УДК 341.1/8:004

Международное регулирование мер укрепления доверия в использовании информационно-телекоммуникационных технологий

Мороз Н.О.
Белорусский государственный университет

В статье рассмотрены актуальные аспекты международного регулирования мер укрепления доверия в использовании информационно-телекоммуникационных технологий в контексте международной безопасности. Автором обосновывается особая важность таких мер не только для снижения политической напряженности или предупреждения международных споров, но и для дальнейшего прогрессивного развития международного права в сфере обеспечения международной информационной безопасности. В публикации выявлены особенности мер доверия, принимаемых как на универсальном, так региональном и межрегиональном уровнях.

Цель статьи – установить специфику международного регулирования мер по укреплению доверия в использовании информационно-телекоммуникационных технологий и разработать научно аргументированные предложения по его совершенствованию.

***Материал и методы.** В ходе проведения исследования подробно анализировались акты мягкого права, принятые в рамках ООН по вопросам принятия мер доверия, а также ответственного поведения государств в киберпространстве; рассматривались международные договоры и акты органов региональных международных организаций (ОДКБ, СНГ, ШОС, ОБСЕ, АСЕАН, Совета Европы, НАТО), содержащие положения, регламентирующие принятие мер доверия в использовании информационно-телекоммуникационных технологий. Научной основой для данного исследования стали как труды ученых Союзного государства, так и стран дальнего зарубежья, посвященные данной проблематике.*

***Результаты и их обсуждение.** Автором выявлена сущность мер доверия, принимаемых в сфере использования ИКТ; сформулированы предложения по совершенствованию принципов ответственного поведения государств в киберпространстве в части применения мер доверия, а также по использованию отдельных мер доверия в сфере использования ИКТ в условиях современной геополитической напряженности в межрегиональном контексте.*

***Заключение.** Перечень мер, разработанных ГПЭ, может быть дополнен заблаговременным предупреждением о киберучениях в целях снижения напряженности в сфере использования ИКТ, а также добровольным приглашением иностранных наблюдателей для ознакомления с деятельностью кибернетических подразделений вооруженных сил. Представляется перспективным принятие мер доверия по линии «региональная международная организация–третьи государства». Это позволит наладить диалог с государствами, проявляющими интерес к снижению политической напряженности в контексте информационной безопасности путем принятия мер доверия.*

***Ключевые слова:** информационная безопасность, международная информационная безопасность, меры доверия, информационно-коммуникационные технологии, предупреждение международных споров, предупреждение вооруженных конфликтов, международный политический диалог.*

International Regulation to Strengthen Confidence-Building Measures while Using Information and Telecommunication Technologies

Moroz N.O.
Belarusian State University

The article addresses topical aspects of international regulation of confidence-building measures in the use of information and telecommunication technologies in the context of international security. The author substantiates the particular importance of such measures not only for reducing political tensions or preventing international disputes, but also for the further progressive development of international law in the field of ensuring international information security. The article reveals the features of confidence-building measures taken both at the universal level and at the regional and interregional level.

The purpose of the article is to establish the specifics of international regulation of confidence-building measures in the use of information and telecommunication technologies and develop scientifically substantiated proposals for its improvement.

***Material and methods.** The research comprehensively analyzes soft law acts adopted within the UN on confidence-building measures, as well as the principles of responsible state behavior in cyberspace; international treaties and acts of bodies of regional international organizations (CSTO, CIS, SCO, OSCE, ASEAN, Council of Europe, NATO) containing provisions regulating the adoption of confidence-building measures in the use of information and telecommunication technologies. The scientific basis for this study includes both academic publications done at the Union State as well as other regions devoted to the issues researched.*

Findings and their discussion. *The author reveals the essence of confidence building measures taken in the field of ICT use. The proposals to improve the principles of responsible state behavior in cyberspace regarding confidence building measures, as well as the use of specific confidence building measures in the field of ICT use in the context of modern geopolitical tensions in the interregional context were formulated.*

