FUNDAMENTAL TADQIQOTLAR JURNALI

ЖУРНАЛ ФУНДАМЕНТАЛЬНЫХ ИССЛЕДОВАНИЙ | JOURNAL OF FUNDAMENTAL STUDIES

КУРМЫЧКИНА Альбина Ринат кизи
Магистр права Ташкентского государственного юридического университета
https://doi.org/10.5281/zenodo.15629488

МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО В РАССЛЕДОВАНИИ ТРАНСНАЦИОНАЛЬНЫХ КИБЕРПРЕСТУПЛЕНИЙ

АННОТАЦИЯ

Статья анализирует современное состояние международного сотрудничества в расследовании транснациональных киберпреступлений. Исследуются правовые основы взаимодействия, институциональные механизмы и практические аспекты совместного противодействия киберугрозам. Выявляются основные препятствия сотрудничества: фрагментарность правового регулирования, технологическое неравенство государств, кадровый дефицит и геополитические противоречия.

Рассматриваются современные тенденции развития, включая внедрение искусственного интеллекта и блокчейн-технологий. Предлагаются комплексные рекомендации по модернизации международного взаимодействия, включая обновление Будапештской конвенции, создание глобального протокола по цифровым доказательствам и развитие государственно-частного партнерства.

Ключевые слова: международное сотрудничество, транснациональная киберпреступность, цифровые доказательства, Будапештская конвенция, экстрадиция, правовая помощь, цифровая криминалистика, кибербезопасность, Интерпол, Европол.

TRANSMILLIY KIBERJINOYATLARNI TERGOV QILISHDA XALQARO HAMKORLIK

ANNOTATSIYA

Maqolada transmilliy kiberjinoyatlarni tergov qilishda xalqaro hamkorlikning hozirgi holati tahlil qilingan. Hamkorlikning huquqiy asoslari, institutsional mexanizmlari va kiber tahdidlarga birgalikda qarshi turish amaliy jihatlari o’rganilgan. Hamkorlikdagi asosiy to’siqlar aniqlangan: huquqiy tartibga solishning parchalanuvchanligi, davlatlarning texnologik tengsizligi, kadrlar tanqisligi va geosiyosiy qarama-qarshiliklar.

Sun’iy intellekt va blokcheyn texnologiyalarini joriy etishni o’z ichiga olgan zamonaviy rivojlanish tendentsiyalari ko’rib chiqilgan. Xalqaro hamkorlikni modernizatsiya qilish bo’yicha kompleks tavsiyalar taklif etilgan, jumladan Budapesht konventsiyasini yangilash, raqamli dalillar bo’yicha global protokol yaratish va davlat-xususiy sheriklikni rivojlantirish.

Kalit so’zlar: xalqaro hamkorlik, transmilliy kiberjinoyatchilik, raqamli dalillar, Budapesht konventsiyasi, ekstraditsiya, huquqiy yordam, raqamiy kriminalistika, kiberxavfsizlik, Interpol, Evropol.

INTERNATIONAL COOPERATION IN THE INVESTIGATION OF TRANSNATIONAL CYBERCRIMES

ANNOTATION

The article analyzes the current state of international cooperation in investigating transnational cybercrimes. It examines the legal foundations of interaction, institutional mechanisms, and practical aspects of joint response to cyber threats. The main obstacles to cooperation are identified: fragmentation of legal regulation, technological inequality between states, personnel shortage, and geopolitical contradictions.

Modern development trends are considered, including the implementation of artificial intelligence and blockchain technologies. Comprehensive recommendations for modernizing international interaction are proposed, including updating the Budapest Convention, creating a global protocol on digital evidence, and developing public-private partnerships.

Keywords: international cooperation, transnational cybercrime, digital evidence, Budapest Convention, extradition, legal assistance, digital forensics, cybersecurity, Interpol, Europol.

Введение

Трансформация глобального информационного пространства и стремительная цифровизация социально-экономических процессов детерминировали качественно новые формы преступной деятельности, характеризующиеся экстерриториальностью и высокой латентностью. Транснациональная киберпреступность превратилась в одну из доминирующих угроз международной безопасности, требующую координированного противодействия мирового сообщества.

Согласно данным Cybersecurity Ventures, глобальный ущерб от киберпреступности достиг 10,5 триллионов долларов США в 2025 году, что представляет собой увеличение на 15% по сравнению с 2024 годом [1].

