Салишев Сергей Николаевич.

Сеюбергенова Дидар Сламовна

Исманов Таалайбек Кадырович

DOI 10.31483/r-149585

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В МЕЖДУНАРОДНОМ ПРАВЕ

Аннотация*: в главе рассматривается проблема формирования многополярного информационного пространства и необходимость регулирования международной информационной безопасности. Анализируются международно-правовые акты, регулирующие вопросы информационных ресурсов. Основное внимание уделяется документам, принятым Генеральной Ассамблеей ООН и Советом Европы, которые направлены на борьбу с преступным использованием информационных технологий и формирование культуры кибербезопасности. Отмечается, что международное сообщество признает значимость информационной безопасности, но существует проблема единого понимания ключевых вопросов, что усложняет глобальное регулирование этой сферы. В связи с этим предлагается разработать новый универсальный документ на глобальном уровне под эгидой ООН и унифицировать международное законодательство в сфере обеспечения информационной безопасности и разработать новые нормативно-правовые акты, способные адекватно реагировать на вызовы цифровой эпохи.*

Ключевые слова*: информационная безопасность, международное сотрудничество, ООН, информационные технологии, киберпространство, экстерриториальность, уголовное право, конвенция.*

Abstract*: the chapter considers the problem of forming a multipolar information space and the need to regulate international information security. It analyzes international legal acts regulating information resources. The main attention is paid to the documents adopted by the UN General Assembly and the Council of Europe, which are aimed at combating the criminal use of information technologies and*

forming a culture of cybersecurity. It is noted that the international community recognizes the importance of information security, but there is a problem of a common understanding of key issues, which complicates the global regulation of this area. In this regard, it is proposed to develop a new universal document at the global level under the auspices of the UN and to unify international legislation in the field of ensuring information security and to develop new regulatory legal acts that can adequately respond to the challenges of the digital age.

***Keywords**: information security, international cooperation, information technology, cyberspace, extraterritoriality, criminal law, convention.*

Формирование многополярного информационного пространства представляет собой сложный процесс, требующий комплексного подхода к регулированию международной информационной безопасности. Этот процесс неизбежно порождает новую сферу межгосударственного соперничества, оказывающую значительное влияние на глобальную систему безопасности. Необходимо четко разграничивать безопасность глобального и национального информационного пространства, поскольку международная информационная безопасность напрямую зависит от защищенности национальных информационных систем. Это обстоятельство подчеркивает необходимость разработки и заключения межгосударственных соглашений, направленных на обеспечение устойчивого функционирования информационной инфраструктуры в условиях многополярности.

Некоторые аспекты информационной безопасности уже получили нормативно-правовую регламентацию в международном праве. Так, одним из ключевых положений является право на информацию, закрепленное в Резолюции A/RES/59 (I) Генеральной Ассамблеи ООН, где оно определено как основное право человека и критерий всех видов свободы, включая свободу информации, под которой понимается «право свободно собирать, передавать и публиковать информацию» [1]. Всеобщая декларация прав человека ООН 1948 года [2] в статье 19 подтверждает право каждого на свободу убеждений, включая свободу искать, получать и распространять информацию и идеи любыми средствами

независимо от государственных границ. Статья 12 Декларации гарантирует защиту личной информации от неправомерного вмешательства [2].

В 2011 году Генеральная Ассамблея ООН признала доступ к интернету неотъемлемым правом [3], что свидетельствует о признании его значимости в современном обществе. Двумя годами позже, в 2013 году, была принята Резолюция Генеральной Ассамблеи ООН 68/167 [4], подчеркивающая, что развитие информационных технологий увеличивает возможности для отслеживания и сбора информации, что в конечном итоге может стать источником нарушения права на неприкосновенность личной жизни, защищенное статьей 12 Всеобщей декларации прав человека [2] и статьей 17 Международного пакта о гражданских и политических правах [5]. Резолюция подчеркнула необходимость защиты этих прав как в офлайновой, так и в онлайновой среде и предотвращения преступлений в этой области [4]. В документе также отмечается, что технический прогресс создает новые возможности для киберпреступности и предлагается комплекс мер, включая законодательное регулирование и обмен информацией между государствами [4].

