13. Secretary General on the war in Ukraine: “a catastrophe that shakes the foundations of the world order”. URL: https://news.un.org/ru/story/2022/03/1420992 (дата обращения: 21.07.2022).

14. The Davos Agenda 2022 brings together world leaders to address the state of the world. URL: https://www.weforum.org/agenda/2022/01/the-davos-agenda-2022-addressing-the-state-of-the-world/ (дата обращения: 21.01 2022).

15. UNDESA World Social Report 2021. URL: https://www.un.org/development/desa/dspd/world-social-report/2021–2.html (дата обращения: 21.07.2022).

16. United Nations Secretary-Generals Report «Our common agenda». URL: https://www.un.org/en/content/common-agenda-report/assets/pdf/Common_Agenda_Report_English.pdf (дата обращения: 21.07.2022).

Е. Е. Гуляева,
кандидат юридических наук, доцент,
Дипломатическая академия Министерства иностранных дел
Российской Федерации

МЕЖДУНАРОДНО-ПРАВОВАЯ КОНЦЕПЦИЯ ПРИМЕНЕНИЯ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ СИСТЕМ И ЦИФРОВЫХ ТЕХНОЛОГИЙ

Аннотация. Настоящая статья посвящена международно-правовой концепции применения информационно-коммуникационных систем и цифровых технологий. Автор рассматривает понятия «информационные права», выделяет два основных юридических подхода к регулированию системы обеспечения международной безопасности: фрагментарный и комплексный. Автор статьи приходит к выводу, что разрыв в техническом обеспечении предполагает существование условно информационно «богатых» и информационно «бедных» государств, что, по сути, негативно влияет на соблюдение принципа суверенного равенства государств в международном праве.

Ключевые слова: право, правовая доктрина, информационные коммуникационные технологии, цифровые технологии, международное сотрудничество, принципы международного права

INTERNATIONAL LEGAL CONCEPT OF THE APPLICATION OF INFORMATION COMMUNICATION SYSTEMS AND DIGITAL TECHNOLOGIES

Abstract. This article is devoted to the international legal concept of the use of information and communication systems and digital technologies. The author considers the concept of «information rights», identifies two main legal approaches to the regulation of the system of ensuring international security: fragmented and complex. The author of the article comes to the conclusion that the gap in technical support implies the existence of conditionally informationally “rich” and informationally “poor” states, which in

fact negatively affects the observance of the principle of sovereign equality of states in international law.

Keywords: Law, Legal concept, Information communication systems, Digital technologies, International cooperation, Principles of international law

В настоящее время довольно сложно предположить, каким образом будет развиваться международное сотрудничество государств в сфере применения информационных телекоммуникационных систем и цифровых технологий для поддержания международного мира и безопасности. Очевидно, что перед государствами всего мира остро встает вопрос о поиске новых путей, парадигм разрешения проблемы обеспечения международной и, как следствие, глобальной безопасности. При этом традиционные методы решения проблемы уже не являются достаточными. Возникает вопрос о возможности применения современных информационных технологий, а также иных достижений науки и техники для обеспечения международной безопасности. Рассмотрение поставленного вопроса с указанных позиций ставит перед научным сообществом множество вопросов: какие технологии могут быть использованы, их пределы, варианты правового регулирования, соотношение практики использования указанных технологий с общепризнанными принципами и нормами международного права и т. д.

Зачастую мы видим попытки управления информационным пространством на государственном уровне с целью манипулирования общественным мнением и преподнесением информации о вопросах (так называемый феномен фэйк-ньюс), затрагивающих международную безопасность в том ключе, который выгоден конкретной политической элите.

В результате потребуется дальнейшее совершенствование нормативно-правового регулирования порядка оказания трансграничных услуг информационными компаниями, являющимися национальными юридическими лицами конкретных государств, например, таких, как Google, Facebook (признана экстремистской организацией, запрещена в РФ), Amazon, Яндекс и т. п.

