Научная статья
УДК 341:004.056
DOI 10.52070/2500-3488_2022_3_844_142

Международное право и его роль в обеспечении информационной безопасности и защите цифрового суверенитета России

Н. С. Грудинин

Московский государственный лингвистический университет, Москва, Россия
nekit-07@mail.ru

Аннотация. В статье анализируется роль и возможности международного права в обеспечении информационной безопасности стран, входящих в состав ООН и региональных интеграционных объединений. Сообщается, что современное международное право не способно в полной мере защитить право человека на свободу слова и информационную безопасность в глобальных масштабах, а может противодействовать лишь отдельным киберугрозам и вызовам, а также в некоторой степени киберпрступности и кибертерроризму.

Ключевые слова: международное право, информационная безопасность, киберугрозы, цифровой суверенитет государства

Для цитирования: Грудинин Н. С. Международное право и его роль в обеспечении информационной безопасности и защите цифрового суверенитета России // Вестник Московского государственного лингвистического университета. Образование и педагогические науки. 2022. Вып. 3(844). С. 142–148. DOI 10.52070/2500-3488_2022_3_844_142

Original article

International Law and Its Role in Information Security and Protecting the Digital Sovereignty of Russia

Nikita S. Grudinin

Moscow State Linguistic University, Moscow, Russia
nekit-07@mail.ru

Abstract. The article analyzes the role and potential of international law in the field of information security of the UN member states and regional integration associations. The author highlights the fact, that modern international law is not able to fully protect human right to freedom of speech and information security on the global scale, but can only counter certain cyber threats and challenges, as well as to some extent, cybercrime and cyberterrorism.

Keywords: international law, information security, cyber threats, a state's digital sovereignty

For citation: Grudinin, N. S. (2022). International law and its role in information security and protecting the digital sovereignty of Russia. Vestnik of Moscow State Linguistic University. Education and Teaching, 3(844), 142–148. 10.52070/2500-3488_2022_3_844_142

ВВЕДЕНИЕ

Ускоренное развитие цифровых технологий последних лет привело к серьезным изменениям системы международных отношений в начале XXI века. Процесс глобализации, включающий в себя активное применение информационно-коммуникационных технологий, которые нацелены на устойчивое развитие цивилизации, способствовал становлению международного информационного (цифрового) общества. Вместе с тем возникшие цифровые возможности привели к появлению не только положительных факторов в киберпространстве, но и к новым вызовам, которые несут в себе угрозу международной безопасности. В числе негативных последствий развития цифровых технологий находятся различные правонарушения, которые наносят вред не только отдельным гражданам, но и международным отношениям в целом. Трансграничный характер информации ставит перед международным сообществом вопрос о поиске механизма, который бы способствовал решению задачи по обеспечению информационной безопасности на универсальном, региональном и национальном уровнях.

Проблемы международной информационной безопасности составляют предмет непростых дискуссий как на национальном, так и на международном уровне в связи с открытыми вопросами о суверенитете государств в киберпространстве и появлении нового термина – цифрового суверенитета государств. Как известно, ежегодно сотни тысяч людей становятся жертвами мошеннических посягательств с использованием интернет-ресурсов. Международные террористические организации и преступные группы активно используют новые технологии для совершения преступлений, для легализации денежных средств, полученных преступным путем в результате торговли оружием, наркотическими средствами и психотропными веществами. Наконец, в последние годы Россия и ее граждане все чаще сталкиваются с вбросами заведомо ложной информации, преследующей цель дискредитации России и ее истории. Очевидно, что данные вызовы являются серьезной угрозой для информационной безопасности России и требуют детального осмысления.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И СОВРЕМЕННОЕ МЕЖДУНАРОДНОЕ ПРАВО

Интерес к информационной безопасности в международной сфере появился после окончания холодной войны. Сам термин «информационная безопасность» начал использоваться в контексте обеспечения безопасности компьютеров и компьютерных сетей и лишь через какое-то время стал включать в свое содержание не только технические, но и политические, социокультурные, экономические, психологические аспекты. Так, в Законе о кибербезопасности Европейского союза используется следующее определение: «Кибербезопасность означает деятельность, необходимую для защиты сетей и информации, пользователей информационных сетей и иных сторон, которые могут быть затронуты киберугрозами»[1].

