DOI: 10.18372/2307-9061.55.14778
УДК 341+342(045)

Октай Эфендиев,
доктор юридических наук, профессор

Этибар Алиев,
доктор юридических наук, профессор

НЕКОТОРЫЕ АКТУАЛЬНЫЕ ПРОБЛЕМЫ МЕЖДУНАРОДНО-ПРАВОВОГО РЕГУЛИРОВАНИЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Азербайджанский государственный экономический университет
ул. Истиглалият, 6, AZ-1001, Баку, Азербайджан
Бакинский государственный университет
ул. Халилова, 23, AZ-1148, Баку, Азербайджан
E-mails: oktay001@rambler.ru, a-etibar@rambler.ru

Цель статьи: *рассмотреть основные проблемы и особенности регулирования международной информационной безопасности в условиях глобализации межгосударственных отношений.* ***Методы исследования:*** *были использованы общепринятые методы научного познания, такие как: аналитический, сравнительно-правовой, семантически-познавательный, системный, статистический и другие.* ***Результаты:*** *система международной информационной безопасности, по мнению авторов статьи, должна представлять собой совокупность международных и национальных институтов, призванных регулировать деятельность различных субъектов глобального информационного пространства.* ***Обсуждение:*** *отдельных вопросов формирования приемлемых для всех стран справедливых международных информационных правоотношений, имеющих важность как для Азербайджана, так и для становления нового информационного миропорядка.*

Ключевые слова: *Азербайджанская Республика; глобализация; международная всеобщая безопасность; информационное пространство; взаимовыгодное сотрудничество и партнёрство; информационно-коммуникационные технологии; средства массовой информации.*

Постановка проблемы и ее актуальность. Обеспечение информационной безопасности в современном мире становится глобальной проблемой, затрагивающей фундаментальные интересы и личности, и общества, и каждого отдельно взятого государства. Общепризнанно, квинтэссенцией этой проблемы является, главным образом, постоянно растущие угрозы как безопасности стран, так и личности, общества именно со стороны информационной сферы, развивающиеся опережающими темпами в сравнении со всеми остальными жизненно важными сферами общественного бытия. Характерно, что в настоящую эпоху эти методы и технологии обеспечения информационной безопасности отстают от темпов развития информационной сферы.

Другой особенностью является то, что информационная безопасность является одной из составных частей всеобщей международной безопасности, цель обеспечения которой, в конечном счёте – решение проблем, связанных с выработкой и реализацией, к примеру, различных правовых средств предотвращения войн и вооружённых конфликтов, нормальных межгосударственных отношений. А потому, в широком плане, очевидно, что весь нормативный материал современного международного права, в конечном счёте, предусматривает решение этих важнейших проблем.

Анализ последних исследований и публикаций. Вопросам информационной безопасности уделяли внимание в своих трудах А.В. Крутских, В.Б. Наумов, И.С. Мелюхин, В.А. Копылов и другие.

Цель статьи – анализ основных проблем и особенностей регулирования международной информационной безопасности в условиях глобализации межгосударственных отношений.

Изложение основного материала. В современной международно-правовой доктрине, хотя в теории и практике межгосударственных нет какой-либо единой или широко признанной концепции международной безопасности, однако можно констатировать наличие некоторых её разновидностей, как например, глобальная, национальная и некоторые другие, каждая из которых может подразумевать определённую систему или комплекс соответствующих политико-правовых отношений.

Что касается международной информационной безопасности, то под ней понимается такое состояние глобального информационного пространства, при котором охватывается особый комплекс социальных отношений, касающийся возможности нарушения не только прав личности, общества, но и прав государства в информационной сфере. Кроме этого, «информационная безопасность определяется как состояние защищенности личности, общества и государства и их интересов от угроз, деструктивных и иных негативных воздействий в информационном пространстве» [1].

Информационную безопасность можно понимать и как комплекс организационных и технических мер, принимаемых для обеспечения защиты, целостности, доступности и управляемости массивов информации. В рамках общей концепции безопасности государства информационная безопасность призвана обеспечивать связанное взаимодействие всех элементов системы.

Поэтому всеобщее межгосударственное противодействие недопустимости подобных противоправных нарушений, злоупотреблений должно осуществляться на основе соответствующих фундаментальных международно-правовых норм и принципов, при активном и взаимовыгодном сотрудничестве и партнёрстве современных государств, установления в интересах такого правового режима, который способствовал бы формированию такой системы.