Составным элементом международной безопасности является также безопасность личности, которая в новых, глобализирующихся условиях принимает вид обеспечения защищенности граждан в информационном пространстве (обеспечение информационных прав). Информационные права граждан признаются и закрепляются не только на национальном, но и на международном уровнях. Поэтому лица, с учетом установленных ограничений, могут реализовывать свои информационные права на территории других государств, что является существенной предпосылкой для международного информационного обмена.

В рамках теоретической проработки вопросов о правах человека в сфере информационного обмена появилась концепция *права человека на коммуникацию*, создатели которой пришли к выводу, что в международном праве на момент разработки концепции отсутствовал единый принцип, на основании которого осуществлялось бы управление вопросами коммуникации в масштабе всей планеты. Поэтому экспертами было предложено включить в международно-правые акты *право человека на уникальную коммуникацию* [1. С. 127–135].

Одной из составных частей права на информацию является право граждан на получение информации о деятельности органов государственной власти. В ходе реализации данного права современные государства не могут сокрыть информацию, которая имеет жизненно важное значение для большого числа граждан. В определенных случаях высказывается мнение об установлении приоритета соответствующего информационного права гражданина над интересами национальной безопасности.

Актуальным в современных условиях является вопрос об обеспечении сохранности персональных данных граждан в условиях формирования информационного общества. Данный аспект права стал чуть ли не важнейшим видом обеспечения прав граждан в последние десятилетия. Так, основополагающим нормативно-правовым актом в сфере прав человека провозглашено право на неприкосновенность частной жизни, которое, однако, может быть ограничено в связи с активной информатизацией общественных отношений.

Стоит отметить, что в связи со сложной эпидемиологической ситуацией в мире из-за распространяющейся коронавирусной инфекции (COVID-19) информационные права граждан отдельно взятого государства претерпевают существенные изменения: нередки случаи, когда вопрос обеспечения национальной безопасности стоит выше любого другого права индивида или отдельно взятой группы лиц.

Другим важным и актуальным аспектом является доступ, использование и применение информации в огромных информационных массивах (Big Data), т. е. такой технологии, когда сведения о гражданах, в том числе составляющие их персонифицированные данные, сосредотачиваются в одном месте и могут использоваться для различных целей. Все это создает не только угрозу нарушения информационных прав граждан, но и увеличивает риск компрометации этих данных.

Принято считать, что развивающиеся стремительными темпами глобальные информационно-коммуникационные технологии оказывают исключительно благоприятное воздействие на человека и общественные отношения. В частности, указывается на огромное расширение возможностей по обмену информацией, по поддержанию социальных связей, по развитию глобальной экономики [2. С. 295]. Именно развитием указанных технологий определяется качественный переход человечества в информационное общество (new information era). Но нельзя забывать о том, что современные коммуникационные технологии, помимо очевидного позитивного эффекта, могут стать источником нарушения состояния защищенности общества или его отдельных элементов.

Современные тренды развития информатизации могут представлять определенную угрозу в случае неконтролируемого развития соответствующего сегмента информационного пространства. Попробуем проследить данные тенденции на примере развития международной глобальной сети Интернет, систем искусственного интеллекта и Big Data.

Существенным моментом в направлении развития правового механизма регулирования использования сети Интернет и обеспечения безопасности стало принятие Лондонского плана действий по международному сотрудничеству в области применения законодательства против спама [3. С. 48–51]. В указанном документе

прослеживается дальнейшее развитие положений, содержащихся в Меморандуме о взаимопомощи в вопросах коммерческих рассылок по электронной почте, составленном Федеральной торговой комиссией США, Офисом по законной торговле Великобритании, Уполномоченным по информации и некоторыми другими уполномоченными органами ряда зарубежных стран. Россия также присоединилась к указанному плану действий.