Невозможно не согласиться с выводами П. А. Карасева, считающего, что сегодня в мире существует как минимум три вида угроз международной информационной безопасности. Во-первых, многие государства рассматривают информационно-коммуникационные технологии как средства для ведения войны, разведки, используют их в политических целях. Во-вторых, современные технологии активно используются террористами для совершения различного рода преступлений, обмена информацией, пропаганды экстремизма и для совершения нападений на другие организации или государства. В-третьих, периодически проводятся атаки на критические информационные инфраструктуры и системы преступными группами или хакерами-одиночками [Карасев, 2015]. В любом случае, права человека всегда оказываются под угрозой, что приводит к возникновению права конкретной личности на информационную безопасность.

Как подчеркивает А. В. Крутских, «с 1998 г. Россия продвигает идею налаживания международного сотрудничества по укреплению МИБ», причем с самого начала «работа по согласованию конкретных мер в интересах упрочения МИБ проводилась главным образом через механизм ООН» [Крутских, 2007, с. 28]. В этом процессе большое значение имеет вовлеченность в обсуждение проблем кибербезопасности главных органов ООН, а также вспомогательных органов и специализированных учреждений. Со времени своего основания ООН уделяет ключевое внимание вопросам повышения эффективности в области обеспечения международного мира и безопасности, закрепленным во множестве документов. Среди них Декларация об укреплении международной безопасности, принятая резолюцией Генеральной Ассамблеи ООН № 2734 (XXV) от 16 декабря 1970 г., Резолюция Генеральной Ассамблеи ООН № A/RES/3314 от 14 декабря 1974 г., Резолюция «Всеобъемлющий подход к укреплению международного мира и безопасности в соответствии с Уставом ООН» от 7 декабря 1988 г.

[1]Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019.

В 2005 году решением Генеральной Ассамблеи ООН была создана Группа правительственных экспертов по достижениям в сфере информатизации и телекоммуникации в контексте международной безопасности. Данная Группа сформулировала угрозы, риски и факторы уязвимости, связанные с обеспечением безопасности при использовании цифровых технологий. Группа также пришла к выводу, что международное право и, в частности, Устав ООН являются основой для поддержания мира и развития киберпространства, принимая во внимание такие аспекты, как открытость, безопасность, стабильность, доступность. Снижение рисков нарушения международного мира, безопасности и стабильности возможно путем согласования между государствами специальных стандартов и правил использования цифровых технологий.

Итогом активного развития электронной коммуникации в последние годы стало появление резолюции A/RES/73/266 от 22 декабря 2018 г. «Поощрение ответственного поведения государств в киберпространстве в контексте международной безопасности»[1]. Однако анализ данной резолюции дает основания полагать, что ее авторы не предлагают каких-либо конкретных норм или принципов по обеспечению информационной безопасности на универсальном уровне, но призывают государства и далее обмениваться информацией. Как отмечает, Т. Ю. Сидорова, авторы этой резолюции были не готовы сформулировать конкретные положения, которые можно было бы адресовать государствам в качестве правил поведения [Сидорова, 2020].

Невозможно не согласиться с тем, что ООН играет важную роль в деле институционализации отношений с применением информационно-коммуникационных технологий, но из-за стремительного их развития работа ООН не поспевает в отражении всех возникающих угроз в сфере обеспечения международной безопасности. Как справедливо отмечает С. А. Костин, в такую работу должны активно вовлекаться и продолжать ее межрегиональные и региональные организации [Костин, 2019].

Как известно, Комитет по киберзащите Североатлантического альянса (НАТО) занимает одно из ключевых мест в управлении и формировании политики в области киберзащиты. За техническую сторону кибербезопасности в НАТО отвечает Технический центр (NCIRC), который реагирует на любые инциденты и сообщает важную информацию по противодействию и снижению рисков международной информационной безопасности.