Conclusion. *The list of measures developed by the GGE can be supplemented by an early warning about cyber exercises in order to reduce tensions in the use of ICT, as well as the voluntary invitation of foreign observers to get acquainted with the activities of the cyber units of the armed forces. Confidence-building measures along the lines of "regional international organization – third states" are recommended to be taken. This could facilitate a dialogue with the states interested in reducing political tensions in the context of information security through the adoption of confidence-building measures.*

Key words: *information security, international information security, confidence building measures, information and communication technologies, prevention of international disputes, prevention of armed conflicts, international political dialogue.*

Широкое использование информационно-коммуникационных технологий (далее – ИКТ) во всех сферах жизнедеятельности общества обусловило и рост числа противоправных деяний, совершаемых в киберпространстве. Так, уже в первом квартале 2023 г. количество кибератак возросло на 7% в сравнении с тем же периодом 2022 г. [1]. При этом такие кибероперации могут совершаться государствами, которые, как правило, не признают своей вовлеченности в их совершение [2, с. 401]. К примеру, единственной кибератакой, в совершении которой признали свое участие Соединенные Штаты Америки, стала операция «Сияющая симфония», целью которой было противодействие ИГИЛ [3]. В то же время представители государств нередко обвиняют другие государства в совершении кибератак и, более того, принимают односторонние принудительные меры в связи со злонамеренной деятельностью государств в киберпространстве [4, с. 9–10]. Учитывая сложности в определении источника инцидента в сфере ИКТ, ошибочная атрибуция такого акта способна привести к дестабилизирующим последствиям, в том числе к возникновению конфликта [5]. В этой связи особую важность приобретают меры укрепления доверия в вопросах использования ИКТ, принятие которых позволяет снизить политическую напряженность, может способствовать предупреждению международных споров или их разрешению.

Материал и методы. Нижеизложенные наблюдения построены на изучении международных договоров, а также актов мягкого права, принимаемых как в рамках ООН на региональном уровне, так и международных организаций регионального характера (ОДКБ, СНГ, ШОС, ОБСЕ, АСЕАН, Совета Европы, НАТО). Кроме того, научной базой для настоящего исследования стали труды ученых как Союзного государства, так и стран дальнего зарубежья, посвященные различным аспектам принятия мер доверия в интересах обеспечения международного мира и безопасности. Для анализа собранного материала были использованы общие методы научного познания (диалектический, индуктивный, дедуктивный), а также частно-научные методы, применяемые в юридических науках – метод сравнительного правоведения и формально-юридический метод.

Результаты и их обсуждение. Меры укрепления доверия в вопросах использования ИКТ хотя и чрезвычайно важны для целей обеспечения международной информационной безопасности, но не нашли достаточного отражения в доктрине международного права. В научных публикациях в основном затрагивались отдельные аспекты укрепления доверия в контексте работы Групп правительственных экспертов (далее – ГПЭ) по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности и Рабочей группы открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (далее – РГОС) (А.А. Даньелян, Е.Е. Гуляева, С.А. Костин, О.С. Макаров, О.О. Самоукин, А.В. Колосов и др.), либо роли международных организаций в укреплении международной информационной безопасности (М.А. Вус, О.С. Макаров, Г.И. Перекопский, М.М. Кучерявый, П.А. Агапов, М.А. Ефремова, Н.О. Мороз и др.). В то же время комплексный анализ эффективности мер укрепления доверия в вопросах использования ИКТ в научных работах не проводился.

Между тем принятие мер доверия в контексте информационной безопасности выходит за рамки предупреждения или улаживания конфликтов и ситуаций напряженности. Во-первых, возможность совершенствования международно-правового регулирования, а также реализация действующих норм мягкого права в области ответственного поведения государств в киберпространстве может быть связана с принятием мер доверия. Существующие различия подходов как к сущности самого понятия «информационная безопасность», так и к возможным направлениям

по ее обеспечению между ведущими державами мира, наряду с геополитическими противоречиями предопределяют необходимость принятия базовых мер доверия для поддержания диалога между всеми заинтересованными сторонами в интересах мира и устойчивого развития. Во-вторых, расширение спектра мер и объема оказываемой поддержки в рамках наращивания потенциала в области информационной безопасности в межрегиональном контексте также находится в зависимости от уровня мер доверия между государствами.