Попыткой урегулирования на международном уровне отношений в части использования сети Интернет и минимизации связанных с этим риском стало принятие программы ЮНЕСКО «Информация для всех». Названный документ призван оказать содействие в выработке единого глобального подхода к этическим и правовым нормам, регулирующим информационное пространство. Проблематика нежелательных информационных сообщений (спама) стала предметом обсуждения на Всемирном саммите по информационному обществу. По результатам проведения данного мероприятия была принята Тунисская программа для информационного общества [4. С. 539], в соответствии с которой должны быть приняты эффективные меры для скорейшего разрешения проблемы спама.

В соответствии с резолюцией Генеральной Ассамблеи ООН A/RES/33/115 от 18.12.1978 «Вопросы, касающиеся информации» закрепляется принцип свободного, широкого и сбалансированного распространения информации. Правовое регулирование распространения информации посредством сети Интернет основывается на базовых принципах, которых предоставляют любому государству возможность создания на своей территории компьютерных сетей и гарантируют возможность участия государств в международном информационном обмене. С другой стороны, констатируется, что каждое государство имеет право на принятие мер защиты от вредной и общественно опасной информации. Соответствующие тезисы нашли свое закрепление в Конвенции Совета Европы «О киберпреступности».

Интересно отметить, что Россия отказалась подписать данный документ. Одним из ключевых положений Конвенции является предоставление доступа государствами к собственным техническим средствам другим участникам Конвенции.

В настоящее время в международной практике правового регулирования распространения информации в сети Интернет сложилось три основных модели, которые стали реакцией международного сообщества и национальных государств на те угрозы, которые исходят от сети Интернет, в частности от неконтролируемого распространения вредоносной информации.

Первая модель заключается в установлении полного контроля государства за распространением информации в сети Интернет. Наиболее ярким примером такой модели является Китай. В соответствии с законом КНР «О телекоммуникациях» для начала своей деятельности интернет-провайдеры обязаны получить лицензию в уполномоченном органе государственной власти с раскрытием основных параметров своей компании. Кроме того, интернет-провайдеры должны хранить информацию о своих сайтах, их посещениях и предоставлять данную информацию сотрудникам правоохранительных органов [7. С. 488–497].

Согласно второй модели, интернет-провайдеры несут ответственность за любые действия пользователя. Так, в соответствии с французским законодатель-

ством они обязаны сообщать информацию о владельцах сайтов и авторах контента на них любым заинтересованным лицам, в противном случае они рискуют быть привлеченными к уголовной ответственности. Пример Франции интересен также тем, что еще в 1978 г. была создана Национальная комиссия информатики и свобод, которая была уполномочена на осуществление контрольных мероприятий в сфере информатизации [8. С. 15–23].

В соответствии с третьей моделью правового регулирования распространения информации в сети интернет-провайдеры освобождаются от несения ответственности при условии, что они выполнили предусмотренные законодательством действия в части предоставления услуг и взаимодействия с пользователями. Например, в соответствии с немецким законодательством интернет-провайдеры не могут нести ответственность за размещение противоправной информации только в том случае, если они являются непосредственными распространителями данной информации или ее собственниками. При этом у провайдеров отсутствует обязанность удалять незаконную информацию, которая была размещена на их серверах.

Искусственный интеллект принято делить на слабый и сильный. Сильный искусственный интеллект характеризуется наибольшей приближенностью к параметрам человеческого разума, что предполагает возможность обработки им чувственной информации. К настоящему времени еще не удалось создать киберфизическую систему общего назначения, но стоит ожидать возможное решение данной задачи в ближайшее время. Поэтому очень важным является формирование соответствующей нормативной базы использования искусственного интеллекта в форме роботов, для чего необходимо выделить приоритетные направления, по которым должно осуществляться правовое регулирование как на национальном, так и на международном уровнях:

1) проведение стандартизации систем искусственного интеллекта;

2) проведение лицензирования деятельности, связанной с созданием и использованием систем искусственного интеллекта;

3) обеспечение конфиденциальности персональных данных;

4) соблюдение норм профессиональной этики.

В настоящее время искусственный интеллект, обучаемый на базе глубоких нейронных сетей, повсеместно применяется специалистами и учеными в различных областях: в прогнозировании, в системах массового обслуживания, в анализе данных и др. Особую популярность набирает направление создания и использования беспилотных летательных и транспортных средств на базе искусственного интеллекта.