Европейский союз также не отстает в вопросе противодействия киберугрозам в информационном пространстве. Он тесно сотрудничает с НАТО в вопросе укрепления обороноспособности и обеспечения защиты, подписав Техническое соглашение о киберзащите в 2016 году. Исходя из того, что государство может одновременно являться и членом Европейского союза, и членом НАТО, можно сделать вывод о растущей заинтересованности в обеспечении информационной безопасности в мире и отдельных регионах не только военных блоков, но и экономических интеграционных объединений.

ОДКБ в 2016 году приняла Стратегию коллективной безопасности до 2025 года, в которой есть упоминание об информационной безопасности. Целью ОДКБ является обеспечение безопасности при участии всех членов ОДКБ на основе общепризнанных норм и принципов международного права. Но при этом ОДКБ не заинтересована в создании похожей интеграции, существующей между ЕС и НАТО, сотрудничество в рамках нее основано лишь на обмене информации между государствами, что существенно снижает уровень международной информационной безопасности.

Российская Федерация является одним из основных государств, заинтересованных в обеспечении международной безопасности. Однако прекращение сотрудничества России с НАТО является камнем преткновения во взаимодействии между НАТО и ОДКБ, приводит к мысли об отсрочке и существенном усложнении возможности появления взаимопонимания и вовлеченности в решение проблем кибербезопасности на евразийском пространстве.

В 2013 г. Парламентской ассамблеей ОБСЕ была принята Резолюция, ключевое внимание которой было направлено на «Стратегию кибербезопасности Европейского союза: открытое, безопасное и защищенное киберпространство». В Стратегии выделены принципы кибербезопасности, стратегические приоритеты и действия, в которых нашли свое отражение основные ценности ЕС, применяемые как в цифровом, так и в физическом мире. В обновленной Стратегии ЕС 2020 года был выделен ряд направлений деятельности в киберпространстве, учитывающий действия по защите основных прав, свободы выражения мнений, персональных данных и конфиденциальности, установления демократического управления с участием заинтересованных сторон.

Ранее, в 2009 году государства – члены ШОС пришли к единодушию в вопросах совместной деятельности в области обеспечения международной информационной безопасности. Подписанное ими межправительственное соглашение стало первым

[1]Резолюция ГА ООН от 22 декабря 2018 г. A/RES/73/266 от 22 декабря 2018 г. «Поощрение ответственного поведения государств в киберпространстве в контексте международной безопасности».

международным актом, цель которого – *отражение* и *предотвращение угроз* международной информационной безопасности, включая различные аспекты, такие как военно-политические, психологические и технические. В то же время страны БРИКС, среди которых Россия и Китай, отказались от подписания таких соглашений о сотрудничестве. Основой существующего разногласия является политико-идеологический аспект, так как некоторые страны, включая Россию, нередко обвиняются в проведении хакерских атак на другие государства.

Сегодня остается нерешенным и ряд других проблем в области обеспечения международной информационной безопасности. Одной из них является разрозненность подходов и единоличное принятие решений каждым из участников региональных интеграционных объединений по развитию того или иного направления информационной безопасности. Отсутствие единой международной конвенции ООН, в которой отражались бы основные понятия, виды угроз, цели, механизмы обеспечения защиты и их реализации, лишь увеличивает разрыв в понимании важности обеспечения информационной безопасности совместными усилиями государств. Другой причиной понятийного разрыва служит разрозненность в подходах к проблеме безопасности, что нередко приводит к восприятию права международной информационной безопасности как «мягкого права», не носящего обязывающего характера для всех государств.