Таким образом, целью настоящего исследования является установление специфики международного регулирования мер по укреплению доверия в использовании информационно-телекоммуникационных технологий и разработка научно аргументированных предложений по его совершенствованию.

Меры укрепления доверия в вопросах использования ИКТ в контексте международной безопасности имеют значительную специфику. Современное международное право не дает определение термину «меры доверия». Более того, в разных контекстах это понятие может иметь разное значение. В доктрине также нет единого подхода к определению данного термина. В самом общем смысле меры доверия «представляют собой запланированные процедуры по предотвращению военных действий, предотвращению эскалации, снижению военной напряженности и укреплению взаимного доверия между государствами» [6].

Впервые меры доверия фактически стали применяться в Европе в 1913 г., когда получила распространение практика приглашения иностранных наблюдателей для наблюдения за военными учениями [7]. Вместе с тем сам термин «меры доверия» стал использоваться, как и сама концепция мер доверия, в период холодной войны в контексте контроля над вооружениями и разоружения в отношениях между СССР и США (1947–1991 гг.). В настоящее время конкретные вопросы принятия мер доверия регулируются в международных договорах, резолюциях Совета Безопасности ООН, актах мягкого права [8]. В то же время сущность, виды, порядок применения мер доверия в целом не регламентированы международным правом.

Группой правительственных экспертов ООН по мерам доверия по поручению Генеральной Ассамблеи ООН в 1981 г. был представлен доклад, содержащий Всеобъемлющее исследовании мер доверия (далее – Исследование), в котором была рассмотрена концепция мер доверия, цели их принятия, характеристика, эволюция, а также специфика имплементации. В данном документе был использован функциональный подход к определению сущности данного понятия (без формулирования конкретного определения через выяснение задач, которые призваны такие меры решать). Так, в частности, в Исследовании указывалось, что конечная цель принятия мер доверия – укрепление международного мира и безопасности, содействие укреплению доверия между государствами, лучшему пониманию и стабильным отношениям между государствами, таким образом, создание и улучшение условий для плодотворного международного сотрудничества. Иными словами, меры доверия ориентированы на содействие, уменьшение или в некоторых случаях даже устранение причин недоверия, страха, напряженности, враждебности <…> [9]. Следовательно, принятие мер доверия необходимо вне зависимости от наличия ситуации вооруженного конфликта или политической напряженности между государствами.

К важнейшим мерам доверия в данном документе причислены распространение и обмен относящейся к делу информации, а также осуществление регулярных контактов на всех уровнях политического и военного руководства (п. 30) [10]. В качестве иных мер доверия, используемых в военном контексте указаны: заблаговременное предупреждение о военных маневрах и учениях, обеспечение большей прозрачности военных бюджетов, стратегических доктрин, толкование норм национального законодательства, выделение «горячей линии» для обеспечения срочной коммуникации между главами государств на случай кризисной ситуации [11].

Это Исследование во многом было положено в основу Руководящих принципов для соответствующих типов мер доверия и их имплементации, представленных Комиссией по разоружению Генеральной Ассамблее ООН в 1988 г. В Руководящих принципах указывается, что конечной целью принятия мер доверия является укрепление международного мира и безопасности, внесение вклада по предупреждению всех войн, и в частности, ядерной (п. 2.2.1) [12]. При этом важной целью принятия таких мер выступает реализация общепризнанных принципов, главным образом, тех, которые закреплены в Уставе ООН (п. 2.2.3) [12]. Основной целью же выступает «уменьшение или даже устранение причин недоверия, страха, непонимания и неправильной

оценки соответствующей военной деятельности и намерений других государств, факторов, которые могут вызвать восприятие нарушения безопасности и предоставить основание для продолжения глобального и регионального наращивания вооружений (п. 2.2.5). К характеристикам мер доверия отнесены: длительность (п. 2.3.1), добровольность (п. 2.3.2), поступательность, измеримость и верификабельность (п. 2.3.3.), конкретность (п. 2.3.4), обмен информацией о вооруженных силах, вооружениях, соответствующей военной деятельности и верификации (п. 2.3.5), учет конкретной ситуации для принятия мер доверия (п. 2.3.6), ненанесение ущерба безопасности других государств и кумулятивного эффекта от принятия мер доверия (п. 2.3.7) [12].