В противном случае, например, противодействие серьёзным нарушениям и злоупотреблениям в киберпространстве на межгосударственном уровне должно способствовать выработке и инициировании не только обсуждение вопросов по регулированию проблем современной информационной безопасности, но и в выработке и принятии взаимоприемлемых, на справедливой, равноправной и взаимовыгодной основе, глобальных норм и правил. Важно, чтобы подобный подход к формированию этих нормативно-правовых положений, касающихся ответственного межгосударственного поведения в информационном пространстве, осуществлялся бы в соответствии с такими принципами, как неприменения силы, невмешательства во внутренние дела, уважения государственного суверенитета и другими общепризнанными принципами и нормами.

Любой другой подход к этой, одной из первостепенных глобальных проблем человечества, не будет эффективным, с точки зрения благоприятного решения международно-правового регулирования любых проблем обеспечения и защиты информационной безопасности государств, поскольку в серьёзную угрозу превратился, в частности, факт растущих масштабов высоко-развитых современных информационно-коммуникационных технологий (ИКТ).

В этой связи, неслучайно, что на последних сессиях Генеральной Ассамблеи ООН всё чаще ведётся полемика по таким проблемам, как например, о том, что из-за низкого, недостаточного уровня защищённости государств в цифровой сфере, необходимы новые, более конструктивные, меры для стабильного, их поступательного развития.

Это обстоятельство, в свою очередь, имеет первостепенное значение не только для обеспечения информационной безопасности, но также такое отсутствие препятствует поступлениям инвестиций в высокотехно-

логические области государств. Что, в конечном счёте, заложником отсутствия широко признанных международно-правовых стандартов поведения в цифровом информационном пространстве являются как научно-технический прогресс, в целом, так и сами высокоразвитые технологии, международные финансы, искусственный интеллект и т.д. [2].

Однако, несомненный научно-практический интерес представляет краткая история рассматриваемой проблемы, которая, в современном её понимании, берёт свое начало с принятия консенсусом документа ООН под названием «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности» от 4 декабря 1998 г. Этот документ, как справедливо отмечается, «…по существу, стал формальным началом создания совершенно нового международно-правового режима, субъектом которого стали информация, информационная технология и методы ее использования» [3].

Согласно этому основополагающему международно-правовому документу, члены ООН договорились содействовать рассмотрению на многостороннем уровне существующих и потенциальных угроз в сфере информационной безопасности, путей их устранения. В практическом плане и с учетом новизны вопроса государствам-членам ООН было предложено сформулировать свои собственные оценки угроз в данной сфере, дать определения таких основных понятий в области информационной безопасности, как «несанкционированное вмешательство» и «неправомерное использование информационных систем и ресурсов».

Следующий важный этап имел место в декабре 2000 г., когда на 55-ой сессии на Генассамблее ООН был представлен очередной доклад Генерального секретаря ООН «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности», в котором было предложено определение таких базовых терминов, как «информационное оружие», «информационная война» и «информационная безопасность».

Основная идея документа была сформулирована в положениях Принципа 1, согласно которому «деятельность каждого государства в информационном пространстве должна способствовать общему прогрессу и не противоречить задаче поддержания мировой стабильности и безопасности, интересам безопасности других государств, принципам неприменения силы, невмешательства во внутренние дела, уважения прав и свобод человека. При этом, однако, подчеркивалось, что право каждого на поиск, получение и распространение информации может быть ограничено законом в целях защиты безопасности каждого государства. Кроме того, все члены международного сообщества должны, в соответствии с Принципами, иметь равные права на защиту своих информационных ресурсов и критически важных структур от несанкционированного информационного вмешательства».

Наряду с этим, в документе были приведены определения и других понятий, основных угроз в сфере международной информационной безопасности, формулированы направления деятельности, которые могли бы способствовать созданию международно-правовой основы ограничения таких угроз. Кроме того, фиксировалось обязательство участников не прибегать к действиям в информационном пространстве, целью которых является нанесение ущерба информационным системам, процессам и ресурсам другого государства, его критически важным структурам, подрыв политической, экономической и социальной систем, массированная психологическая обработка населения с целью дестабилизации общества и государства, и др.