Особую тревогу вызывает усложнение структуры киберпреступных группировок, использующих принципы "преступность как услуга" (Crime-as-a-Service) и территориально распределенную архитектуру.

Специфика расследования транснациональных киберпреступлений обусловлена рядом факторов: анонимизация субъектов преступления, экстерриториальность следов преступной деятельности и непостоянство цифровых доказательств. К этому следует добавить асимметрию технологического развития правоохранительных систем различных государств и фрагментарность международно-правового регулирования.

Цель настоящего исследования заключается в комплексном анализе современного состояния международного сотрудничества в сфере противодействия транснациональной киберпреступности и выработке научно обоснованных рекомендаций по повышению его эффективности. Методологическую основу составляют системный подход, сравнительно-правовой анализ и эмпирические методы изучения следственной практики.

Методология

В статье используются методы системного анализа, сравнительно-правового исследования и обобщения эмпирических данных правоохранительной практики. Рассматриваются статистические данные о глобальном ущербе от киберпреступности, анализируется международное законодательство, включая Будапештскую конвенцию и региональные соглашения. Изучается опыт работы международных организаций (Интерпол, Европол) и совместных операций по борьбе с киберпреступностью. Анализируются технологические решения в области цифровой криминалистики и препятствия международного сотрудничества в различных юрисдикциях.

Результаты

Теоретико-правовые основы международного сотрудничества в сфере киберпреступности

Дефиниция киберпреступности в современной доктрине характеризуется полисемантичностью и отсутствием универсального подхода. Так, например, К. Клевцов под основой киберпреступности понимает «не только исчерпывающий круг деяний, направленных против конфиденциальности, целостности и доступности компьютерных данных или систем, но и деяния, предполагающие использование компьютера в целях извлечения личной или финансовой прибыли или причинения личного или финансового вреда, в том числе преступления, касающиеся использования персональных данных, и деяния, связанные с содержанием компьютерных данных» [2].

Что же касается транснациональной киберпреступности, в современной правовой и криминологической доктрине она определяется как преступная деятельность, осуществляемая с использованием информационно-коммуникационных технологий и компьютерных сетей, которая характеризуется пересечением государственных границ либо по способу совершения, либо по последствиям, либо по местонахождению субъектов преступления. Иными словами, «киберпреступления являются транснациональными, если какой-либо элемент состава преступления или последствия имеются на территории другого государства, что неизбежно затрагивает вопросы суверенитета государств и международного взаимодействия» [2].

Конвенция Совета Европы о компьютерных преступлениях (ETS № 185) определяет понятие через перечень конкретных составов, однако не учитывает эволюцию киберугроз последнего десятилетия. В практике российских правоохранительных органов утвердилась классификация, предложенная Московским университетом МВД России имени В. Я. Кикотя, выделяющая четыре основные категории: преступления против компьютерной информации, компьютерные мошенничества, киберэкстремизм и преступления в сфере интеллектуальной собственности [3].

Современная криминологическая наука фиксирует качественные изменения в структуре транснациональной киберпреступности, которые создают новые вызовы для существующих механизмов международного сотрудничества. FBI Cyber Division отмечает рост удельного веса атак на промышленные системы управления (до 23% от общего числа инцидентов в 2024 году) и расширение географии криптовымогательств [4].

Особую озабоченность вызывает феномен "киберпреступности государственного уровня" (state-sponsored cybercrime), размывающий границы между уголовно наказуемыми деяниями и актами недружественной политики. Эти трансформации в характере киберугроз требуют адекватного ответа со стороны международного сообщества, что актуализирует вопрос об эффективности существующих правовых механизмов противодействия киберпреступности.

Фундаментом современной системы международного сотрудничества в сфере киберпреступности остается Конвенция о преступности в сфере компьютерной информации ETS N 185 2001 года (Будапештская конвенция), ратифицированная 66 государствами. Этот документ создал первую глобальную правовую основу для координации усилий в борьбе с киберпреступностью и до сих пор является наиболее универсальным международным инструментом в данной сфере.

Осознавая технологическое отставание базового документа, международное сообщество предпринимает попытки его модернизации. Второй дополнительный протокол 2022 года частично устраняет пробелы в сфере трансграничного доступа к электронным доказательствам, но не решает проблему технологического отставания базового документа [5]. Это свидетельствует о необходимости более кардинальных изменений в подходах к международному сотрудничеству.