Международно-правовое регулирование мер доверия в сфере использования ИКТ на универсальном уровне к настоящему времени включает резолюции Совета Безопасности ООН и охватывают обмен информацией, передовым опытом и специальными техническими знаниями по вопросам противодействия использования ИКТ в террористических целях (резолюции Совета Безопасности ООН 2617 от 30 декабря 2021 г., 2396 от 21 декабря 2017 г.).

Меры доверия специального характера в сфере использования ИКТ предусматриваются в целом ряде актов мягкого права. Перечень таких мер был разработан Группой правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, а также конкретизирован Рабочей группой открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. По справедливому замечанию российского исследователя А.В. Колосова, «в первую очередь мерой укрепления доверия в сфере обеспечения информационной безопасности должна стать деятельность самой Группы» [13, с. 129]. К настоящему времени можно выделить 15 мер доверия, которые могут быть обобщены следующим образом: обмен информацией и позициями относительно национальной практики в области кибербезопасности; создание двусторонних, региональных и многосторонних консультативных рамок для укрепления доверия; расширение обмена информацией между государствами об инцидентах, связанных с безопасностью ИКТ, обмен информацией и связь между национальными группами реагирования на компьютерные чрезвычайные ситуации (CERT), расширение сотрудничества для устранения инцидентов, которые могут повлиять на ИКТ или критически важную инфраструктуру, промышленные системы управления с поддержкой ИКТ; усовершенствование механизмов сотрудничества правоохранительных органов для сокращения числа инцидентов, которые в противном случае могли бы ошибочно истолкованы как враждебные действия государства; определение соответствующих контактных лиц на политическом и техническом уровнях для решения серьезных ИКТ-инцидентов и создание каталога таких контактов; разработка и поддержка механизмов и процессов для двусторонних, региональных, субрегиональных и многосторонних консультаций по мере необходимости, для укрепления доверия между государствами и сокращения риска неправильного восприятия, эскалации и конфликтов, которые могут возникнуть в результате инцидентов в области ИКТ [5].

Важно отметить, что участие в имплементации ряда мер доверия должны принимать не только государства, но и негосударственные акторы (частный сектор, гражданское общество, представители академической среды и др.) (например, участвуя в обмене информацией, обмене опытом и др.) [5].

Таким образом, меры доверия, разработанные в результате деятельности ГПЭ в основном охватывают налаживание диалога и, частично, обеспечение прозрачности позиции государств в области кибербезопасности. Спецификой рассмотренного выше перечня является отсутствие ограничивающих мер, а также мер, связанных с верификаций. Полагаем, что это обусловлено, во-первых, технической спецификой функционирования самих информационно-коммуникационных технологий. Представляется достаточно проблематичным использование традиционных ограничивающих мер (например, в виде создания зон ограниченного развертывания сил или удержание кибервойск государств на расстоянии друг от друга). Во-вторых, в отсутствие международного договора универсального характера, а также принятых Советом Безопасности мер доверия, обладающих характеристикой конкретности, как это указано в Руководящих принципах, принятие мер по верификации пока также фактически не представляется возможным. В то же время полагаем, что перечень мер, разработанных ГПЭ, может быть дополнен заблаговременным предупреждением о киберучениях в целях снижения напряженности в сфере использования ИКТ, а также добровольным приглашением иностранных наблюдателей

для ознакомления с деятельностью кибернетических подразделений вооруженных сил.