Принципиально важно, что проблематика международной информационной безопасности была закреплена за Первым комитетом Генеральной Ассамблеи ООН, что подчеркивало ее особый политический аспект, подтверждало ее непосредственную связь с общим состоянием международной безопасности.

Другим важным событием на пути создания международно-правового режима информационной безопасности явилось принятие Окинавской «Хартии глобального информационного

общества» (июль 2000 г.), в которой, по-существу, признавалось, так называемое «революционное воздействие информационно-коммуникационных технологий на все сферы жизнедеятельности общества».

Одновременно, в документе подчёркивалось: «…чтобы ИКТ служили достижению взаимодополняющих целей обеспечения устойчивого экономического роста, повышения общественного благосостояния, стимулирования социального согласия и полной реализации их потенциала в области укрепления демократии, транспарентного и ответственного управления международного мира и стабильности».

Особое внимание в Хартии уделялось не только поиску правовых решений проблемы информационного неравенства, но и доступности информационных технологий для людей в мире, - в качестве одного из основополагающих принципов. Поэтому, не случайно, уже тогда было принято считать, что международно-правовое регулирование Интернета и решение проблем информационной безопасности должно осуществляться комплексно соответствующими специализированными международными организациями в интересах, как скорейшего создания таких институтов, так и выработке необходимых международно-правовых норм в данной области.

В свете изложенного, нельзя не согласиться с В.Б. Наумовым, который предлагал следующие возможные пути решения проблемы юрисдикции использования Интернет: «В первую очередь, это международные договоры, определяющие статус международного информационного пространства и фиксирующие коллизионные нормы использования законодательства различных государств. Не панацеей, но временным выходом могут служить региональные многосторонние соглашения, а также двусторонние договоры о правовой помощи. В идеале необходима унификация норм национальных законодательств относительно использования Сети» [4].

Становился более очевидным тот факт, что уже в глобализирующихся условиях существования государств, ООН приобрела значение все более ведущей, приоритетной и безальтернативной Организации. Особенно это касается вопросов регулирования международно-правовых проблем, имеющих первостепенное значение для обеспечения информационной безопасности, а также выработке, принятии универсальных нормативно-правовых документов или кодекса, положений, и стандартов для формирования информационного мирового порядка.

Ясно, что для более эффективного такого регулирования первостепенное значение имеет необходимость закрепления их в цифровом пространстве ИКТ основополагающие принципы ООН, что, наиболее вероятно, исключит не только возможность любого вида и формы милитаризации современного информационного пространства государств, но и предотвратит его превращения в арену военно-политического противоборства. Вместе с тем, оно будет иметь принципиальное значение в вопросе использования ИКТ как инструмента давления, угроз, нанесения экономического ущерба, а также пропаганды идей террористической и экстремисткой идеологии создающих непосредственную опасность правам и свободам человека.

Как видно, проблемы регулирования и обеспечения информационной безопасности имеют не только международно-правовой, но и гуманитарный характер, поскольку могут возникнуть, в частности, в связи с бесконтрольным использованием и распространением персональных данных граждан, вторжением в их частную жизнь, клеветой и кражами личности.

Эти направления имеют существенное значение для каждого государства, тем более для вновь возникших стран, которые со дня образования, в своей деятельности постоянно уделять особое внимание проблемам международно-правового регулирования международной информационной безопасности. При этом, придавая первостепенное значение участию в обсуждении и принятии решений в интересах отстаивания собственных национальных интересов в международном информационном пространстве.

Характерно, что для нынешних субъектов международных отношений, независимо от формы их устройства, способа их возникновения, охрана национальных интересов имеет ключевое значение, как при вступлении их во взаимные информационные связи, так и в целом, в контексте развития межгосударственных торгово-экономических, политических, культурных и иных отношений. Что касается теорий этих отношений, то они, как известно, всесторонне анализируют реалии и тенденции развития мирового сообщества по различным направлениям, по различным аспектам межгосударственных, в том числе, информационных связей.

В интересах взаимовыгодного, равноправного сотрудничества и партнерства Азербайджан последовательно осуществляет и связывает национальные интересы с пересекающимися и сталкивающимися интересами государств мира, для получения международных гарантий своей независимости и безопасности, в том числе в информационной области. При этом наше государство, вместе с другими странами, в первую очередь, с Российской Федерацией [5], прилагает определённые усилия во многих направлениях развития своей информационной деятельности по обустройству международной информационной сферы.