Традиционно новеллы правового регулирования, прежде чем стать предметом регулирования международно-правовых актов, принимаются на уровне национальных государств. Если говорить о сфере искусственного интеллекта, и в частности робототехники, то первым государством в мире, в котором были на официальном государственном уровне утверждены правила передвижения курьеров-роботов, стала Эстония. В Германии действует закон, в соответствии с которым вводятся более простые правила относительно перемещений транспортных средств, управляемых искусственным интеллектом. Но при этом для владельцев такого транспорта установлены повышенные санкции за допущенные нарушения. При этом ответственность

за любые происшествия с транспортным средством все равно несет водитель, т. е. участие человека во время управления транспортным средством признается обязательным [9. С. 99–102].

В Японии несколько лет назад были разработаны законы, посвященные осуществлению контроля за использованием систем искусственного интеллекта. В указанных документах в первую очередь решаются вопросы, связанные с авторским правом на технологии искусственного интеллекта. В соответствии с японским законодательством авторские права на указанные технологии принадлежат заказчикам, но в последующем предполагается осуществление перехода исключительных прав к разработчикам. Также интересной особенностью японского законодательства является возложение на компании-разработчики систем искусственного интеллекта ответственности за возникновение любых негативных последствий от использования искусственного интеллекта, в том числе возмещение ущерба пострадавшим лицам.

Стоит отметить, что Япония уже сравнительно длительное время предпринимает попытки по разработке наиболее оптимальных способов регулирования рынка искусственного интеллекта. Планируется введение сертификатов соответствия требованиям безопасности для робототехники [10. С. 117–124].

Важно отметить и тот факт, что новые технологии могут нести определенный риск для жизни и здоровья граждан – проведение DDoS-атак на важные объекты инфраструктуры, создание фейковых новостей на базе искусственного интеллекта или даже обычное использование беспилотных транспортных средств. Распространение же антиправительственной информации через скрытые сетевые ресурсы сети Интернет несет непосредственную угрозу для конституционной целостности государства и поддержания общественного порядка.

Наличие у государства информационного оружия дает ему преимущества перед другими государствами, у которых такого оружия нет. Все это ставит проблему так называемого цифрового разрыва, когда существует неравенство государств в распределении научно-технологических ресурсов и доступа к информационным технологиям. Этот разрыв предполагает существование условно информационно «богатых» и информационно «бедных» государств [11. С. 70–74].

Информация стала источником появления новых проблем по причине слишком активного развития информационных технологий. Появление высокоточного оружия, оружия массового уничтожения и вооружений, основанных на новых физических принципах, создает непосредственную угрозу для существования всего человечества. Ведение войны традиционными способами и средствами не идет ни в какое сравнение с современными видами вооружения и последними достижениями научно-технического прогресса.

Современные конфликты между государствами все чаще переходят из ведения боевых действий на земле в информационное пространство. В результате воюющие стороны стали активно использовать информационно-коммуникационные технологии для причинения ущерба другим государствам, что противоречит правилам и нормам международного общения.

Деятельность, связанная с обеспечением международной информационной безопасности, является одним из актуальных направлений международного со-

трудничества государств по вопросам обеспечения и поддержания международной безопасности в целом. К настоящему времени сложились два основных юридических подхода к регулированию системы обеспечения международной безопасности: фрагментарный и комплексный.

Данные подходы образуют основу современных концепций обеспечения информационной безопасности на различных уровнях регулирования. Изучая содержание этих подходов, можно установить основные положения соответствующих концепций. В отличие от содержания нормативно-правовых актов международного уровня по вопросам обеспечения безопасности, правовые концепции являются стабильными и мало изменчивыми. Они определяют базовые позиции государств по вопросам международной безопасности [12. С. 124–135].

Кроме того, для всех моделей концепций международной информационной безопасности характерно наличие общей цели, а именно формирование международной кибербезопасности.