Следует отметить, что критерии эффективности принятия мер доверия пока не были разработаны ГПЭ и РГОС. Полагаем, что в рамках работы РГОС в течение ее мандата (2021–2025) годы такие критерии нуждаются в обсуждении (резолюция Генеральной Ассамблеи ООН 75/240 от 31 декабря 2020 г.). Считаем, что общие критерии эффективности, содержащиеся в Руководящих принципах, могут быть использованы и в контексте мер, принимаемых в сфере ИКТ. В то же время считаем, что специфика использования ИКТ, проблемы атрибуции деяний в киберпространстве и различие подходов к сущности информационной безопасности наряду с недостаточной готовностью государств, находящихся в состоянии политической конфронтации, к диалогу предопределяет необходимость обеспечения транспарентности и доступности тех положений законодательства в области информационной безопасности, которые определяют трактовку основных терминов, перечень основных угроз информационной безопасности, пределы государственного суверенитета в киберпространстве, а также внешнеполитическую позицию по поводу использования ИКТ в контексте международного мира и безопасности. Это может быть обеспечено: во-первых, путем добровольного информирования Генерального секретаря ООН и Института ООН по исследованию проблем разоружения о практике применения норм международного права в контексте использования ИКТ (предусмотрено Докладом ГПЭ 2015 г.); во-вторых, путем размещения на официальном сайте государственного органа соответствующих документов государства.

Так, Концепция информационной безопасности Республики Беларусь была переведена Министерством иностранных дел Республики Беларусь на английский язык и размещена на его официальном сайте наряду с разъяснением позиции Республики Беларусь относительно вопросов информационной безопасности. Данный подход является, несомненно, оправданным, обеспечивает прозрачность государственной политики Республики Беларусь в области информационной безопасности на внешнем контуре, и таким образом способствует повышению доверия в международных отношениях в контексте использования ИКТ и обеспечению международной информационной безопасности.

Еще одним актом, содержащим положения, направленные на принятие мер доверия в киберпространстве, является Парижский призыв к доверию и безопасности в киберпространстве, принятый на Парижском форуме мира в 2018 г. Спецификой данного документа является признание «ответственности основных субъектов частного сектора за то, чтобы развивать доверие, безопасность и стабильность в киберпространстве», необходимости частно-публичного партнерства для содействия доверию и безопасности в сфере использования ИКТ.

Меры доверия, закрепленные в международных договорах, являются обязательными для применения сторонами, и в настоящее время содержатся в региональных соглашениях в области информационной безопасности или международной информационной безопасности. Меры доверия в региональном контексте закреплены также и в актах мягкого права.

Анализируя сложившиеся региональные подходы к определению мер укрепления доверия в связи с использованием ИКТ, можно отметить, что они в основном также ориентированы на обмен информацией о национальном законодательстве, государственных органах и политике в области кибербезопасности, обмен информацией о кибериницидентах, функционирование совместной системы мониторинга киберугроз. В то же время нельзя не отметить, что в рамках региональных международных организаций сложилась некоторая специфика в части использования отдельных мер доверия в сфере использования ИКТ. Так, в рамках таких организаций предпринята попытка организации канала связи по вопросам кибербезопасности либо через предоставление возможности использовать существующие сети (Коммуникационная сеть ОБСЕ, поддерживаемая Центром предотвращения конфликтов Секретариата ОБСЕ для обмена информацией по поводу мер доверия), создание специальных каналов для онлайн-обмена информацией в режиме реального времени (АСЕАН), создание специальных координирующих структур (Рабочая группа по сотрудничеству и мерам доверия в киберпространстве ОАГ). В рамках АСЕАН организуются совместные дискуссии – учения о том, как предупредить инциденты, связанные с безопасностью и использованием ИКТ, которые становятся региональными проблемами безопасности [14]. Для СНГ характерна разработка программ сотрудничества в борьбе с преступлениями в сфере высоких технологий, что в том числе также выполняет роль укрепления доверия между государствами-членами этих региональных

международных организаций [15, с. 113]. В ОДКБ (в традиционном формате) и АСЕАН (в формате дискуссии) проводятся совместные учения в области кибербезопасности [14; 16]. В ОДКБ также осуществляется операция «ПРОКСИ». Таким образом, мероприятия, проводимые в рамках региональных международных организаций, и которые могут рассматриваться также в качестве мер доверия, довольно сильно отличаются. При этом как справедливо отмечает Х. Хиггинс, «перечень мер доверия, используемых в одном регионе, не может целиком заимствоваться другим регионом» в силу исторической, культурной и иной специфики, существующей в каждом регионе [14].

Поддержание диалога между международными организациями регионального характера – как одна из важнейших мер доверия – используется в отношениях ОДКБ–СНГ, ОДКБ–ШОС, ОДКБ–ОБСЕ, СНГ–ШОС, ШОС–АСЕАН, ЕС–НАТО, ЕС–Африканский союз, ЕС–ОАГ.