Молодые, вновь образованные на постсоветском пространстве страны, в первую очередь, в рамках деятельности в ООН, придают важное значение, особенно, к проблеме не только применимости норм и принципов современного международного права к сфере использования ИКТ, но и конкретным проблемам и аспектам международной информационной безопасности. Так, серьезной угрозой для международного сообщества является также постоянный рост преступлений, совершаемых с использованием ИКТ [6].

Среди них, например, проблемы происхождения источников угроз в киберпространстве, необходимость более согласованной борьбы с киберпреступностью и кибертерроризмом, предупреждение конфликтов в информационном пространстве, за равноправный и справедливый миропорядок в цифровой сфере, при котором были бы защищены интересы всех стран вне зависимости от уровня их технологического развития, многие другие. Примечательно новые, молодые развивающиеся страны, в том числе и Азербайджан, безусловно, считают неприемлемыми любые международно-правовые концепции, допускающие возможность применения силы или препятствующих использованию ИТК исключительно в мирных целях. Особо акцентировалось внимание на необходимости соблюдения таких уставных принципов и норм, как суверенное равенство государств, неприменение силы или угрозы силой, невмешательство во внутренние дела государств, и др.

Другая особенность в вопросах регулирования проблем международной информационной безопасности заключается, в частности, в том, что существующие региональные международно-правовые механизмы, такие как Конвенция Совета Европы о киберпреступности 2001 г. (так называемая Будапештская конвенция) [7] уже не могут справиться с новыми рисками, вызовами и угрозами цифровых технологий в сфере ИКТ. Более того, данный документ буквально навязывается Западом мировому сообществу, в том числе постсоветским странам, как единственно возможный формат международного правового регулирования в сфере противодействия информационной преступности.

Однако, быстрорастущее развитие информационно-коммуникационных технологий, ставшее толчком для становления информационного общества как во всем мире, так и в странах, входящих в СНГ, неизбежно приводит к тому, что перед государствами встала новая задача – не только обеспечение информационной безопасности, но и потребность разработки и принятия новых международно-правовых документов, к примеру, универсальной Конвенции о сотрудничестве в сфере противодействия информационной преступности, или Конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях и других нормативно-правовых документов [8].

Что касается нашей страны, то она, в

соответствии со своими национальными интересами, в рамках СНГ, предпринимает соответствующие усилия в поиска справедливого, взаимовыгодного решения проблем международной безопасности в информационной сфере, старается быть в авангарде государств, борющихся за недопустимость использования ИТК в преступных и антигуманных целей. И это естественно, поскольку информационная среда, как широко известно, всегда и везде, оказывает активное влияние на состояние политической, экономической, военной и других составляющих национальной безопасности государств – участников СНГ. Благодаря существенным успехам дипломатической деятельности нашего государства, достижениям по реализации крупных энергетических проектов мирового значения, возрождению и укреплению отечественной экономики Азербайджанская Республика превратилась в стабильное, динамичное и лидирующее южно-кавказское государство с высоким авторитетом в мировом сообществе. Это обстоятельство и активизация переговорных процессов с заинтересованными сторонами свидетельствуют о значительных достижениях внешнеполитической деятельности Азербайджана и его миролюбивой дипломатии. Наше государство, как и другие постсоветские страны, отстаивая и защищая собственные национальные интересы и безопасность, в силу своего уникального географического и стратегического положения, объективно продолжает играть важную роль, как в мировых процессах, так и в общей системе современных международных отношений.

Для всех новых постсоветских развивающихся стран на информационное пространство представляет собой самостоятельную сферу их безопасности, в которой необходимо, как минимум, обеспечить а) защиту информационных ресурсов, систем их формирования, распространения и использования, информационной инфраструктуры, б) защиту сведений, составляющих государственные секреты и иную охраняемую информацию. С течением времени возрастающая роль информационной сферы стала очевидной, так как данный фактор общественной жизни во многом предопределяет перспективы успешного осуществления этих стран социально-политических и экономических преобразований.

