Научная специальность
12.00.10 «Международное право; Европейское право»

УДК 341.1/8
DOI https://doi.org/10.26516/2071-8136.2021.2.125

МЕРЫ УКРЕПЛЕНИЯ ДОВЕРИЯ В СФЕРЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КАК ОСНОВА МЕЖДУНАРОДНОГО СОТРУДНИЧЕСТВА

© **Колосов А. В., 2021**
Иркутский государственный университет, г. Иркутск, Россия

Статья является продолжением исследований, результаты которых были опубликованы ранее в журнале «Сибирский юридический вестник» (2021, № 1). Исследованы особенности мер укрепления доверия в сфере обеспечения информационной безопасности. Отмечается, что международный мир и безопасность имеют глобальное значение в современных условиях и одним из видов обеспечения стабильности международных отношений является равноправное партнерство государств на основе общепризнанных принципов и норм международного права. Проанализирован актуальный вопрос международного права – создание мер укрепления доверия в сфере обеспечения информационной безопасности. Особое внимание уделено анализу международно-правовой основы сотрудничества в информационных отношениях. Изучены деятельность Рабочей группы открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности и одно из важнейших достижений Рабочей группы – Итоговый доклад от 12 марта 2021 г. Установлено, что возможности современных технических устройств постоянно расширяются и эволюционируют, подобного рода технологии могут быть использованы злоумышленниками с целью сделать общество более уязвимым и создать масштабные отрицательные последствия для большинства стран, поэтому ни одно государство не защищено от возможных угроз. Утверждается, что для решения подобных проблем необходимо предпринимать общие усилия со стороны всех стран для укрепления взаимного сотрудничества и достижения масштабных результатов в области создания безопасной информационной среды. Сделан вывод о том, что одной из форм сотрудничества государств являются меры укрепления доверия в сфере обеспечения информационной безопасности (confidence-building measures). Предложена классификация мер и сделан вывод о фундаментальном значении мер для успешного сотрудничества государств в целях обеспечения международной информационной безопасности каждого государства.

Ключевые слова: меры укрепления доверия, информационная безопасность, Рабочая группа открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, киберполитика, кибербезопасность.

На протяжении всей мировой истории государства стремились обеспечить стабильный мир и безопасность, основанную на выполнении принципов и норм международного права всеми участниками международных отношений.

В процессе сотрудничества у государств возникает объективная необходимость взаимодействия в различных областях с целью поддержания всеобщего мира и безопасности. Однако при реализации различных форм сотрудничества у субъектов международного права могут возникнуть взаимные недопонимания и разногласия, что, возможно, ухудшит отношения между ними и создаст угрозу их безопасности.

В этой связи в международном праве сравнительно недавно появился новый элемент системы безопасности – меры укрепления доверия.

Меры укрепления доверия направлены на предупреждение возникающих осложнений во взаимоотношениях субъектов международного права, установление доверительных взаимосвязей и углубление сотрудничества между ними.

Понятие «меры укрепления доверия» было установлено Заключительным актом Совета по безопасности и сотрудничеству в Европе 1975 г.,[1] предусматривающим необходимость уведомления государствами друг друга о любых крупномасштабных военных учениях, взаимный обмен наблюдателями для присутствия на военных учениях, организацию военных делегаций и т. п.

Также существуют и иные международно-правовые акты, регулирующие вопросы мер укрепления доверия. Например, Итого-

[1] Заключительный акт Совета по безопасности и сотрудничеству в Европе 1975 г. // Ведомости Верховного Совета СССР. 1975. № 33.

вый документ Стокгольмской конференции по мерам укрепления доверия и безопасности и разоружению в Европе 1986 г.[1], двусторонние соглашения между СССР и США о мерах по уменьшению опасности возникновения ядерной войны 1971 г.[2], о предотвращении ядерной войны 1973 г.[3] и другие акты.

Однако указанные международно-правовые акты не содержат нормативного определения термина «меры укрепления доверия». Поэтому данный пробел восполняется разнообразными доктринальными толкованиями.

Так, А. Н. Вылегжанин отмечает, что меры укрепления доверия – это меры, направленные на укрепление сотрудничества, снижение напряженности, предотвращение внезапных действий с применением различных видов оружия [1, с. 619].

По мнению Ю. М. Колосова и Э. С. Кривчиковой, меры укрепления доверия – это специальные организационно-технические меры, направленные на достижение взаимопонимания, уменьшение военного противостояния, предотвращение внезапного нападения или несанкционированного конфликта, в том числе ядерного [4, с. 444].