Идея налаживания межрегионального сотрудничества между межрегиональными международными организациями, государства-члены которых находятся в ситуации политической напряженности, не является новой, но ее реализация сталкивается со значительными затруднениями. Так, например, генеральный секретарь ОДКБ Н. Бордюжа еще в 2013 г. отмечал, что НАТО игнорирует все попытки ОДКБ начать диалог между организациями по общим вызовам безопасности [17]. В 2019 г. было проигнорировано открытое обращение к главам МИД НАТО с призывом создать механизм регулярных консультаций между секретариатами организаций по региональной и европейской безопасности [18]. К настоящему времени, к сожалению, ситуация не претерпела никаких изменений [19]. В таких условиях представляется перспективным принятие мер доверия по линии «региональная международная организация–третьи государства». Это позволит наладить диалог с государствами, проявляющими интерес к снижению политической напряженности в контексте информационной безопасности путем принятия мер доверия. Так, в приоритетах белорусского председательства в ОДКБ является эффективное позиционирование ОДКБ на внешнем контуре через развитие сотрудничества с международными организациями и третьими странами в целях соответствия эволюционирующим вызовам региональной и глобальной безопасности (в частности, с КНР и Индией) [20].

Заключение. На основании проведенного исследования представляется целесообразным сформулировать следующие выводы:

1. Выявлено, что в документах, закрепляющих принятия мер доверия в области ИКТ, в качестве базовой меры доверия выступает информационный обмен. В то же время полагаем, что до установления диалога между сторонами может использоваться обеспечение прозрачности государственной политики в области информационной безопасности на внешнем контуре через опубликование соответствующих базовых документов на английском языке на официальных Интернет-ресурсах компетентных органов государств.

2. Считаем, что перечень мер, разработанных ГПЭ, может быть в будущем в рамках работы РГОС дополнен заблаговременным предупреждением о киберучениях в целях снижения напряженности в сфере использования ИКТ, а также добровольным приглашением иностранных наблюдателей для ознакомления с деятельностью кибернетических подразделений вооруженных сил.

3. Установлено, что в условиях недостаточной готовности международных организаций, государства-члены которых находятся в состоянии политической конфронтации, представляется перспективным принятие мер доверия по линии «региональная международная организация–третьи государства», что позволит наладить диалог с государствами, проявляющими интерес к снижению политической напряженности и предупреждению конфликтов, порождаемых недостатком межгосударственного доверия в области использования ИКТ в контексте информационной безопасности.

Литература

1. Mascellino, A. Global Cyber Attacks Rise by 7% in Q1 2023 [Electronic resource] / A. Mascellino // Infosecurity magazine. – Mode of access: https://www.infosecurity-magazine.com/news/global-cyber-attacks-rise-7-q1-2023/. – Date of access: 12.05.2023.

2. Brown, J.M. #SorryNotSorry: Why states neither confirm nor deny responsibility for cyber operations / J.M. Brown, T.M. Fazal // European Journal of International Security. – 2021. – Vol. 6, iss. 4. – P. 401–417.

3. Bloxberg, D. Cyber Warfare: Nation State Sponsored Cyber Attacks [Electronic resource] / D. Bloxberg // A10. – Mode of access: https://www.a10networks.com/blog/cyber-warfare-nation-state-sponsored-cyber-attacks/. – Date of access: 15.05.2023.

4. Довгань, Е.Ф. Теория и практика введения санкций за злонамеренную деятельность в информационном пространстве / Е.Ф. Довгань // Журн. междунар. права и междунар. отношений. – 2022. – № 1–2 (100–101). – С. 9–18.

5. Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности [Электронный

ресурс]. – 2015. – A/70/174 // Организация Объединенных Наций. – Режим доступа: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/228/37/PDF/N1522837.pdf?OpenElement. – Дата доступа: 12.11.2022.

6. Lachowski, Z. Confidence-Building Measures [Electronic resource] / Z. Lachowski / SIPRI. – Mode of access: https://www.sipri.org/sites/default/files/files/RR/SIPRIRR18.pdf. – Date of access: 12.07.2023.