Это обусловливается следующими основными обстоятельствами:

- в условиях реализации конституционных прав граждан на свободу экономической, информационной, интеллектуальной и иной деятельности существенно возрастают потребности социально активной части общества в расширении информационного взаимодействия как внутри СНГ, так и с внешним миром, иными межгосударственными образованиями;

- интенсивное развитие информационной инфраструктуры, и прежде всего информационно-телекоммуникационных систем, средств и системы связи, интеграция в мировое информационное пространство, а также информатизация всех сторон общественной жизни, деятельности государств существенно усилили зависимость эффективности функционирования политических систем от состояния информационной сферы;

- индустрия информатизации, телекоммуникации и связи, информационных услуг на современном этапе развития человечества является одной из наиболее динамично развивающихся сфер мировой экономики;

- информационная инфраструктура, информационные ресурсы все больше становятся ареной межгосударственной борьбы за мировое лидерство, достижение противоборствующими государствами определенных политических и экономических целей;

- индивидуальное, групповое и массовое сознание людей все больше зависят от деятельности средств массовой информации.

Принимая во внимание вышеизложенные обстоятельства, к основным национальным интересам государств – участников СНГ в информационной сфере следует отнести, к примеру, реализацию конституционных прав граждан на получение, хранение и распространение полной, достоверной и своевременной информации; формирование и поступательное развитие информационного общества СНГ; равноправное взаимодействие

стран – участниц СНГ в мировых информационных отношениях; эффективное информационное обеспечение государственной политики в рамках СНГ, и др.

Целью обеспечения безопасности государств - участников СНГ в информационной сфере является достижение информационного суверенитета как исключительного права в соответствии с национальным законодательством и нормами международного права.

Реализация этой цели неразрывно связана с другими задачами первостепенной важности: а) самостоятельным и независимым проведением внутренней и внешней государственной информационной деятельности; б) распоряжением собственными информационными ресурсами; в) формированием инфраструктуры национального информационного пространства, г) созданием условий для интеграции в мировое информационное пространство, д) соблюдением баланса интересов объектов безопасности для определения национальных интересов в информационной сфере, и др.

Всё это, как видно, предопределяет необходимость общих подходов стран - участниц СНГ к эффективному сотрудничеству и партнёрству в области правового регулирования современной информационной безопасности, которая достаточно многогранна и многоаспектна. А потому важно иметь соответствующие модельные законодательные акты, которые могли бы гармонизировать и упорядочить нормативно-правовую базу в рамках сотрудничества и партнёрства этой группы стран, а также систематизировать и кодифицировать их информационное законодательство с сугубо «информационными» нормами.

Подобный подход, на наш взгляд, способствовал бы решению одной из главных задач – обеспечить собственную, правомерную информационную безопасность посредством системы или комплекса норм конституционного, гражданского, административного и уголовного права [9].

Важно при этом создать не только условия для их взаимосвязи, но и для действенного и эффективного механизма правового обеспечения информационной безопасности посредством гармонизации информационного законодательства в интересах обеспечения информационной безопасности. Правомерная информатизация общества, будет способствовать как развитию международного информационного обмена, так и обеспечению безопасности информационных условий экономического и таможенного сотрудничества и партнёрства, стимулированию использования информационно-коммуникативных технологий в социальной и культурной сфере, и т.д.

Так или иначе, несмотря на высокоразвитые современные технологические разработки, формы и методы хранения и передачи информации, их применение повышенного внимания к международно-правовому регулированию информационной безопасности. Это естественно, поскольку, свою очередь, один факт – например, уничтожение информационных ресурсов. Их недоступность или несанкционированное использование вследствие нарушений информационной безопасности может вызвать серьёзные проблемы, как у государств, так и других слоёв общества. Учитывая данное обстоятельство, предпочтительно отметить следующие группы важнейших проблем современной информационной безопасности: а) политические, б) экономические и в) гуманитарные.

К политическим можно отнести проблемы информационной безопасности, возникающие из-за информационных войн, кибервойн и электронной разведки в интересах политических групп, компрометации государственной тайны, атак на информационные системы оборонных, транспортных и промышленных объектов, неполного информирования и дезинформации руководителей крупных учреждений.

Экономические – это проблемы информационной безопасности, возникающие в результате утечки, искажения и потери коммерческой и финансовой информации, краж брендов и интеллектуальной собственности, раскрытия информации о материальном положении граждан, промышленного шпионажа и распространения материалов, наносящих ущерб репутации компаний.

