Shestak V.A., Adigamov A.I. (2020) "Sovremennye podkhody v zakonodatelstve stran-chlenov ES k ugolovnoy otvetstvennosti za prestupleniya v kiberprostranstve" [Modern approaches in the legislation of EU member states to criminal liability for crimes in cyberspace]. Obrazovanie i pravo [Education and Law], no. 8, pp. 277-282.
6. Kostenko M.A., Aksenova E.A. (2020) "Globalnoe i natsionalnoe regulirovanie kiberprestupleniy i kiberterrorizma kak ugroz mezhdunarodnoy bezopasnosti" [Global and national regulation of cybercrimes and cyberterrorism as threats to international security]. Upravlenie v ekonomicheskikh i sotsialnykh sistemakh [Management in Economic and Social Systems], no. 3(5), pp. 27-34.
7. Aliev N.T.O., Borbat A.V. (2020) "Transnatsionalnaya organizovannaya prestupnaya deyatelnost v epokhu globalizatsii" [Transnational organized criminal activity in the era of globalization]. Vserossiyskiy kriminologicheskiy zhurnal [All-Russian Criminological Journal], vol. 14, no. 3, pp. 431-440.
8. Perebeinosov M.S. (2020) "Borba s kiberprestupnostyu kak novym proyavleniem transnatsionalnoy organizovannoy prestupnosti" [Combating cybercrime as a new manifestation of transnational organized crime]. Dnevnik nauki [Science Diary], no. 6(42), p. 55.
9. Zaporozhets S.A., Krainova N.A. (2023) "K voprosu o protivodeystvii kiberprestupnosti v usloviyakh novoy geopoliticheskoy realnosti" [On the issue of countering cybercrime in the context of the new geopolitical reality]. Uchenye zapiski Krymskogo federalnogo universiteta imeni V.I. Vernadskogo. Yuridicheskie nauki [Scientific Notes of V.I. Vernadsky Crimean Federal University. Legal Sciences], vol. 9(75), no. 3, pp. 448-456.
10. Kambarov A.K., Baigundinov E.N. (2023) "International cooperation in combating criminal offences in the field of informatization and communications". Vestnik Akademii pravookhranitelnykh organov pri Generalnoy prokurature Respubliki Kazakhstan [Bulletin of the Academy of Law Enforcement Agencies under the Prosecutor General's Office of the Republic of Kazakhstan], no. 2(28), pp. 74-80.
11. Gorelik I.B. (2023) "Vozmozhnye napravleniya razvitiya mezhdunarodno-pravovykh institutov v oblasti obespecheniya globalnoy kiberbezopasnosti" [Possible directions for the development of international legal institutions in the field of global cybersecurity]. Mezhdunarodnoe pravo [International Law], no. 2, pp. 33-44.
12. Ivlyushkin A.S. (2023) "Primenimost norm mezhdunarodnogo publichnogo prava k obespecheniyu bezopasnosti v kiberprostranstve: pozitsiya NATO" [Applicability of international public law norms to ensuring security in cyberspace: NATO's position]. Mezhdunarodnoe sotrudnichestvo evraziyskikh gosudarstv: politika, ekonomika, pravo [International Cooperation of Eurasian States: Politics, Economics, Law], no. 4, pp. 32-39.

13. Lepeshkina O.I. (2023) "Mezhdunarodnoe sotrudnichestvo gosudarstv SNG po protivodeystviyu kiberprestupnosti" [International cooperation of CIS states in combating cybercrime]. Evraziyskaya integratsiya: ekonomika, pravo, politika [Eurasian Integration: Economics, Law, Politics], vol. 17, no. 4(46), pp. 82-91.
14. Tetyukhin V.V. (2023) "Otsenka effektivnosti mer Rossiyskoy Federatsii po neytralizatsii ugroz transnatsionalnoy prestupnosti" [Assessment of the effectiveness of measures of the Russian Federation to neutralize threats of transnational crime]. Sotsialno-gumanitarnye znaniya [Social and Humanitarian Knowledge], no. 3, pp. 152-156.
15. Davlatzoda K.D. (2023) "Аҳаммияти санадҳои байналмилалӣ дар муқовимат бо киберҷиноятҳо" [The importance of international documents in combating cybercrime]. Payomi Donishgohi millii Tojikiston. Bakhshi ilmhoi ijtimoī-iqtisodī va jam'iyatī [Bulletin of the Tajik National University. Department of Socio-Economic and Social Sciences], no. 2, pp. 221-229. [In Tajik with parallel Russian title: "Znachenie mezhdunarodnykh dokumentov v borbe s kiberprestupnostyu" [The importance of international documents in combating cybercrime]. Vestnik Tadzhikskogo natsionalnogo universiteta. Kafedra sotsialno-ekonomicheskikh i obshchestvennykh nauk [Bulletin of the Tajik National University. Department of Socio-Economic and Social Sciences], no. 2, pp. 221-229.]