Меры укрепления доверия, как считают Г. В. Игнатенко и О. И. Тиунов, представляют собой совокупность норм, регламентирующих военную деятельность государств посредством установления мер информационного и контрольного характера с целью достижения взаимопонимания, предотвращения внезапного нападения или несанкционированного конфликта, а также обеспечения процесса разоружения [3, с. 477].

Исходя из анализа вышеперечисленных определений, можно прийти к выводу, что меры укрепления доверия относятся в большей степени к военной сфере и преследуют цель – снятие военной напряженности, противостояния и установление взаимопонимания между участниками международных отношений.

Подобная трактовка рассматриваемого понятия в современных условиях требует уточнения. Сегодня решение проблем мирного сосуществования государств требует комплексного подхода не только в военной сфере, но и в иных областях.

В настоящее время информационный аспект при реализации мер укрепления доверия является одним из основных, что побуждает государства к взаимной открытости в различных информационных сферах, обмену информацией по разнообразным вопросам с целью укрепления международного мира с соблюдением мер в сфере обеспечения международной информационной безопасности.

Современное общество характеризуется активным развитием информационных процессов, постоянным обменом информацией различного рода с целью обеспечения экономического подъема, укрепления политической стабильности, становлением гражданского общества и демократии. Расширение и распространение информационных связей государств, внедрение новых технологий и создание новых технических устройств остро обозначили существующие проблемы правового регулирования данных областей и обеспечения информационной безопасности. Данная проблема приобрела особую актуальность в период распространения коронавирусной инфекции, когда страны оказались в изоляции, а отдельные отрасли экономики, культуры, образования, науки перешли в дистанционный формат работы.

Потенциальная возможность утечки данных, незаконное использование информации или недружелюбное информационное воздействие на других субъектов международного права становится одним из главных вопросов в свете обеспечения безопасности участников международных отношений.

Все это привело к осознанию факта, что неправомерное использование информационно-коммуникационных технологий может представлять угрозу для международной информационной безопасности, мира, стабильности стран, а также повлечь нарушение прав и свобод граждан.

Таким образом, проблема международной информационной безопасности приобретает все большую значимость и требует тщательного изучения.

Под международной информационной безопасностью отдельные ученые понимают состояние глобального информационного пространства, при котором исключены возможности нарушения прав личности, общества и государства в информационной сфере, а также деструктивного и противоправного воздействия

[1] Итоговый документ Стокгольмской конференции по мерам укрепления доверия и безопасности и разоружению в Европе 1986 г. // URL: https://www.osce.org/files/f/documents/a/f/41242.pdf (дата обращения: 26.04.2021).

[2] Соглашение о мерах по уменьшению опасности возникновения ядерной войны между Союзом Советских Социалистических Республик и Соединенными Штатами Америки. Заключено в г. Вашингтоне 30 сентября 1971 г. URL: https://docs.cntd.ru/document/901764297 (дата обращения: 26.04.2021).

[3] Соглашение о между Союзом Советских Социалистических Республик и Соединенными Штатами Америки о предотвращении ядерной войны. Заключено в г. Вашингтоне 22 июня 1973 г. URL: https://docs.cntd.ru/document/901865688 (дата обращения: 26.04.2021).

на элементы национальной критической информационной инфраструктуры [6, с. 25].

Как видно из приведенного определения, ключевым моментом обеспечения информационной безопасности являются меры, направленные на охрану личности, общества и государства. В государствах создаются специальные программы и стратегии с целью обеспечения подобной безопасности.

В Российской Федерации действует Доктрина информационной безопасности, утвержденная Указом Президента РФ от 5 декабря 2016 г., которая устанавливает, что информационная безопасность Российской Федерации – это состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства[1].

Следует обратить внимание, что Российская Федерация в соответствии с вышеназванной Доктриной содействует формированию системы международной информационной безопасности. Этот момент представляется весьма принципиальным и крайне важным.

26 марта 2021 г. Президентом РФ было проведено заседание Совета безопасности, в ходе которого рассматривался проект основ государственной политики Российской Федерации в области международной информационной безопасности (далее – Основы).

Президент России обратил внимание на необходимость налаживания механизмов практического сотрудничества в обеспечении безопасности глобальной информационной сферы путем обмена опытом, совместного реагирования на компьютерные инциденты, подготовки кадров и проведения научных исследований[2].

12 апреля 2021 г. Основы были утверждены Указом Президента РФ № 213[3].