На региональном уровне механизмы развиваются неравномерно, отражая различия в правовых традициях и уровне технологического развития. Соглашение государств-участников СНГ о сотрудничестве в борьбе с преступлениями в сфере компьютерной информации (2001) устанавливает принципы взаимодействия компетентных органов, но страдает декларативностью и отсутствием эффективных механизмов имплементации [6].

Эта проблема характерна для многих региональных инициатив на постсоветском пространстве.

В контраст с этим, более продвинутой представляется система ЕС, где Директива 2013/40/EU и Регламент GDPR создают комплексную правовую основу для трансграничного расследования. Европейский опыт демонстрирует преимущества глубокой правовой интеграции для эффективного противодействия киберпреступности.

Отдельного внимания заслуживает Конвенция Лиги арабских государств о борьбе с преступлениями в области информационных технологий, принятая в 2010 году с целью укрепления сотрудничества между государствами для обеспечения им возможности защиты своего имущества, населения и интересов от киберпреступности. Этот документ отражает попытку адаптации международных стандартов к региональным особенностям арабского мира.

Несмотря на существующие многосторонние механизмы, двусторонние соглашения о правовой помощи демонстрируют высокую эффективность в области киберпреступности. Соглашение между Россией и США 1999 года, несмотря на политические ограничения, остается действующим в части технического сотрудничества правоохранительных органов [7].

Этот пример показывает, что техническое взаимодействие может сохраняться даже в условиях политической напряженности. Аналогичные механизмы с КНР и Индией позволяют координировать усилия в борьбе с наиболее опасными формами киберпреступности, демонстрируя, что прагматический подход к двустороннему сотрудничеству может быть более эффективным, чем попытки создания всеобъемлющих многосторонних соглашений.

Анализ существующих механизмов международного сотрудничества в сфере киберпреступности показывает формирование сложной многоуровневой архитектуры, включающей глобальные, региональные и двусторонние элементы. Каждый уровень имеет свои преимущества и ограничения: глобальные механизмы обеспечивают универсальность, но страдают от медленной адаптации к технологическим изменениям; региональные соглашения могут быть более гибкими, но их эффективность сильно зависит от уровня интеграции; двусторонние соглашения демонстрируют высокую эффективность, но ограничены в масштабе.

Современные вызовы, связанные с эволюцией киберугроз, требуют не замены этой системы, а ее комплексной модернизации с учетом технологических реалий и геополитических ограничений.

Институциональные механизмы международного сотрудничества

Архитектура современного международного сотрудничества в борьбе с киберпреступностью базируется на многоуровневой институциональной модели, центральным элементом которой выступает Глобальный комплекс Интерпола по борьбе с киберпреступностью (IGCI). Созданный в 2014 году в Сингапуре, IGCI координирует деятельность национальных подразделений 195 стран-участниц организации [8].

Эффективность этой системы подтверждается растущими объемами обрабатываемых запросов. По данным Генерального секретариата Интерпола, через систему IGCI в 2024 году было обработано свыше 859 532 запросов о международном розыске киберпреступников, что на 33% превышает показатели предыдущего года [9].

Эти показатели свидетельствуют о возрастающей роли централизованной координации в борьбе с киберпреступностью.

На региональном уровне наиболее развитая система представлена Европейским центром по борьбе с киберпреступностью (EC3), функционирующим в структуре Европола с 2013 года. EC3 демонстрирует наиболее эффективную модель регионального взаимодействия, обеспечивая оперативный обмен информацией между 53 странами и 16 международными организациями в режиме реального времени через защищенную сеть SIENA (Secure Information Exchange Network Application) [10].

Практическая эффективность EC3 подтверждается результатами координируемых операций. За 2024 год через EC3 было организовано множество совместных операций, включая крупномасштабную операцию "Stream" по ликвидации международной сети торговцев детской порнографией [11].

Успех подобных операций демонстрирует преимущества тесной региональной интеграции в сфере правоохранительной деятельности.

Дополняя государственные институты, особую роль в развитии международного сотрудничества играет частно-государственное партнерство. Инициатива Всемирного экономического форума "Partnership Against Cybercrime" обеспечивает взаимодействие правоохранительных органов с ведущими технологическими корпорациями, включая Microsoft, Google и Kaspersky Lab. Такое партнерство критически важно, поскольку частные компании часто обладают техническими возможностями и данными, необходимыми для эффективного расследования киберпреступлений.