Гуманитарного характера – это проблемы информационной безопасности, возникающие в связи с бесконтрольным использованием и распространением персональных данных граждан, вторжениями в частную жизнь, клеветой и кражами личности.

Среди необходимых условий по надлежащему и эффективному решению каждой из этих проблем в области информационной безопасности, можно выделить как принятие необходимых и целесообразных действий государственной власти с заинтересованными лицами, так и согласованная деятельность национальных и международных органов, занимающихся противодействующих острыми нарушениям информационной безопасности и борьбой с киберпреступностью.

Однако, рассматривая гуманитарный аспект современной международной информационной безопасности, необходимо подчеркнуть, что одной из его важнейших правовых проблем (не только технического характера), является проблема ответственности за, например, противоправное распространение персональных данных граждан, что есть непосредственная угроза их конституционных прав и свобод. Это касается, в первую очередь, провайдеров, распространяющих экстремистские материалы, обычно, с помощью трансграничных информационно-телекоммуникационных сетей и технологий.

Появление и рост высокоразвитой информационной индустрии, а также активное использование информационных и телекоммуникационных технологий средствами массовой информации привело к созданию качественно нового источника информации – электронных СМИ, который объединил в себе черты теле- и радионовостей и газетных и журнальных публикаций.

Так или иначе, в современном мире, как на международном, так и на национальном уровне, всё больше внимания уделяется роли средств массовой информации (СМИ). Это необходимо, они, используя современные информационные технологии, могут не только быть мощным средством отражения общественного мнения, но и содействовать его созданию. Очевидно и их влияние на деятельность всех тех субъектов, кто задействован в гуманитарной сфере, например, международные, правительственные и основные неправительственные организации. Поэтому категорически важно, чтобы СМИ отчитывались, исчерпывающим образом, обо всех соответствующих элементах конкретной ситуации так, чтобы общественность смогла получить объективную и исчерпывающую картину.

Именно такой подход необходим, поскольку есть достаточно фактов, при подаче информации общественности, сознательного, злонамеренного её искажения, вызывающая разжигание национальной, расовой или религиозной нетерпимости и ненависти, что, в свою очередь, приводит к дискриминации, враждебности или насилию. Конкретно, такая отрицательная способность СМИ была систематически отмечена, как в зонах многочисленных, вооруженных конфликтов (и не только таковых), так и за их пределами. Подобная деятельность, безусловно, противоречит и идёт в очевидный разрез общепризнанным принципам и нормам современного международного права, хотя и совместима с другими международно-правовыми положениями: о свободе выражения мнения и свободой информации.

Наряду с этим, такое соотношение и «совместимость», рассматривается в современной правовой доктрине, как одно из острых и дискуссионных. Проблема усугубляется и тем, что в современную эпоху, к сожалению, правовой статус электронных СМИ еще не нашёл своего авторитетного определения ни в международном праве, ни на уровне национального законодательства государств, что может привести к многочисленным нарушениям в области прав и свобод человека. Несомненно, что данные проблемы требуют детального изучения с учётом международной практики, поскольку ущемление основополагающих прав на свободу выражения мнения и свободу информации может привести к весьма нежелательным последствиям.

Что касается деятельности информационных провайдеров, то наличие специального института их ответственности определено

многомерностью и техническим разнообразием информационно-правовых отношений, в которые они вступают. Особенностью их деятельности является тот факт, что провайдер не инициирует такое отношение, не занимается выбором содержания информации и выбором её получателя, т.е. фактически не влияет на её содержание. Его целью является хранение таковой только в пределах времени, определяемого техническими стандартами и протоколами для нужд передачи конкретной информации.

Поэтому можно отметить, что ответственность провайдеров носит ограниченный характер, поскольку базируется на том, что они имеют организационно-техническую возможность в любой момент времени воздействовать на информационные общественные отношения своих пользователей. Форма же воздействия может быть довольно разнообразной: от блокирования информационного обмена до информирования третьих лиц о содержании передаваемой информации. Можно также отметить, что, возложив полную ответственность за содержание информации в Сети на провайдера, данная проблема становится ещё более неразрешимой на основе общепринятых международно-правовых норм в информационной области.

Однако, с учётом вышеизложенных соображения, вполне правомерной является мнение И.С. Мелюхина, считающего, что: «…сетевые операторы обычно не могут привлекаться к ответственности за содержание, которое передаётся по сетям. Однако у них могут требовать на условиях выданных лицензий принять необходимые меры по отношению к клиентам, которые используют сети для передачи незаконного содержания» [10].