К одному из направлений реализации государственной политики в области международной информационной безопасности в Основах отнесена выработка на глобальном, региональном, многостороннем и двустороннем уровнях мер укрепления доверия в области противодействия использованию информационно-коммуникационных технологий для осуществления в глобальном информационном пространстве действий, представляющих угрозу международному миру, безопасности и стабильности.

Как справедливо отмечают Н. А. Молчанов и Е. К. Матевосова, целесообразно «согласование и закрепление общих, унифицированных глобальных мер, которые должны "вплетаться" в государственную внутреннюю и внешнюю политику каждого государства» [5, с. 138].

Решение глобальных проблем в информационной сфере требует совместных усилий и объединения мирового сообщества в борьбе с попытками применения современных устройств и технологий во вред международному миру и безопасности. Организация Объединенных Наций (далее – ООН) должна стать форумом для выработки общих принципов, правил и особенностей их применения в информационной среде для обеспечения информационной безопасности всех участников международных отношений.

Как обоснованно указывают некоторые авторы, подобные правоотношения характеризуются повышенной сложностью и координатором в купировании общих угроз должна выступить универсальная международная организация – ООН [2, с. 137].

Одним из первых документов, посвященных международной информационной безопасности, является Резолюция Генеральной Ассамблеи ООН «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» от 4 января 1999 г.,[4] которая призвала всех членов ООН к совместному сотрудничеству в борьбе с разнообразными угрозами в информационной среде.

В дальнейшем были приняты и иные резолюции по обеспечению международной информационной безопасности. Например, Резолюция «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» от 5 декабря 2018 г.[5], Резолюция «Поощрение ответственного поведения государств в киберпространстве в контексте международной безопасности» от 22 декабря

[1] Об утверждении Доктрины информационной безопасности Российской Федерации : указ Президента РФ от 5 декабря 2016 г. № 646 // Собр. законодательства РФ. 2016. № 50. Ст. 7074.

[2] URL: http://www.kremlin.ru/events/president/news/65231 (дата обращения: 26.04.2021).

[3] Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности : указ Президента РФ от 12 апреля 2021 г. № 213 // официальный интернет-портал правовой информации. URL: http://pravo.gov.ru (дата обращения: 26.04.2021).

[4] Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности: Резолюция Генеральной Ассамблеи ООН от 4 января 1999 г. URL: https://www.un.org/ru/development/ict/res.shtml (дата обращения: 26.04.2021).

[5] Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности: Резолюция Генеральной Ассамблеи ООН от 5 декабря 2018 г. URL: https://www.un.org/ru/ga/73/docs/73res1.shtml (дата обращения: 26.04.2021).

2018 г.[1] Также были одобрены и иные документы ООН, которые составили основу будущего сотрудничества государств и иных субъектов международного права.

Поиск путей решения проблем в области международной информационной безопасности привел к созданию в рамках ООН особых структур. В 2004 г. появилась Группа правительственных экспертов ООН в сфере информационно-коммуникационных технологий. Несмотря на противоречия, возникающие среди участников во время работы Группы, были подготовлены доклады, в которых содержались фундаментальные положения, ставшие базой для развития дальнейших форм сотрудничества государств. Особо хотелось бы отметить результат работы Группы 4-го созыва, которая приступила к работе в 2014 г. Итогом работы стало предложение создать Кодекс ответственного поведения государств в Сети в сфере обеспечения международной информационной безопасности.

В 2018 г. по инициативе России была создана Рабочая группа открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (далее – Рабочая группа).

Одним из важнейших достижений Рабочей группы стало принятие 12 марта 2021 г. итогового доклада. Во вступительной части доклада отмечается, что «сегодня как никогда очевидна насущная необходимость создания и поддержания доверия и безопасности в цифровой среде. Негативные тенденции в сфере цифровых технологий могут подорвать международную безопасность и стабильность, негативно сказаться на экономическом росте и устойчивом развитии и помешать полному осуществлению прав человека и основных свобод»[2].

Информационно-коммуникационные технологии потенциально могут быть использованы со злым умыслом, что непременно отразится на международной безопасности, стабильности стран и негативно повлияет на права и свободы человека. Возможности современных технических устройств постоянно расширяются и эволюционируют, подобного рода технологии могут быть использованы злоумышленниками с целью сделать общество более уязвимым и создать масштабные отрицательные последствия для большинства стран, потому ни одно государство не защищено от возможных угроз.