Среди международно-правовых актов, регулирующих вопросы информационных ресурсов, значительную роль играют Конвенция о международном обмене изданиями и Конвенция об обмене официальными изданиями и правительственными документами между государствами, принятые в 1958 году. Эти документы направлены на содействие обмену изданиями и официальными документами между государственными и неправительственными учреждениями без коммерческих целей, исключая конфиденциальную информацию.

Одним из ключевых международных документов в сфере глобальной информационной безопасности является также Резолюция Генеральной Ассамблеи ООН №55/63, которая направлена на борьбу с киберпреступностью и преступным использованием информационных технологий. Этот акт стал ключевым в международной стратегии по обеспечению кибербезопасности и защите информационного пространства от незаконных действий. Резолюция настоятельно рекомендует активизировать координацию усилий на глобальном уровне с целью

минимизации рисков, связанных с киберугрозами. Документ обращает внимание государств на необходимости формирования собственной нормативно-правовой базы, способной адекватно и своевременно реагировать на вызовы, обусловленные стремительным развитием информационных технологий и их интеграцией в различные сферы общественной жизни [6].

Резолюция 57/239 обращает внимание на создании глобальной культуры кибербезопасности, указывая на то, что эффективная защита требует не только технологических решений, но и комплексного подхода, включающего планирование, управление и превентивные меры. В приложении к резолюции выделены ключевые элементы культуры кибербезопасности: осведомленность, ответственность, реагирование, этика, демократия, оценка рисков, проектирование и внедрение средств защиты, а также управление безопасностью [7].

Конвенция Совета Европы «О киберпреступности», принятая в 2000 году [8], стала первым международным документом, рекомендующим странам-участницам включить в национальное законодательство нормы об уголовной ответственности за киберпреступления. В ней определяются составы преступлений, включая незаконный доступ, перехват данных, воздействие на компьютерные системы, мошенничество и подлог с использованием информационных технологий, а также правонарушения, связанные с детской порнографией и нарушением авторских прав. Документ включает положения, касающиеся уголовно-правовых аспектов, процедурных вопросов и международного сотрудничества, требуя от стран принятия мер для обеспечения сохранности компьютерных данных и предоставления полномочий компетентным органам на обыск и доступ к системам [8].

Конвенция Совета Европы также направлена на обеспечение международного сотрудничества в сфере расследования и судебного преследования преступлений, связанных с использованием информационных технологий на принципах взаимной правовой помощи между государствами-участниками. В чрезвычайных ситуациях запросы о помощи могут передаваться через оперативные каналы связи, такие как факс и электронная почта, с последующим официальным

подтверждением. Стороны также могут просить друг друга о сохранении данных, находящихся на территории другой стороны и необходимых для расследования. Для оперативной координации действий каждая сторона создает круглосуточный контактный центр, через который осуществляется обмен сообщениями.

Статья 32 Конвенции Совета Европы о киберпреступности предусматривает возможность получения одной стороной доступа к общедоступным данным другой стороны без ее предварительного согласия. Данная норма фактически санкционирует проведение оперативно-розыскных мероприятий, включая обыски и изъятия данных в компьютерных сетях, расположенных на территории иностранных государств [8]. Вместе с тем имплементация подобных мер может вступать в коллизию с основополагающими принципами государственного суверенитета и правовой автономии, что порождает серьезные сомнения в их легитимности и правомерности на международной арене. Конечно, данный вопрос требует детального и многоаспектного исследования с учетом актуальной нормативно-правовой базы и принципов международного права.

К слову сказать, международное право, включая и международное уголовное право, в настоящее время находится в процессе трансформации. Проблема обеспечения информационной безопасности на международном уровне возникла давно, но универсального механизма для противодействия преступлениям в этой сфере до сих пор не разработано. Хотя отдельные институты и предпосылки для такого механизма имеются, а межгосударственные политические отношения способствуют реализации института экстрадиции и привлечения к уголовной ответственности лиц, нарушивших информационную безопасность, эти меры носят скорее эпизодический, чем системный характер. Вызывает сегодня тревогу и ослабление ООН вместе с Советом Безопасности. Основные причины кроются в усилении геополитических противоречий между крупными державами и их альянсами, а также в изменении глобального баланса сил. Эти факторы подрывают доверие к традиционным международным институтам. Такое ослабление, по мнению ряда исследователей, может привести к серьезным последствиям, таким

как формирование блоков и коалиций, игнорирующих международные нормы [9, с. 107].