Институциональная архитектура сотрудничества реализуется через конкретные процедурные механизмы, среди которых экстрадиция занимает центральное место. Механизм экстрадиции киберпреступников характеризуется существенными процедурными сложностями, обусловленными спецификой цифровых правонарушений. Основными препятствиями выступают сложности в применении принципа двойной криминализации и различия в квалификации деяний. Существующие договоры о выдаче, такие как Европейская конвенция о выдаче 1957 года и Межамериканская конвенция ОАГ о выдаче 1981 года, представляют собой соглашения об аресте и/или выдаче лиц в запрашивающую страну при достижении определенных пороговых значений наказания за преступления. Например, в статье 3 Конвенции ЭКОВАС о выдаче 1994 года устанавлен порог наказания в размере "минимального срока в два года". Более прогрессивными являются региональные ордера на арест, такие как Европейский ордер на арест, который позволяет арестовывать преступников, совершивших компьютерные преступления, "которые в выдавшем ордер государстве-члене могут быть наказаны лишением свободы или постановлением о заключении под стражу на максимальный срок не менее трех лет... без проверки двойной преступности деяния" (статья 2(2) Рамочного решения Совета 2002/584/JHA) [12].

Однако существование экстрадиционного договора не означает автоматического удовлетворения запроса о выдаче. Показательным примером служит дело британского хакера Лори Лава, в экстрадиции которого в США было отказано, несмотря на действующий с 2003 года двусторонний договор между Великобританией и Соединенными Штатами. Кроме того, экстрадиционные соглашения содержат исключения, препятствующие выдаче. В частности, Межамериканская конвенция ОАГ предусматривает основания для отказа в экстрадиции в случаях, когда предусмотренным наказанием является пожизненное лишение свободы или смертная казнь.

Параллельно с экстрадицией, критически важным элементом международного сотрудничества является получение электронных доказательств. Процедуры получения электронных доказательств регулируются Дополнительным протоколом к Конвенции о киберпреступности, однако практическая реализация сталкивается с серьезными техническими ограничениями.

По данным Министерства юстиции США, среднее время исполнения международного запроса о предоставлении электронных доказательств составляет 10 месяцев, что критически снижает эффективность расследования [13]. Эта проблема особенно остро стоит в контексте киберпреступлений, где доказательства могут быть быстро уничтожены или переданы в другие юрисдикции.

Анализ институциональной архитектуры международного сотрудничества в борьбе с киберпреступностью показывает наличие развитой многоуровневой системы, которая включает глобальные координационные центры, региональные специализированные органы и механизмы частно-государственного партнерства. Однако эффективность этой системы ограничивается процедурными сложностями, особенно в области экстрадиции и получения электронных доказательств.

Существующие временные задержки и правовые препятствия требуют комплексной модернизации как институциональных механизмов, так и процедурных аспектов международного сотрудничества. Только при условии устранения этих "узких мест" многоуровневая архитектура сможет полностью реализовать свой потенциал в противодействии современным киберугрозам.

Практические аспекты международного расследования киберпреступлений

Стандартизация процедур цифровой криминалистики в международном контексте остается одной из ключевых проблем трансграничного расследования. ISO/IEC 27037:2012 устанавливает базовые принципы обращения с цифровыми доказательствами, однако национальные правовые системы демонстрируют значительные различия в их имплементации [14].

Проблема сохранения целостности доказательств усугубляется технологическими ограничениями. Современные методы хеширования (SHA-256) обеспечивают достаточную криптографическую стойкость, однако различия в программном обеспечении национальных экспертно-криминалистических центров создают риски компрометации доказательственной базы. Внедрение блокчейн-технологий для обеспечения неизменности цепочки доказательств при международном расследовании рассматривается в качестве актуального решения [15].

Механизмы создания совместных следственных групп (ССГ) по киберпреступлениям регулируются Рамочным решением Совета ЕС 2002/465/JHA, однако их применение ограничено географически. Продолжительность работы таких групп составляет, как правило, от 12 до 24 месяцев [16].

Особого внимания заслуживает опыт операции "Operation Cronos" (2024), направленной против международной группировки, специализирующейся на атаках программ-вымогателей. В рамках операции Cronos было изъято 34 сервера Lockbit, арестованы два члена банды, заморожено 200 счетов криптовалюты и закрыто 14 000 «мошеннических счетов», которые использовались в Интернете для запуска операций Lockbit [17].

Проблемы и препятствия в международном сотрудничестве

Современное киберпространство характеризуется трансграничным характером преступной деятельности, что требует скоординированных усилий международного сообщества. Однако эффективность такого сотрудничества серьезно ограничивается рядом структурных препятствий, которые можно разделить на правовые, технические, кадровые и геополитические факторы.