Еще одной проблемой является стремление отдельных государств и, в первую очередь, США, занять монопольное положение в современном киберпространстве и навязывать свое видение мироустройства остальным государствам, что подрывает международную безопасность. Данный факт противоречит возможности эффективного взаимного сотрудничества и взаимодействия между государствами на универсальном уровне, а также оставляет свой след в деле охраны права человека на информационную безопасность, которое явно может пострадать из-за заведомо ложной информации вследствие тотального контроля сети Интернет и прекращения доступа к альтернативным СМИ, отражающим иные точки зрения, как правило, не выгодные американской военно-политической машине. Фактически, современное международное право не способно защитить право человека на свободу слова и информационную безопасность, а также не может противостоять информационной гегемонии США и стран НАТО. В настоящее время международное право только начинает испытывать потребность в создании универсальной платформы и механизмов для обеспечения информационной безопасности всех стран, входящих в ООН.

МЕЖДУНАРОДНО-ПРАВОВОЕ РЕГУЛИРОВАНИЕ БОРЬБЫ С КИБЕРУГРОЗАМИ

Российская Федерация в 1998 г. впервые привлекла внимание к киберугрозам, направив в ООН доктрину о мировой информационной безопасности. В 1999 г. ООН озвучила проблему обеспечения кибербезопасности в Резолюции A/RES/54/49 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», в которой главное внимание было сфокусировано на киберугрозах. С того времени ежегодно проводятся международные конференции и съезды для обсуждения программ по борьбе с опасностью в киберпространстве.

В сфере международной информационной безопасности сегодня можно выделить три вида наиболее критичных угроз: кибертерроризм, киберпреступность и кибервойны. Определение термину «кибертерроризм» было предложено в 2007 г. А. Колариком и Л. Занчевски: «кибертерроризм – это преднамеренная, политически мотивированная атака субнациональных группировок или иных злонамеренных агентов и индивидов против информации и компьютерных систем, компьютерных программ и данных, направленная против гражданских целей» [цит. по: Зиновьева, 2017, с. 108]. Стоит отметить, что ООН в своих документах не использует данный термин, употребляя вместо него возможность использования новых информационных инструментов террористическими организациями[1].

В сети Интернет террористы активно ведут пропагандистскую деятельность, обмениваются информацией с помощью теневых сайтов и так называемого Даркнета. Деятельность ИГИЛ (организация запрещена в России) в глобальном информационном обществе является показателем использования сети Интернет для распространения в открытых источниках видеороликов и фотографий с места боевых действий в целях устрашения мирного населения, разжигания вражды и ненависти. В 2020 году глава Контртеррористического управления ООН Владимир Воронков заявил, что данная террористическая группировка при помощи Интернета демонстрирует готовность совершать новые масштабные теракты по всему миру[2].

Подчеркнем, что борьба с кибертерроризмом не может осуществляться только при помощи

[1]Developments in the Field of Information and Telecommunications in the Context of International Security, UN document A/RES/63/37.

2ИГИЛ: ослаблены, но не побеждены. В Совбезе обсудили новый доклад Генерального секретаря. URL: https://news.un.org/ru/story/2020/02/1372102

односторонних действий. Россия не раз призывала решать проблему совместно, в рамках ООН, предлагая сотрудничество с международными региональными организациями, такими как СНГ, ШОС и ОДКБ. Тем не менее политические споры и разногласия становятся серьезной преградой для взаимодействия и координации действий в борьбе с терроризмом.

Характерной особенностью кибертерроризма является его масштаб, интенсивность, открытость и масштабные последствия. В свою очередь киберпреступность согласно позиции Управления ООН по наркотикам и преступности (2005) представляет собой поведение, которое влечет за собой преступные действия против конфиденциальности, целостности и доступности компьютерных данных или систем. На основе данного определения можно сделать вывод, что киберпреступление направлено зачастую на причинение ущерба отдельным членам общества или отдельным государствам. Особую значимость в рамках этой проблематики приобретают вопросы, связанные с обеспечением безопасности электронной торговли и электронных расчетов в сети Интернет.