Вместе с тем, информационные посредники не освобождаются от ответственности за незамедлительное выполнение решений суда, а также предписаний прокуратуры по удалению или блокированию экстремистских материалов, содержащихся на сайте или других предписаний вышестоящих государственных органов. В обязанность провайдера входит также информирование лиц, размещающих информацию на его сайте, об ответственности за размещение экстремистских материалов, и в случае необходимости информировать органы исполнительной власти об имеющихся правонарушениях.

Таким образом, проблема ответственности провайдеров является актуальным не только для государственной политики, но и для всего мирового сообщества, поскольку это определено спецификой сети Интернет как единого мирового электронного информационного пространства. В этой связи примечательно мнение В.А. Копылова, утверждающего, что «…в Интернет отсутствуют географические и геополитические границы государств - участников ТИТС (трансграничных информационно-телекоммуникационных сетей), происходит «столкновение» и «ломка» национальных законодательств стран в этих сетях. На этой основе возникает проблема формирования нового международного информационного законодательства» [11].

Выводы. Так или иначе, проблематика международной информационной безопасности не ограничивается только вопросами защиты информационных систем и сетей – приоритетом государственной политики является, главным образом, защита интересов личности. Одновременно, следует подчеркнуть, что основной целью государственной политики любого современного государства в области международной информационной безопасности было и остаётся формирование приемлемой для всех всеобъемлющей системы международной информационной безопасности.

Эта система, по нашему мнению, должна представлять собой совокупность международных и национальных институтов, призванных регулировать деятельность различных субъектов глобального информационного пространства. Создание системы международной информационной безопасности призвано обеспечить эффективное противодействие угрозам стратегической стабильности и способствовать равноправному стратегическому партнерству в глобальном информационном пространстве.

Литература

1. Данное определение нашло свое закрепление в принятом в ноябре 2014 г. модельном законе Российской Федерации «Об информации, информатизации и обеспечении информационной безопасности».

2. См., например, документы 72 сессии ООН, сентябрь 2017 г.

3. Крутских А.В. Информационный вызов безопасности на рубеже XXI века. *Международная жизнь*. 1999. № 2. С. 48.

4. Наумов В.Б. Право и Интернет: Очерки теории и практики. Москва: Книжный дом «Университет», 2002. С. 16-17.

5. Так, в формате переговорного процесса в ООН по развитию и совершенствованию международной информационной сферы, большой научно-практический интерес представляет деятельность Группы правительственных экспертов (ГПЭ) по проблемам международной информационной безопасности. Ещё в 2015 г. эта Группа консенсусом приняла три подробных доклада, которые в качестве рекомендаций вынесли на рассмотрение международного сообщества нормы ответственного поведения государств в информационном пространстве.

6. Convention on Cybercrime. Будапешт, 23 ноября 2001 г. URL: http://conventions. coe.int.

7. Данные, представленные Генеральным секретарем ООН А. Гутерришем о растущем уровне киберпреступности: ежегодный ущерб от деятельности преступников в информационном пространстве достигает 1,5 трлн долл. См. доклад 2017 г., на 72 сессии Генассамблеи ООН. Документ ООН-А/72/1.

8. Проект «Конвенции об обеспечении международной информационной безопасности (концепция)», предложенный в качестве альтернативы Конвенции Совета Европы о киберпреступности. URL: http://www.scrf.gov.ru/documents/6/112.html (дата обращения: 10 янв. 2014 г.).

9. Постановление Межпарламентской Ассамблеи государств – участников СНГ от 23 ноября 2012 г. № 38-6. URL: http://www.iacis.ru/activities/documents/

10. Мелюхин И.С. Информационное общество: истоки, проблемы, тенденции развития. Москва: Изд-во МГУ, 1999. С. 18-19.

11. Копылов В.А. Информационное право. Москва: Изд-во «Юристъ», 2002. 235 с.

References

1. Dannoe opredelenie nashlo svoe zakreplenie v prinjatom v nojabre 2014 g. model'nom zakone Rossijskoj Federacii «Ob informacii, informatizacii i obespechenii informacionnoj bezopasnosti».