Общепризнано, что государство на международной арене должно своими усилиями способствовать социальному и экономическому развитию общества. При этом соответствующая деятельность государств должна соотноситься с идеями поддержания мира и международной безопасности, неприкосновенности суверенитета государств и защиты прав и свобод человека и гражданина. Также важны принципы международной информационной безопасности. Например, государства в ходе осуществления своей информационной деятельности должны принимать во внимание принцип неделимости безопасности, принцип ответственности за находящееся в их юрисдикции информационное пространство. Неделимость безопасности означает, что для обеспечения национальной безопасности государства имеет значение состояние защищенности всех основных сфер жизни общества у других государств и всего мирового сообщества в целом.

В соответствии с постулатами первой концепции, которая получила название фрагментарной, современная международная информационная безопасность направлена в первую очередь на противодействие совершению уголовных преступлений в сфере высоких технологий. Именно данный аспект нуждается в правовом регулировании нормами международного права. Но в неразрывной связи с указанным аспектом находится и такая задача правового регулирования, как противодействие террористической деятельности, совершаемой посредством информационно-коммуникационных технологий и реализуемой непосредственно в информационном пространстве [13. С. 71–75].

Вторая концепция именуется комплексной. В соответствии с ее идеями требуется широкое освещение проблематики в сфере международной информационной безопасности. Сторонники названной концепции считают, что международная безопасность является неделимой, поэтому государства должны обеспечивать комплексный подход к вопросу обеспечения национальной и международной безопасности в целом, не акцентируя внимания исключительно на вопросах информационной безопасности.

Исходя из названия концепции, использование информационно-коммуникационных технологий для предотвращения военных, террористических и преступных

угроз должно реализовываться комплексно. Вследствие этой базовой идеи, соответствующее международно-правовое регулирование должно распространяться на все составные части международной информационной безопасности.

Проблемным вопросом в данной доктрине является необходимость осуществления правового регулирования как составной части международной информационной безопасности. Известно, что международно-правовое регулирование может иметь как информационное, так и коммуникационное направление. С точки зрения международного права, названные направления принято рассматривать с позиций недопущения использования информационно-коммуникационных технологий в двух случаях:

– при причинении ущерба правам и законным интересам граждан;

– при причинении ущерба основополагающим частям государства.

Наиболее общим проявлением вышеперечисленных негативных действий является трансграничное распространение информации при помощи информационно-коммуникационных технологий. Причем речь идет об информации, содержание которой вступает в противоречие с принципами и нормами международного права. Также не исключено, что негативными проявлениями незаконных действий станет использование информационных сетей государств для распространения запрещенной информации.

Говоря о техническом направлении, соответствующее противодействие направлено на причинение вреда различным структурным элементам государства (например, финансовой, политической и другим сферам).

Представители фрагментарной концепции вообще не рассматривают вопрос о регулировании и соотношении содержательного и технического элементов международной информационной безопасности. Сторонники фрагментарной концепции полагают, что достаточными являются нормы Конвенции о киберпреступности с соответствующими дополнительными протоколами. В соответствии с положениями комплексной концепции допускается возможность правового регулирования одновременно функциональных и структурных элементов международной информационной безопасности. В качестве примера такого типа регулирования можно привести Соглашение между правительствами государств – членов Шанхайской организации сотрудничества в области обеспечения международной информационной безопасности, подписанное в 2009 г.

Особое внимание стоит обратить и на тот факт, что еще в 80-е гг. XX в. предлагались концепции, в соответствии с которыми должна быть сформирована единая концепция международной безопасности без видового разделения. Эта концепция являлась, прежде всего, документом политического характера с соответствующим инструментарием, но специалистами она все же увязывалась с международным правом [15. С. 77–80]. Довольно популярным является мнение о том, что нормы в сфере международной информационной безопасности должны получить развитие в контексте обеспечения полной системы международной безопасности [16. С. 30–35]. В подтверждение обоснованности предложенного взгляда на решение проблемы, можно привести принятую Генеральной Ассамблеей ООН резолюцию № 41/92 «О создании всеобъемлющей системы международно-

го мира и безопасности». В ходе обсуждения содержания указанного документа выдвигались предложения о создании Всемирной программы обеспечения мира и безопасности на планете.