Отдельно стоит выделить инициативу некоторых стран использовать технологию блокчейн, криптовалюту и цифровые валюты. Так, в 2018 году ООН запустила международную программу под названием «Цели устойчивого развития», в рамках которой подразделение Международного детского фонда ООН (ЮНИСЕФ) заявило, что начнет принимать пожертвования в виде криптовалют. Однако на международном уровне пока так и не создана нормативная база, которая бы могла стать основой системы противодействия преступной деятельности с использованием криптовалюты, что только создает новые риски эффективности применения международного права. Также в последнее время существенно возросла продажа скомпрометированных банковских карт, данные которых воруют с помощью фишинговых сайтов и банковских троянов.

Следует особо отметить, что единственным источником международного характера в данной сфере на текущий момент является Будапештская конвенция по борьбе с киберпреступностью 2001 года, принятая Советом Европы. Она констатирует, что международное сотрудничество в целях предотвращения, расследования и устранения киберпрестулений является одной ключевых задач данной Конвенции. Сложностью противодействия такой преступной деятельности является то, что она имеет трансграничный характер, и трудно оценить, где на самом деле имело место преступное деяние, поскольку данные могли быть загружены в одной стране, хостинг предоставлялся во второй стране, а жертва могла находиться в третьей стране, в то время как украденные данные были отправлены в четвертую юрисдикцию.

На текущий момент государства – участники Будапештской конвенции по борьбе с киберпреступностью определили современные технологии связи и обработки данных в борьбе с компьютерной киберпреступностью, особенно в связи с изначально транснациональным характером лежащей в их основе технологии. Однако данная Конвенция не предусмотрела сколь-нибудь надежных гарантий защиты от необоснованного вмешательства в национальное киберпространство с целью получения закрытых (секретных) данных. Иными словами, под предлогом противодействия киберугрозам и киберпреступности любое государство – участник Конвенции может получить доступ к закрытым данным других государств-участников. Безусловно, такая ситуация создает прямую угрозу нарушения цифрового суверенитета России, именно по этой причине наша страна так и не присоединилась к данной Конвенции. К тому же Будапештская конвенция отчасти устарела и не отражает всего многообразия существующих киберугроз. Очевидно, что к настоящему времени назрела необходимость принятия нового документа о борьбе с киберпреступностью на пространстве Совета Европы.

Необходимо отметить, что в сфере противодействия международной преступной деятельности с помощью информационных технологий уже существуют универсальные механизмы сотрудничества государств, которые заложены в рамках специализированных международных организаций, таких как Интерпол, Европол, Евроюст. При этом основную роль в осуществлении и совершенствовании правоохранительного межгосударственного сотрудничества играет Международная организация уголовной полиции (Интерпол), в рамках которой реализуются ключевые формы и направления международного сотрудничества, определяются тенденции и выявляются проблемы, связанные с расследованием киберпреступлений.

Тем не менее деятельность Интерпола ограничена, так как она предполагает регистрацию сведений о международных преступниках и преступлениях и проведение международных розысков. Такой сбор информации может быть малоэффективен в случае киберпреступлений, совершаемых за долю секунды, в связи с чем собранная информация может оказаться устаревшей при поиске преступника. Представляется, что эффективная и полноценная борьба с киберпреступностью должна осуществляться не только по линии Интерпола, но и посредством взаимодействия и обмена данными

о киберпреступниках между региональными интеграционными объединениями и государствами. Такая работа позволит повысить уровень взаимного доверия и сотрудничества государств, состоящих в различных интеграционных объединениях.

ЗАКЛЮЧЕНИЕ

Результаты проведенного исследования позволяют констатировать наличие нерешенной проблемы по международно-правовому обеспечению и регулированию информационной безопасности и сделать ряд выводов.

1. Современное международное право не способно защитить право человека на свободу слова и информационную безопасность, а также не может противостоять информационной гегемонии США и стран НАТО. В настоящее время международное право только начинает испытывать потребность в создании универсальной платформы и механизмов для обеспечения информационной безопасности всех стран, входящих в ООН. Международное сотрудничество государств основано на взаимном интересе в противодействии киберпреступности, кибертерроризму и киберугрозам, что сужает обеспечение информационной безопасности и устойчивости на глобальном уровне. Проблема обеспечения информационной безопасности связана с защитой национального цифрового суверенитета государств и не может быть успешно решена в случае его игнорирования. При этом цифровой суверенитет государства предполагает надежную защиту государства, общества и граждан от различного рода посягательств в цифровой сфере.