Как отмечается в докладе, для решения подобных проблем необходимо прилагать общие усилия со стороны всех стран для укрепления взаимного сотрудничества и достижения масштабных результатов в области создания безопасной информационной среды. Необходимо обеспечить сокращение цифровых различий стран и создать условия для расширения доступа всех к информационно-коммуникационным технологиям. Подобные предложения Рабочей группы связаны с тем, что угрозы, возникающие в информационном пространстве, могут оказывать разное воздействие на различные группы субъектов, таких как молодежь, пожилые люди, представители отдельных профессий, женщины, мужчины и т. п. В этой связи была отмечена необходимость дальнейшего укрепления сотрудничества с гражданским обществом, частным сектором, научными кругами и техническим сообществом.

В целях предотвращения опасных и конфликтных ситуаций Рабочая группа подчеркивает необходимость соблюдения свода правил, норм и принципов ответственного поведения государств в информационном пространстве. Данные добровольные правила ответственного поведения государств были зафиксированы в Резолюции «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» от 5 декабря 2018 г.[3]. Была отмечена прерогатива их применения в соответствии с национальными интересами государств с целью снижения международной напряженности и предотвращения возможных конфликтов.

В докладе высказан призыв к правительствам стран предотвращать распространение вредоносных программ, отказаться от использования технических устройств с целью вмешательства во внутренние дела государств, запретить распространение дезинформации.

В итоговом докладе Рабочей группы были зафиксированы меры укрепления доверия в сфере обеспечения информационной безопасности (confidence-building measures). Эти меры служат основой для сотрудничества и повышения стабильности отношений между странами, имеют добровольный характер и призваны разрешить ситуации, связанные с недопониманием происходящих событий участниками международных правоотношений, предотвратить возможные

[1] Поощрение ответственного поведения государств в киберпространстве в контексте международной безопасности : резолюция Генеральной Ассамблеи ООН от 22 декабря 2018 г. URL: https://www.un.org/ru/ga/73/docs/73res3.shtml (дата обращения: 26.04.2021).

[2] Final Substantive Report of Open-ended working group on developments in the field of information and telecommunications in the context of international security 12 March 2021. URL: https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf (дата обращения: 26.04.2021).

[3] Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности : резолюция Генеральной Ассамблеи ООН от 5 декабря 2018 г. URL: https://www.un.org/ru/ga/73/docs/73res1.shtml (дата обращения: 26.04.2021).

конфликты между странами и устранить любые формы недоверия. Они представляют собой совместные усилия по укреплению общей безопасности, открывают возможности для дальнейшего многостороннего и двустороннего сотрудничества государств.

И в первую очередь мерой укрепления доверия в сфере обеспечения информационной безопасности должна стать деятельность самой Рабочей группы, которая направлена на стабилизацию отношений между государствами, предотвращение возможных конфликтов и обеспечение ясности в международной информационной среде.

Проведенный анализ доклада позволяет классифицировать меры укрепления доверия следующим образом.

В зависимости от территории распространения и применения меры укрепления доверия можно разделить на международные, которые актуальны для всего мирового сообщества, и национальные – в сфере обеспечения информационной безопасности, характерные для национальной практики конкретной страны.

К международным мерам укрепления доверия можно отнести проведение многосторонних обсуждений для решения вопросов практического применения конкретных мер укрепления доверия, разработку новых норм в сфере обеспечения информационной безопасности, стимулирование дополнительных инициатив и повышение информационной осведомленности стран.

Одной из национальных мер укрепления доверия будет являться создание национальных контактных центров (National Points of Contact (PoCs)) для координации деятельности и обмена информацией между странами по дипломатическим, политическим, правовым и техническим вопросам, а также для уведомления о случившихся нарушениях в области информационной безопасности. Также к национальным мерам будет относиться формирование национальных групп реагирования на компьютерные происшествия (Computer Emergency Response Teams (CERTs)) для своевременной реакции на возникающие инциденты, связанные с нарушением обеспечения информационной безопасности в стране.

В зависимости от формы информационного взаимодействия меры укрепления доверия можно разделить на меры, связанные с обменом: 1) национальными мнениями между государствами по вопросам применения норм международного права в сфере обеспечения кибербезопасности; 2) сведениями, направленными на информирование о существующих и потенциальных угрозах, национальной политике и подходах государств с целью взаимного обучения; 3) опытом, предполагающим уведомление о конкретных мерах, применяемых при расследовании инцидентов; 4) опытом на техническом уровне для расследования происшествий в области информационной безопасности. Особое место среди форм информационного взаимодействия занимает добровольное информирование Генерального секретаря ООН и Института ООН по исследованию проблем разоружения о практике применения страной международного права в контексте международной безопасности и размещение необходимой информации на портале по вопросам киберполитики.