Следует заметить, что указанные концепции не являются устойчивыми. Причинами этого является деятельность отдельных государств, направленная на разработку средств информационного подавления и ведения информационных войн. С другой стороны, большинство государств заинтересованы и предпринимают соответствующие действия для выработки наиболее оптимальных подходов к регулированию проблем международной информационной безопасности.

Ведущая роль в координации усилий международного сообщества по обеспечению международной информационной безопасности принадлежит ООН, деятельность которой преимущественно направлена на создание нормативно-правовой базы противодействия совершению преступных деяний при помощи информационно-коммуникационных технологий, но не предусматривает при этом механизма превентивных действий для купирования подобной угрозы еще на стадии планирования и проектирования. На международном уровне нет общепризнанного списка запрещенных для посещения сетевых ресурсов, доступ к которым должен быть заблокирован на национальном и региональном уровне с учетом интересов региональных стратегических партнеров – поставщиков информации в глобальной сети Интернет.

Возвращаясь к вопросу о концепциях регулирования системы обеспечения международной безопасности по части вопросов информационной безопасности, резюмируем, что исторически сложились две основные противоборствующие концепции. Наиболее предпочтительной является комплексная концепция, так как проблематика обеспечения международной безопасности в современных условиях не может не учитывать всю совокупность негативных факторов, действующих на состояние защищенности основных сфер жизнедеятельности общества. Более того, недопустимо игнорировать и другие возрастающие риски для международной безопасности в целом. Однако, учитывая скорость распространения информации и потенциальный ущерб, к которому может привести дезинформация о важных событиях в стране или регионе, акцент стоит делать именно на информационную безопасность как компонент регулирования международной безопасности.

Важно отметить, что использование злоумышленниками современных технологий для совершения противоправных деяний в киберпространстве не проходит бесследно и предполагает оставление цифровых следов их деятельности. То есть существует принципиальная возможность использования новейших технологий для раскрытия и расследования подобных преступлений. Такие возможности составляют основу соответствующего международно-правового регулирования в сфере информационной безопасности.

Как следует из вышесказанного, отдельные государства и международное сообщество в целом едины в понимании того факта, что сеть Интернет предоставляет не только определенные преимущества, но и вызывает к жизни существенные проблемы, которые необходимо решать. К таким проблемам относится, в частности,

обеспечение глобальной информационной безопасности, защита персональных данных, вопросы юрисдикции и идентификация пользователей.

Список литературы

1. Павлов В. И. Идеи правовой коммуникации и современная антропология права // Известия высших учебных заведений. Правоведение. 2014. № 5. С. 127–135.

2. Инновационные направления современных международных отношений: учебное пособие для студентов вузов / под ред. А. В. Крутских, А. В. Бирюкова. Москва: Аспект Пресс, 2010. 295 с.

3. Михайлусов С. Н. Международно-правовое регулирование Интернета // Право и управление. XXI век. 2010. № 2. С. 48–51.

4. Касенова М. Б. Институциональная структура и нормативно-правовые основы трансграничного управления интернетом: дис. … д-ра. юрид. наук. Москва, 2014. 539 с.

5. Вопросы, касающиеся информации: резолюция ГА ООН от 18.12.1978. URL: https://undocs.org/ru/A/RES/33/115 (дата обращения: 16.09.2022).

6. Конвенция о преступности в сфере компьютерной информации (ETS N 185) (заключена в Будапеште 23.11.2001) // СПС «Консультант-плюс».

7. Трощинский П. В. Особенности правового регулирования безопасности сети Интернет Китая // Журнал зарубежного законодательства и сравнительного правоведения. 2014. № 3. С. 488–497.

8. Иванова К. А., Степанов А. А. Ограничения свободы слова во Франции в эпоху цифровых технологий // Правоприменение. 2019. № 1. С. 15–23.