2. Современное сотрудничество государств в борьбе с киберугрозами осложняется различными подходами к данной проблеме, а также блоковым характером современного мира. Представляется, что успешная борьба с кибертеррористами невозможна без объединения усилий всего мирового сообщества. Представляется, что на международном уровне следует институализировать понятие «кибертерроризм», а также провести унификацию правовых норм в информационной сфере на региональном и универсальном уровнях. Необходимо также обсудить вопрос о принятии нового документа о борьбе с киберпреступностью на евразийском пространстве. В перспективе данный вопрос следует обсудить и на площадке ООН.

3. В целях справедливого наказания за преступления, совершенные с применением цифровых технологий, следует создать глобальную сеть международной информационной безопасности посредством специального международного договора между заинтересованными сторонами под эгидой Совета Безопасности ООН. Такая сеть позволит проводить поиск в компьютерных сетях, осуществляемый в одном государстве по запросу другого государства, обеспечит сбор и перехват данных о содержании передаваемой информации в режиме реального времени. При этом должно учитываться национальное законодательство страны-исполнителя запроса при выдаче той или иной информации, которая может быть использована для разжигания информационной войны или конфликта.

СПИСОК ИСТОЧНИКОВ

1. Карасев П. А. Политика безопасности США в глобальном информационном пространстве: дис. … канд. полит. наук. М., 2015.
2. Крутских А. В. К политико-правовым основаниям глобальной информационной безопасности // Международные процессы. 2007. Т. 5. № 1. С. 28–37.
3. Сидорова Т. Ю. Международная информационная безопасность: правовые аспекты и деятельность ООН // Сибирский юридический вестник. 2020. № 3. С. 103–108.
4. Костин С. А. Международно-правовое обеспечение коллективной безопасности – направление для сотрудничества и интеграции в Европе и на Евразийском пространстве // Международные отношения и общество. 2019. № 3. Т. 1. С. 41–50.
5. Зиновьева Е. С. Международное сотрудничество по обеспечению информационной безопасности: проблемы, субъекты, перспективы: дис. … д-ра полит. наук. М., 2017.

REFERENCES

1. Karasev, P. A. (2015). Politika bezopasnosti SShA v global'nom informatsionnom prostranstve: dis. … kand. polit. nauk = U.S. security policy in the global information space: PhD in Political Sciences. Moscow(In Russ.)
2. Krutskikh, A.V. (2017). On the political and legal foundations of global information security. International processes, 5(1), 28–37. (In Russ.)

3. Sidorova, T. Y. (2020). International information security: legal aspects and un activities. Siberian Legal Bulletin, 3(90), 103–108. (In Russ.)
4. Kostin, S. A. (2019). International legal provision of collective security – a direction for cooperation and integration in Europe and in the Eurasian space. International relations and society, 3(1), 41–50. (In Russ.)
5. Zinovieva, E. S. (2017). Mezhdunarodnoe sotrudnichestvo po obespecheniyu informatsionnoi bezopasnosti: problemy, sub"ekty, perspektivy = International cooperation in ensuring information security: problems, subjects, prospects: Senior Doctorate in Political Sciences. Moscow. (In Russ.)

ИНФОРМАЦИЯ ОБ АВТОРЕ

Грудинин Никита Сергеевич

кандидат юридических наук, доцент, доцент кафедры международного права
Московского государственного лингвистического университета

INFORMATION ABOUT THE AUTHOR

Grudinin Nikita Sergeevich

PhD (Law), Associate Professor, Associate Professor of the Department of International Law,
Moscow State Linguistic University,

Статья поступила в редакцию 01.04.2022
одобрена после рецензирования 15.04.2022
принята к публикации 10.06.2022

The article was submitted 01.04.2022
approved after reviewing 15.04.2022
accepted for publication 10.06.2022