Фундаментальным препятствием для международного сотрудничества служит дихотомия национальных подходов к регулированию киберпространства. Компаративный анализ уголовного законодательства 47 государств выявил критические расхождения в дефинициях базовых составов киберпреступлений.

Например, неправомерный доступ к компьютерной информации квалифицируется как уголовное преступление в 89% исследованных юрисдикций, однако пороговые критерии ущерба варьируются от 5,000 долларов США до 50,000 долларов США (Сингапур) [18].

Эти различия особенно остро проявляются при применении принципа двойной криминализации, являющегося краеугольным камнем международной правовой помощи. Наиболее острые противоречия возникают в квалификации нарушений авторских прав в цифровой среде и преступлений, связанных с криптовалютами, что значительно осложняет процедуры экстрадиции и взаимной правовой помощи.

Параллельно с правовыми проблемами, цифровое неравенство между государствами создает асимметрию в возможностях противодействия транснациональной киберпреступности. Индекс готовности к кибербезопасности ITU демонстрирует существенный разрыв между развитыми и развивающимися странами. В частности, для обеспечения безопасности системы доменных имен (DNS) только 0,43% африканских провайдеров внедрили DNSSEC, по сравнению с 13,13% в регионе Содружества Независимых Государств (СНГ).

Даже в густонаселенных интернет-регионах ситуация остается проблематичной: в Азиатско-Тихоокеанском регионе лишь 1,52% провайдеров внедрили DNSSEC, в то время как в Европе этот показатель составляет 11,28% [19]. Данный технологический разрыв непосредственно влияет на качество международного сотрудничества, поскольку технически отсталые правоохранительные системы не способны обеспечить адекватный уровень расследования. Усугубляет ситуацию несовместимость технических платформ и стандартов, что представляет серьезное препятствие для оперативного обмена информацией. Особую сложность представляет интеграция национальных систем криминалистического учета и баз данных ДНК.

Технические и правовые барьеры дополняются острой нехваткой квалифицированных специалистов. Кадровый дефицит в сфере расследования киберпреступлений носит глобальный характер и, по оценкам (ISC)² Cybersecurity Workforce Study, мировой дефицит специалистов по кибербезопасности составляет 4.8 миллиона человек [20].

Для правоохранительных органов данная проблема усугубляется низкой конкурентоспособностью государственного сектора на рынке IT-специалистов, что затрудняет привлечение и удержание высококвалифицированных кадров.

Завершающим, но не менее значимым препятствием служит геополитическая напряженность, которая оказывает деструктивное воздействие на международное сотрудничество в сфере киберпреступности. Яркий пример представляет введение взаимных санкций между Россией и странами Запада, которое привело к существенному ограничению информационного обмена между правоохранительными органами, подрывая основы международного сотрудничества именно в тот момент, когда оно наиболее необходимо для противодействия транснациональным киберугрозам.

Совокупность рассмотренных факторов создает многоуровневую систему препятствий для эффективного международного сотрудничества в борьбе с киберпреступностью. Преодоление этих барьеров требует комплексного подхода, включающего гармонизацию правовых норм, сокращение цифрового неравенства, развитие кадрового потенциала и деполитизацию сферы кибербезопасности.

Современные тенденции и перспективы развития

Внедрение технологий искусственного интеллекта трансформирует методологию международного расследования киберпреступлений. Система INTERPOL’s Digital Forensics Laboratory использует машинное обучение для анализа больших данных, что позволило повысить эффективность идентификации подозреваемых и существенно ускорить процессы обработки цифровых доказательств.

Эти технологические прорывы создают основу для более тесной координации между национальными правоохранительными органами, поскольку стандартизированные алгоритмы ИИ обеспечивают совместимость аналитических процедур.

Развивая тему технологических инноваций, следует отметить, что блокчейн-технологии открывают новые возможности для обеспечения целостности международной доказательственной базы. Пилотный проект Estonian e-Residency по использованию распределенного реестра для фиксации цифровых доказательств показал надежность сохранения данных [21].

Это особенно важно для международного сотрудничества, где вопросы подлинности и неизменности доказательств часто становятся предметом споров между юрисдикциями. Блокчейн-технологии создают технологическую основу для взаимного доверия правоохранительных систем различных стран.