7. Military Confidence-building [Electronic resource] / United Nations Office for Disarmament Affairs. – Mode of access: https://disarmament.unoda.org/cbms/. – Date of access: 22.06.2023.

8. Ge, J. A Review of U.S.-USSR Confidence-Building Measures During the Cold War [Electronic resource] / J. Ge // CSIS. Interpret : China. – Mode of access: https://interpret.csis.org/translations/a-review-of-u-s-ussr-confidence-building-measures-during-the-cold-war/. – Date of access: 05.05.2023.

9. Robinson, J. The Role of Transparency and Confidence-Building Measures in Advancing Space Security [Electronic resource] / J. Robinson // European Space Policy Institute. – Mode of access: https://www.files.ethz.ch/isn/124827/ESPI_Report_28_online.pdf – Date of access: 05.05.2023.

10. Comprehensive Study on Confidence-Building Measures A/36/474, 1982 [Electronic resource]: Report of the Secretary General / UN i-Library. – Mode of access: https://www.un-ilibrary.org/content/books/9789210585125/read. – Date of access: 22.06.2023.

11.Overview of existing confidence building measures as applied to cyberspace [Electronic resource] / Cybil. – Mode of access: https://cybilportal.org/wp-content/uploads/2020/05/GFCE-CBMs-final.pdf. – Date of access: 02.07.2023.

12. Guidelines for appropriate types of confidence-building measures and for their implementation, Special report of the Disarmament Commission to the General Assembly at its third special session devoted to disarmament, A/S-15/3*, 28 May 1988 [Electronic resource] / United Nations. Digital library – Mode of access: https://digitallibrary.un.org/record/39665. – Date of access: 22.07.2023

13. Колосов, А.В. Меры укрепления доверия в сфере информационной безопасности / А.В. Колосов // Сиб. юрид. вестн. – 2001. – № 2(93). – С. 125–130.

14. Higgins, H. Applying confidence-building measures in a regional context [Electronic resource] / H. Higgins // Institute for Science and International Security. – Mode of access: https://isis-online.org/uploads/conferences/documents/higginspaper.pdf. – Date of access: 15.07.2023.

15. Мороз, Н.О. Международно-правовое сотрудничество в борьбе с преступностью в сфере высоких технологий: монография / Н.О. Мороз. – Минск: Междунар. ун-т «МИТСО», 2017. – 266 с.

16. ДОСЬЕ: К 30-летию Договора о коллективной безопасности [Электронный ресурс] / Белта. – Режим доступа: https://www.belta.by/society/view/dose-k-30-letiju-dogovora-o-kollektivnoj-bezopasnosti-501907-2022/. – Дата доступа: 10.08.2023.

17. Дубровин, Д. НАТО игнорирует все попытки ОДКБ начать диалог по общим вызовам безопасности, заявил Николай Бордюжа, подводя итоги визита в Брюссель [Электронный ресурс] / Д. Дубровин. – Режим доступа: https://odkb-csto.org/news/smi/nato_ignoriruet_vse_popytki_odkb_nachat_dialog_po_obshchim_vyzovam_bezopasnosti_zayavil_nikolay_bord/#loaded. – Дата доступа: 15.07.2023.

18. И.о. генсека ОДКБ призвал НАТО ответить на предложение об установлении диалога [Электронный ресурс] / ТАСС. – Режим доступа: https://tass.ru/mezhdunarodnaya-panorama/6928446. – Дата доступа: 15.07.2023.

19. Коренев, Е. Модернизация ОДКБ: Главные интриги председательства Беларуси в 2023 году [Электронный ресурс] / Е. Коренев // Евразия эксперт. – Режим доступа: https://eurasia.expert/modernizatsiya-odkb-glavnye-intrigi-predsedatelstva-belarusi-v-2023-godu/. – Дата доступа: 15.07.2023.

20. Организация Договора о коллективной безопасности / Мин-во иностранных дел Респ. Беларусь. – Режим доступа: https://mfa.gov.by/mulateral/organization/list/eedc372b31f45ff8.html. – Дата доступа: 10.08.2023.

Поступила в редакцию 06.09.2023