2. Sm., naprimer, dokumenty 72 sessii OON, sentjabr' 2017 g.

3. Krutskih A.V. Informacionnyj vyzov bezopasnosti na rubezhe XXI veka. *Mezhdunarodnaja zhizn'*. 1999. № 2. S. 48.

4. Naumov V.B. Pravo i Internet: Ocherki teorii i praktiki. Moskva: Knizhnyj dom «Universitet», 2002. S. 16-17.

5. Tak, v formate peregovornogo processa v OON po razvitiju i sovershenstvovaniju mezhdunarodnoj informacionnoj sfery, bol'shoj nauchno-prakticheskij interes predstavljaet dejatel'nost' Gruppy pravitel'stvennyh jekspertov (GPJe) po problemam mezhdunarodnoj informacionnoj bezopasnosti. Eshhjo v 2015 g. jeta Gruppa konsensusom prinjala tri podrobnyh doklada, kotorye v kachestve rekomendacij vynesli na rassmotrenie mezhdunarodnogo soobshhestva normy otvetstvennogo povedenija gosudarstv v informacionnom prostranstve.

6. Convention on Cybercrime. Budapesht, 23 nojabrja 2001 g. URL: http://conventions. coe.int.

7. Dannye, predstavlennye General'nym sekretarem OON A. Guterrishem o rastushhem urovne kiberprestupnosti: ezhegodnyj ushherb ot dejatel'nosti prestupnikov v informacionnom prostranstve dostigaet 1,5 trln doll. Sm. doklad 2017 g., na 72 sessii Genassamblei OON. Dokument OON-A/72/1.

8. Proekt «Konvencii ob obespechenii mezhdunarodnoj informacionnoj bezopasnosti (koncepcija)», predlozhennyj v kachestve al'ternativy Konvencii Soveta Evropy o kiberprestupnosti.
URL: http://www.scrf.gov.ru/documents/6/112.html (data obrashhenija: 10 janv. 2014 g.).

9. Postanovlenie Mezhparlamentskoj Assamblei

gosudarstv – uchastnikov SNG ot 23 nojabrja 2012 g. № 38-6. URL: http://www.iacis.ru/activities/documents/

10. Meljuhin I.S. Informacionnoe obshhestvo: istoki, problemy, tendencii razvitija. Moskva: Izd-vo MGU, 1999. S. 18-19.

11. Kopylov V.A. Informacionnoe pravo. Moskva: Izd-vo «Jurist'», 2002. 235 s.

Oktay Efendiev, Etibar Ali oglu Aliyev

SOME ACTUAL PROBLEMS OF THE INTERNATIONAL LEGAL REGULATION OF THE PROVISION OF INFORMATION SECURITY

Azerbaijan State Economic University
Istiglaliyat str., 6, AZ-1001, Baku, Azerbaijan
Baku State University
Khalilova str., 23, AZ-1148, Baku, Azerbaijan
E-mails: oktay001@rambler.ru, a-etibar@rambler.ru

The purpose of the article: *to consider the main problems and features of the regulation of international information security in the context of globalization of interstate relations.* ***Research methods:*** *generally accepted methods of scientific knowledge were used, such as: analytical, comparative legal, semantic-cognitive, systemic, statistical and others.* ***Results:*** *the system of international information security, according to the authors of the article, should be a combination of international and national institutions designed to regulate the activities of various subjects of the global information space.* ***Discussion:*** *of individual issues of forming acceptable for all countries fair international information legal relations, which are important both for Azerbaijan and for the establishment of a new information world order.*

Ensuring information security in the modern world is becoming a global problem affecting the fundamental interests of both individuals, society, and each individual state. It is generally recognized that the quintessence of this problem is mainly the constantly growing threats to both the security of countries and the individual, society precisely from the information sphere, developing at a faster pace in comparison with all other vital areas of social life. It is characteristic that in the present era, these methods and technologies for ensuring information security lag behind the pace of development of the information sphere.

Another feature is that information security is one of the components of global international security, the goal of which, ultimately, is to solve the problems associated with the development and implementation, for example, of various legal means to prevent wars and armed conflicts, normal interstate relations. And therefore, in a broad sense, it is obvious that all the normative material of modern international law, ultimately, provides for the solution of these most important problems.

Keywords: *Azerbaijan Republic; globalization; international universal security; information space; mutually beneficial cooperation and partnership; information and communication technologies; mass media.*