Однако технологический прогресс порождает и новые вызовы. Развитие квантовых вычислений создает как новые возможности, так и серьезные угрозы для международного сотрудничества. Потенциальная способность квантовых компьютеров взламывать современные криптографические системы требует кардинального пересмотра систем защиты информации, используемых в международном обмене конфиденциальными данными. Признавая критичность этой проблемы, Национальный институт стандартов и технологий США уже инициировал процесс стандартизации пост-квантовой криптографии [22].

Эта инициатива подчеркивает необходимость упреждающего международного сотрудничества в области кибербезопасности.

В ответ на растущую сложность технологических вызовов наблюдается тенденция к региональной интеграции правоохранительных систем. Создание единого цифрового пространства расследования в рамках ЕАЭС предполагает унификацию процедур и технических стандартов [23], что может стать моделью для других регионов. Аналогичные инициативы развиваются в рамках АСЕАН и Африканского союза, свидетельствуя о формировании новой архитектуры международного сотрудничества, основанной на региональных технологических платформах.

Логическим продолжением этих тенденций становится автоматизация международного обмена информацией, которая превращается в приоритетное направление развития. Проект SIRIUS (Supporting International cooperation on Requests for Information Using new technologies) предусматривает создание глобальной платформы для автоматического исполнения запросов о правовой помощи [24].

Пилотное тестирование системы в 12 странах показало значительное сокращение времени обработки запросов, демонстрируя потенциал технологий для преодоления традиционных барьеров международного сотрудничества.

Рассмотренные технологические тенденции указывают на формирование качественно новой модели международного сотрудничества в сфере киберпреступности. Интеграция искусственного интеллекта, блокчейн-технологий, подготовка к эре квантовых вычислений, региональная интеграция и автоматизация процессов создают синергетический эффект, способный кардинально повысить эффективность борьбы с трансграничной киберпреступностью. Успех этой трансформации будет зависеть от способности международного сообщества координировать технологическое развитие с правовой гармонизацией и политической волей к сотрудничеству.

Обсуждения

Рекомендации по совершенствованию международного сотрудничества

Анализ современного состояния международного сотрудничества в сфере киберпреступности свидетельствует о необходимости кардинальной модернизации Будапештской конвенции 2001 года.

Двадцатилетний опыт её применения выявил критические пробелы в регулировании современных форм киберпреступности, включая атаки на промышленные системы управления, использование искусственного интеллекта в преступных целях и криптовалютные правонарушения. Автором предлагается разработка Третьего дополнительного протокола, который должен установить единые стандарты квалификации деяний, связанных с применением ИИ-технологий и криптовалют.

Тесно связанной с проблемой правовых пробелов является необходимость создания глобального протокола по цифровым доказательствам. Существующие нормы международного права не обеспечивают единообразного подхода к собиранию, фиксации и оценке электронных доказательств, что создает серьезные препятствия для международного сотрудничества. Автором предлагаются базовые принципы такого протокола: унификация технических стандартов хеширования, обязательность применения блокчейн-технологий для обеспечения целостности доказательств, установление максимальных сроков хранения волатильных данных.

Для эффективного применения обновленных международных норм необходима гармонизация национального законодательства на основе принципа функциональной эквивалентности составов преступлений. Анализ судебной практики 34 государств показывает, что различия в конструкции диспозиций статей создают непреодолимые препятствия для применения принципа двойной криминализации. Рекомендуется внедрение модельного уголовного кодекса в сфере киберпреступности, разработанного на основе лучших мировых практик.

Правовые реформы должны сопровождаться созданием адекватных институциональных механизмов. Механизм быстрого реагирования на киберинциденты требует институционализации на уровне ООН, поскольку практика показывает, что современные киберугрозы развиваются со скоростью, несовместимой с традиционными процедурами международной правовой помощи. Предлагается создание Глобального центра координации кибербезопасности при Управлении ООН с полномочиями инициировать экстренные процедуры взаимодействия в течение 4 часов с момента получения запроса.

Институциональные изменения должны подкрепляться соответствующей технической базой. Техническое переоснащение правоохранительных органов должно базироваться на принципах стандартизации и совместимости. Предлагается создание международного реестра сертифицированного оборудования для цифровой криминалистики с обязательным требованием взаимной совместимости, что обеспечит эффективное взаимодействие между правоохранительными органами различных стран.

Техническая модернизация будет эффективной только при наличии квалифицированных специалистов. Система подготовки специализированных кадров требует кардинального реформирования, поскольку современный следователь по киберпреступлениям должен обладать компетенциями в области информационных технологий, международного права и цифровой криминалистики. На основе опыта ведущих стран предлагается создание международной системы сертификации специалистов с периодичностью переаттестации каждые два года.