9. Лавриненко А. В. К вопросу о правовом регулировании использования беспилотных транспортных средств // Юридическая наука в XXI веке: сборник научных статей по итогам работы круглого стола. 2018. С. 99–102.

10. Чучаев А. И., Маликов С. В. Ответственность за причинение ущерба высокоавтоматизированным транспортным средством: состояние и перспективы // Актуальные проблемы российского права. 2019. № 6. С. 117–124.

11. Нежельский А. А. Теоретические основы исследования информационных войн и информационной безопасности государства // Власть. 2018. № 6. С. 70–74.

12. Дюкарев В. В. Современные проблемы и концепции международной безопасности // Вопросы права и политики. 2011. С. 124–135.

13. Ибрагимов Л. Х. Интернет-терроризм как феномен современных политических коммуникаций // Информационные войны. 2016. № 2. С. 71–75.

14. Соглашение между правительствами государств – членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности (заключено в г. Екатеринбурге 16.06.2009) // СПС «Консультант-плюс».

15. Лисаускайте В. В. Проблемы реформирования концепции международной безопасности в международном публичном праве // Безопасность XXI века: материалы конференции. 2001. С. 77–80.

16. Кочетков В. В. Изменения в подходах к международной безопасности в начале XXI века // Вестник Московского университета. Серия 12: Политические науки. 2010. № 4. С. 30–35.

17. Резолюция Генеральной Ассамблеи ООН № 41/92 от 04.12.1986 «О создании всеобъемлющей системы международного мира и безопасности». URL: https://undocs.org/ru/A/RES/41/92 (дата обращения: 16.09.2022).

18. Положения Всемирной программы обеспечения мира и безопасности на планете. URL: https://www.un.org/ru/sections/issues-depth/peace-and-security/index.html (дата обращения: 16.09.2022).

Е. В. Дятлова,
старший преподаватель,
Казанский инновационный университет имени В. Г. Тимирясова

ПРОБЛЕМЫ МЕЖДУНАРОДНО-ПРАВОВОГО РЕГУЛИРОВАНИЯ УПРАВЛЕНИЯ ИНТЕРНЕТОМ

Аннотация. В статье рассматривается техническая архитектура Интернета, которая определяет содержание институтов и субъектов, вовлеченных в правовые отношения в Интернете, и необходимость правового надзора за их использованием, выявляется основополагающее значение на национальном и международном уровне,поспособствовавшее развитию многих форм управления Интернетом, для которых основным принципом является участие всех сторон. Поскольку интернет – это многоуровневая сеть технической информации, можно сказать о том, что ее деятельность осуществляется в установленных пределах. При этом невозможно точно определить объект и субъект управления правоотношениями, связанными с использованием Интернета. Вышеупомянутые правовые отношения по контролю за сетью, распространяются на программное и аппаратное обеспечение для подключения различных частей сети передачи данных в разных странах, включая систему корневых серверов, которая направляет основной поток данных в Интернете, каналы и оборудование физического соединения, технические стандарты и методы фактической реализации сетевых адресов устройства связи и многое другое. Именно поэтому можно говорить о том, что эти отношения возникают у очень специфических регулирующих субъектов. На протяжении долгого времени Интернет не воспринимался государством как предмет международно-правового научного исследования. В статье проанализированы международные акты международных межправительственных организаций и международных конференций, которые связаны напрямую с управлением Интернетом, их сотрудничество можно разделить на несколько областей, которые связаны с обыденной деятельностью оперативного характера, а также с ролью правительств и выполнением их основополагающих обязанностей на международной арене. Управление Интернетом в международном праве является многогранной моделью, в сущность которой входит партнерство стран в данной сфере. Выявлена специфика механизма контроля за управлением Интернетом, которая была исторически заложена в тот момент, когда он только начал формироваться. Если рассматривать с одной стороны, то можно сказать, что Интернет зародился в рамках ММПО, с другой стороны, он