Российская Федерация активно участвует в продвижении уголовно-правового регулирования информационной безопасности на международном уровне. В 1998 году она предложила резолюцию ООН «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», что стало основой для обсуждения пределов использования информационно-коммуникативных технологий.

В 2000 году была принята Окинавская хартия глобального информационного общества [10], признающая информационные технологии ключевым фактором развития XXI века. Документ призывает государства развивать информационные технологии и формировать международное партнерство в этой сфере.

Мировое сообщество признает значимость информационной безопасности, однако существуют проблемы с единым пониманием ключевых вопросов, что приводит к точечной работе и принятию актов, охватывающих лишь отдельные аспекты этой сферы. Вместе с тем в условиях стремительного развития цифровой инфраструктуры и роста киберугроз сегодня возникла острая необходимость в создании нового глобального нормативного акта, который бы заменил Конвенцию Совета Европы о киберпреступности 2001 года. Несмотря на значимость этого документа в борьбе с киберпреступностью, на сегодняшний день он не отражает всех современных вызовов и реалий, связанных с технологическим прогрессом и глобализацией киберпространства. В связи с этим требуется разработка более всеобъемлющего и адаптивного документа, который учитывал бы не только правовые, но и технические, социальные и экономические аспекты кибербезопасности. Создание нормативного акта под эгидой ООН обеспечит его универсальность и правомерность, что имеет решающее значение для эффективного международного сотрудничества по противодействию киберугрозам. Участие множества стран и экспертов в разработке документа позволит учесть разнообразие национальных правовых систем и практик и поможет создать более сбалансированный и приемлемый для всех участников документ.

На региональном уровне Шанхайская организация сотрудничества (ШОС) уже предприняла подобную попытку. Одним из существенных документов в этой области является межправительственное Соглашение государств-членов ШОС «О сотрудничестве в области обеспечения международной информационной безопасности», подписанное 16 июня 2009 года в Екатеринбурге [11]. Соглашение выделяет ключевые угрозы: разработка и использование информационного оружия, ведение информационных войн, терроризм, преступность, стремление к доминированию в информационном пространстве, распространение вредоносной информации и атаки на информационные инфраструктуры. В документе также представлен список основных источников и признаков этих угроз. Информационная преступность определяется как использование информации в противоправных целях, ее признаками являются: несанкционированный доступ, создание и распространение вирусов, DOS-атаки, ущерб ресурсам, нарушение прав граждан и использование информации для совершения преступлений. Хотя определение информационной преступности в Соглашении не является идеальным, его подписание имеет важное значение. Документ устанавливает направления, принципы, формы и механизмы сотрудничества, а также анализирует основные угрозы [11]. Это соглашение стало важным шагом к унификации законодательства в странах ШОС и может быть расширено на международном уровне.

На уровне другой региональной организации, участницей которой является Россия, чуть ранее, 1 июня 2001 года в Минске было подписано Соглашение стран СНГ «О сотрудничестве в борьбе с преступлениями в сфере компьютерной информации» [12], направленное на эффективную борьбу с этим явлением. В документе уголовно наказуемыми признаются такие деяния, как: неправомерный доступ к охраняемой информации, создание и распространение вредоносных программ, нарушение правил эксплуатации ЭВМ и незаконное использование авторских программ [12]. Это Соглашение также является важным шагом к унификации законодательства стран постсоветского пространства.

В процессе создания международных правовых норм возникает ряд проблем, связанных с определением квалификации киберпреступлений. Одна из

таких проблем – установление статуса целенаправленного воздействия на критически важные информационные системы государств. Необходимо определить, является ли подобное воздействие актом агрессии, который дает право на применение мер самообороны в соответствии с международным правом. Кроме того, необходимо разработать критерии для оценки последствий кибератак, чтобы определить, можно ли считать их вооруженным нападением. Это сложная задача, требующая тщательного анализа и согласования между странами. Важно создать эффективный механизм для совместного расследования кибератак и привлечения к ответственности лиц, причастных к их совершению. Особое внимание при этом следует уделить проблеме квалификации киберсаботажа в космическом пространстве, включая блокировку или иное воздействие на государственные спутники. Этот вопрос также требует комплексного подхода, учитывающего специфику космических технологий и их важность для национальной безопасности.