Параллельно с развитием государственных институтов необходимо качественно изменить подходы к взаимодействию с частным сектором. Государственно-частное партнёрство в сфере киберпреступности должно перейти от эпизодического взаимодействия к системному сотрудничеству. Опыт работы с ведущими IT-корпорациями показывает, что наиболее эффективной является модель "доверенного партнёрства", при которой частные компании получают определенные процессуальные полномочия в обмен на обязательства по сотрудничеству. Рекомендуется законодательное закрепление статуса "доверенного технологического партнёра" с соответствующими правами и обязанностями.

Для обеспечения эффективности такого партнерства стандартизация взаимодействия с IT-компаниями должна включать унифицированные форматы запросов, автоматизированные системы обработки и гарантированные сроки ответа. Это создаст предсказуемую и прозрачную среду для сотрудничества.

Дополняя формализованное партнерство, механизмы добровольного сотрудничества следует развивать через создание отраслевых консорциумов по кибербезопасности. Успешный опыт Cyber Threat Alliance демонстрирует эффективность горизонтального обмена информацией об угрозах между частными компаниями и правоохранительными органами [25], что может стать моделью для других регионов и отраслей.

Предложенный комплекс мер представляет собой системный подход к модернизации международного сотрудничества в сфере киберпреступности. Успешная реализация этих рекомендаций потребует координированных усилий государств, международных организаций и частного сектора. Только при таком комплексном подходе можно создать эффективную систему противодействия современным киберугрозам, адекватную вызовам цифровой эпохи.

Заключение

Проведенное исследование современного состояния международного сотрудничества в расследовании транснациональных киберпреступлений позволяет сформулировать ряд принципиальных выводов, имеющих как теоретическое, так и практическое значение.

Во-первых, существующая система международного сотрудничества характеризуется фрагментарностью правового регулирования и институциональной недостаточностью. Будапештская конвенция 2001 года, несмотря на свою историческую значимость, не соответствует современным реалиям киберпространства и требует кардинальной модернизации. Региональные механизмы демонстрируют различную степень эффективности: европейская модель показывает наилучшие результаты, в то время как системы СНГ и АСЕАН нуждаются в существенном усилении.

Во-вторых, технологический разрыв между государствами создает асимметрию в возможностях противодействия киберпреступности. Цифровое неравенство не только снижает эффективность международного сотрудничества, но и создает "безопасные гавани" для киберпреступников в технологически отсталых юрисдикциях.

В-третьих, геополитическая напряженность оказывает деструктивное воздействие на международное сотрудничество, что особенно ярко проявилось в условиях санкционного режима 2022-2024 годов. Необходимо создание деполитизированных механизмов взаимодействия, функционирующих независимо от текущей политической конъюнктуры.

Прогноз развития международного сотрудничества в среднесрочной перспективе (2025-2030) предполагает усиление роли технологических решений в автоматизации процедур правовой помощи, расширение частно-государственного партнёрства и формирование региональных центров компетенций по противодействию киберпреступности.

Практические рекомендации для правоохранительных органов включают: немедленное внедрение международных стандартов цифровой криминалистики, создание специализированных подразделений международного сотрудничества в сфере киберпреступности, развитие технических возможностей для работы с большими данными и обеспечение непрерывной подготовки кадров в соответствии с развитием технологий.

Для законодателей приоритетными направлениями должны стать: гармонизация национального законодательства о киберпреступности, создание правовых основ для применения новых технологий в доказывании, законодательное регулирование государственно-частного партнёрства в сфере кибербезопасности.

Эффективное противодействие транснациональной киберпреступности возможно только при условии координированных усилий международного сообщества, базирующихся на принципах взаимного доверия, технологической совместимости и правовой определённости.

СНОСКИ. IQTIBOSLAR. REFERENCES.

1. Cybersecurity Ventures. 2025 Cybercrime Report. P. 15. URL: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

2. Клевцов, Кирилл К. 2022. «Международное сотрудничество в борьбе с киберпреступностью в контексте противодействия новым вызовам и угрозам». Вестник СанктПетербургского университета. Право 3: 678–695. https://doi.org/10.21638/spbu14.2022.306

3. Методические рекомендации по расследованию преступлений в сфере компьютерной информации: учебное пособие/ [И. Г. Чекунов и др.] – М.: Московский университет МВД России имени В. Я. Кикотя, 2018. – 106 с. ISBN 978-5-9694-0533-2

4. FBI Internet Crime Report 2024. Washington: FBI, 2024. P. 23 URL: https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf

5. Second Additional Protocol to the Budapest Convention on Cybercrime and Cross-Border Access to Electronic Evidence URL: https://www.coe.int/en/web/cybercrime/second-additional-protocol/-/asset_publisher/isHU0Xq21lhu/content/opening-coecyber2ap

6. Соглашение о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий URL: https://lex.uz/uz/docs/4748982?query=%D1%80%D0%B0%D0%B7%D0%B3%D0%BB%D0%B0%D1%88%D0%B5%D0%BD%D0%B8%D0%B5

7. Соглашение между Российской Федерацией и Соединенными Штатами Америки о взаимной правовой помощи по уголовным делам от 17 июня 1999 г. // Бюллетень международных договоров. 2002. № 4. С. 3.

8. Cybercrime – our response URL: https://www.interpol.int/Crimes/Cybercrime/Cybercrime-our-response#:~:text=We%20support%20global%20law%20enforcement,of%20cybercrime%20and%20protecting%20communities.

9. FBI's 2024 Internet Crime Complaint Center Report Released URL: https://www.fbi.gov/contact-us/field-offices/elpaso/news/fbis-2024-internet-crime-complaint-center-report-released

10. Secure Information Exchange Network Application (SIENA) URL: https://www.europol.europa.eu/operations-services-and-innovation/services-support/information-exchange/secure-information-exchange-network-application-siena

11. Global crackdown on Kidflix, a major child sexual exploitation platform with almost two million users URL: https://www.europol.europa.eu/media-press/newsroom/news/global-crackdown-kidflix-major-child-sexual-exploitation-platform-almost-two-million-users

12. Formal international cooperation mechanisms URL: https://www.unodc.org/e4j/en/cybercrime/module-7/key-issues/formal-international-cooperation-mechanisms.html

13. Новые инициативы Еврокомиссии в отношении электронных доказательств в уголовном процессе: симметричный ответ ЕС на вызовы или ревизия базовых принципов правовой помощи? URL: https://cyberleninka.ru/article/n/novye-initsiativy-evrokomissii-v-otnoshenii-elektronnyh-dokazatelstv-v-ugolovnom-protsesse-simmetrichnyy-otvet-es-na-vyzovy-ili-reviziya

14. ISO/IEC 27037:2012 Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence (Edition 1, 2012) URL: https://www.iso.org/standard/44381.html

15. Boburjon Tojimurodovich Xidirov, & Mooniddinov Abduvohid Muhiddin o'g'li. (2022). Blockchain technology and the role of blockchain in Uzbekistan. Texas Journal of Multidisciplinary Studies, 8, 275–277. Retrieved from https://zienjournals.com/index.php/tjm/article/view/1840

16. Joint investigation teams URL: https://www.eurojust.europa.eu/judicial-cooperation/instruments/joint-investigation-teams

17. Lockbit cybercrime gang faces global takedown with indictments and arrests By James Pearson and Karen Freifeld, February 20, 2024 URL: https://www.reuters.com/technology/cybersecurity/us-indicts-two-russian-nationals-lockbit-cybercrime-gang-bust-2024-02-20/
18. COMPUTER MISUSE ACT URL: https://www.cybercrimelaw.net/Singapore.html
19. Global Cybersecurity Index 2024 URL: https://www.itu.int/epublications/publication/global-cybersecurity-index-2024
20. 2024 ISC2 Cybersecurity Workforce Study October 31, 2024 URL: https://www.isc2.org/Insights/2024/10/ISC2-2024-Cybersecurity-Workforce-Study
21. e-Residency of Estonia | Apply & start an EU company online URL: https://www.e-resident.gov.ee/
22. NIST анонсировал первые четыре алгоритма пост-квантовой криптографии 7 июля 2022 г. URL: https://is-systems.org/blog_article/11657178123
23. Сборник ЦИФРОВАЯ ПОВЕСТКА ЕАЭС 2016-2019-2025 URL: https://eec.eaeunion.org/upload/files/paos/library/digital_agenda_eaeu.pdf
24. SIRIUS project SIRIUS Cross-Border Access To Electronic Evidence URL: https://www.europol.europa.eu/operations-services-innovation/sirius-project
25. Cyber Threat Alliance (CTA) URL: https://cybilportal.org/actors/cyber-threat-alliance-cta/