В настоящее время международное регулирование информационной безопасности сталкивается с еще рядом сложных и многоаспектных проблем, требующих комплексного анализа и системного подхода. Одной из центральных проблем является идентификация субъектов, участвующих в киберпреступной деятельности. Этот процесс осложняется анонимностью киберпространства и его трансграничным характером. Доказывание причастности к киберпреступлениям представляет значительные трудности вследствие особенностей цифровых следов и необходимости преодоления юридических барьеров, связанных с государственным суверенитетом. К тому же, квалификация целей и мотивов кибератак требует детального изучения и применения интегративного подхода, учитывающего как технические, так и социальные аспекты. Понимание мотивов киберпреступников, будь то финансовые, политические или идеологические цели, также имеет ключевое значение для разработки эффективных стратегий противодействия и предотвращения подобных инцидентов в будущем.

И все эти задачи необходимо решать с помощью междисциплинарного подхода и координации усилий государств на глобальном уровне.

Безусловно, такие международно-правовые акты, как Резолюция Совета Европы, Шанхайское и Минское соглашение, несмотря на высокую значимость, обладают ограниченным эффектом и представляют собой, по сути, инструменты «мягкого права», ориентированные на региональное применение. Для создания эффективной системы обеспечения информационной безопасности на глобальном уровне необходимо разработать и внедрить унифицированные механизмы, что требует консолидации политической воли и достижения договоренностей между государствами.

Сегодня отсутствие единого международного соглашения, регулирующего вопросы кибератак и мер противодействия им, представляет серьезную опасность. Ведь в условиях, когда киберпространство не имеет четких правовых рамок, злоумышленники могут использовать информационные технологии для политического давления, шпионажа, саботажа и даже терроризма. Поэтому все усилия международного сообщества должны быть направлены на нейтрализацию этих угроз. Разработка Хартии информационных прав станет важным шагом на пути создания единой правовой основы для защиты информационных ресурсов и противодействия киберугрозам. Этот документ должен включать принципы обеспечения конфиденциальности и целостности данных, ответственности за нарушения, международного сотрудничества и обмена информацией. Только совместными усилиями государств и международного сообщества можно создать эффективную систему защиты информационного пространства и обеспечить безопасность в эпоху цифровых технологий.

Также для решения современных проблем информационной безопасности необходимо разработать новую Конвенцию ООН, в которой должны быть учтены последние достижения в цифровых технологиях и отражены текущие вызовы и угрозы. Документ необходимо разрабатывать на основе новейших научных исследований в области криптографии, кибербезопасности и правового регулирования цифровых технологий. Конвенция должна охватывать комплексные меры по предотвращению кибернетических атак, защите критически важной информационной инфраструктуры, обеспечению конфиденциальности,

целостности и доступности данных, а также противодействию киберпреступности на глобальном уровне. Для достижения этой цели необходимо междисциплинарное сотрудничество экспертов в области права, информатики, социологии и смежных дисциплин. Это сотрудничество позволит разработать и внедрить эффективные механизмы защиты, учитывающие динамичный характер киберугроз и многообразие их проявлений.

Большие проблемы связаны с международным правовым регулированием преступлений, совершаемых с помощью интернета. К сожалению, на международном и региональном уровнях в настоящее время отсутствует систематизированная нормативно-правовая база, регламентирующая мониторинг и контроль за функционированием технических средств перехвата информации. Правда, в рамках СНГ разработаны и утверждены комплексные документы, направленные на повышение прозрачности и эффективности использования данных технологий. Также Российская Федерация предприняла инициативу по унификации подходов к противодействию информационной преступности, в том числе и на просторах интернета, представив в ООН проект Конвенции «Об обеспечении международной информационной безопасности». Этот документ предполагал интеграцию усилий международного сообщества на уровне Интерпола, включая обмен компьютерной информацией для проведения совместных расследований трансграничных преступлений. Однако проект Конвенции не получил поддержки со стороны других государств-участников, что еще раз подтверждает недостаточную степень консенсуса по данному вопросу на глобальном уровне.

Выводы.

1. В условиях отсутствия унифицированной системы правовых норм, регулирующих сферу информационной безопасности, возникает правовой вакуум, который существенно затрудняет международное сотрудничество и создает предпосылки для правовой неопределенности.

2. Отсутствие унифицированной нормативно-правовой базы в сфере информационной безопасности представляет собой значимое препятствие для эффективного регулирования и защиты критически важных информационных

ресурсов. Данная проблема приводит к фрагментации правового режима, что затрудняет координацию международных усилий по обеспечению информационной безопасности и снижает уровень доверия и сотрудничества между государствами.

3. Для решения этой проблемы необходимо разработать комплексные международные стандарты, учитывающие специфику цифровой среды и обеспечивающие высокий уровень защиты информации. Такие стандарты должны базироваться на принципах прозрачности, подотчетности и международного сотрудничества, что позволит создать действенную систему правового регулирования в области информационной безопасности.

4. Разработка и внедрение международных стандартов в сфере информационной безопасности являются ключевыми для обеспечения устойчивого развития в условиях цифровой трансформации. Только через создание унифицированной нормативно-правовой базы можно достичь гармонизации правовых режимов и обеспечить надежную защиту информационных ресурсов на глобальном уровне.

Список литературы

1. Резолюция Генеральной Ассамблеи ООН A/RES/59 (I) «Созыв международной Конференции по вопросу о свободе информации» 14 декабря 1946 года [Электронный ресурс]. – Режим доступа: http://un.org (дата обращения: 03.03.2025).

2. Всеобщая декларация прав человека. Принята резолюцией 217 A (III) Генеральной Ассамблеи ООН от 10 декабря 1948 года [Электронный ресурс]. – Режим доступа: https://clck.ru/3MzXvW (дата обращения: 03.03.2025).

3. Доклад Генеральной Ассамблеи ООН от 16 мая 2011 года [Электронный ресурс]. – Режим доступа: https://clck.ru/3MzXwF (дата обращения: 06.03.2025).

4. Резолюция Генеральной Ассамблеи ООН 68/167 «Право на неприкосновенность личной жизни в цифровой век» 8 декабря 2013 года [Электронный ресурс]. – Режим доступа: https://online.zakon.kz/Document/?doc_id=31499342 (дата обращения: 08.03.2025).

5. Международный пакт о гражданских и политических правах. Принят резолюцией 2200 A (XXI) Генеральной Ассамблеи от 16 декабря 1966 года [Электронный ресурс]. – Режим доступа: https://clck.ru/3MzXxi (дата обращения: 10.03.2025).

6. Резолюция Генеральной Ассамблеи ООН 55/63 «Борьба с преступным использованием информационных технологий» [Электронный ресурс]. – Режим доступа: http://un.org/ (дата обращения: 03.03.2025).

7. Резолюция Генеральной Ассамблеи ООН 57/239 «Создание глобальной культуры кибербезопасности» [Электронный ресурс]. – Режим доступа: http://un.org/ (дата обращения: 06.03.2025).

8. Конвенция Совета Европы о киберпреступности от 23 ноября 2001 года // Международное уголовное право в документах. В 2 т. Т. 1. – Казань: Казан. гос. ун-т, 2005. – С. 467–482.

9. Сидорова Т.Ю. Международная информационная безопасность: правовые аспекты и деятельность ООН / Т.Ю. Сидорова // Сибирский юридический вестник. – 2020. – №3 (90). – С. 103–108. – EDN XQJXUJ

10. Окинавская хартия глобального информационного общества от 21 июля 2000 года [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/cons/cgi/online.cgi?req=d…odXDwttG (дата обращения: 08.03.2025).

11. Соглашение государств-членов ШОС «О сотрудничестве в области обеспечения международной информационной безопасности». Подписано 16 июня 2009 года [Электронный ресурс]. – Режим доступа: https://clck.ru/3MzY2o (дата обращения: 06.03.2025).

12. Соглашение стран СНГ «О сотрудничестве в борьбе с преступлениями в сфере компьютерной информации». Подписано 1 июня 2001 года // Собрание законодательства Российской Федерации. – 2009. – №13. – Ст. 1460.

Салишев Сергей Николаевич – аспирант, Отдела аспиратуры и докторантуры Кыргызский национальный университет им. Жусупа Баласагына, Бишкек, Республика Кыргызстан.

Сеюбергенова Дидар Сламовна – докторант PhD / по юриспруденции, Международный университет Кыргызстана, Бишкек, Республика Кыргызстан.

Исманов Таалайбек Кадырович – руководитель направления докторанты PhD / по юриспруденции, Международный университет Кыргызстана, Бишкек, Республика Кыргызстан.