В зависимости от привлекаемых к сотрудничеству субъектов можно выделить меры укрепления доверия, в реализации которых участвуют гражданское общество, частный сектор, научные круги и техническое сообщество. Указанные субъекты занимаются проведением информационно-разъяснительной работы по вопросам использования различных информационных источников. Кроме того, они размещают всю необходимую информацию на всевозможных форумах в целях обеспечения прозрачности и распространения сведений об информационно-коммуникативных технологиях для неограниченного круга лиц.

В зависимости от вида объекта защищаемой инфраструктуры меры укрепления доверия можно разделить на меры, направленные на защиту таких объектов критически важной инфраструктуры, как объекты энергетики, связи, здравоохранения и т. д.

Принятию итогового доклада предшествовало два года кропотливой работы. Рабочей группой велась подготовка текста итогового документа, и первоначально был сделан проект доклада, в котором содержались также иные меры укрепления доверия в сфере обеспечения информационной безопасности, не вошедшие в итоговую редакцию документа[1].

Так, в проекте доклада Рабочей группы были зафиксированы следующие меры укрепления доверия: создание глобального справочника контактных центров для координации деятельности стран и обмена информацией по аналогии с национальными контактными центрами; создание глобального хранилища информации о мерах укрепления доверия (global repository of confidence-building measures) для обеспечения условий взаимного обучения на основе имею-

[1] Draft substantive report of Open-ended working group on developments in the field of information and telecommunications in the context of international security 12 March 2021. URL: https://documents-dds-ny.un.org/doc/UNDOC/LTD/N20/378/94/PDF/N2037894.pdf?OpenElement (дата обращения: 26.04.2021).

щегося опыта, помощи государствам в разработке дополнительных мер укрепления доверия с учетом региональных и национальных условий; проведение добровольных обследований (voluntary surveys) под эгидой ООН для обмена имеющимся опытом и практикой стран, а также для выявления потребностей дополнительного регулирования в отдельных сферах информационной безопасности и другие меры.

Как представляется, данные меры укрепления доверия в сфере обеспечения информационной безопасности могли бы быть эффективными средствами дальнейшего сотрудничества стран в целях создания общих стандартов и условий обеспечения информационной безопасности всех стран – членов ООН. Включение мер в редакцию итогового доклада Рабочей группы могло бы стать основой для более тесного взаимодействия стран – членов ООН в области оказания поддержки, обеспечения прозрачности и слаженности усилий по укреплению международной информационной безопасности.

В настоящее время современные информационные технологии широко применяются для обеспечения деятельности объектов, которые являются базовыми для жизнедеятельности государств. С учетом своих особенностей государства формируют свою основу реализации информационной безопасности. Однако в связи с появлением новых потенциальных угроз и развитием технологий страны становятся все более уязвимыми и их защита невозможна без сотрудничества всех участников международных отношений. В условиях глобализации создание общих мер укрепления доверия в сфере обеспечения информационной безопасности и их развитие может стать фундаментом для успешного сотрудничества государств в целях обеспечения международной информационной безопасности каждого государства.

СПИСОК ЛИТЕРАТУРЫ

1. Вылегжанин А. Н. Международное право : учебник / отв. ред. А. Н. Вылегжанин. М. : Юрайт, 2009. 1012 с.

2. Забара И. Н. Деятельность ООН в развитии международно-правового регулирования информационных отношений // Вестник РУДН. Сер.: Юридические науки. 2013. № 1. С. 136–143.

3. Игнатенко Г. В. Международное право : учеб. для вузов / отв. ред. Г. В. Игнатенко, О. И. Тиунов. 3-е изд., перераб. и доп. М. : Норма, 2005. 624 с.

4. Колосов Ю. М. Международное право : учеб. 2-е изд., перераб. и доп. / отв. ред. Ю. М. Колосов, Э. С. Кривчикова. М. : Междунар. отношения ; Юрайт-Издат, 2007. 1026 с.

5. Молчанов Н. А., Матевосова Е. К. Концептуально-политический и формально-юридический анализ Парижского призыва к доверию и безопасности в киберпространстве и российские инициативы в области международного права // Актуальные проблемы российского права. 2020. Т. 15. № 1. С. 133–141. https://doi.org/10.17803/1994-1471.2020.110.1.133–141.

6. Ромашкина Н. П. Проблема международной информационной безопасности в ООН // Мировая экономика и международные отношения. 2020. № 64. С. 25–32.

REFERENCES

1. Vylegzhanin A.N. *Mezhdunarodnoe pravo: uchebnik* [International law: textbook]. Moscow, Yurait, 2009, 1012 p. (in Russian)

2. Zabara I. N. Deyatel'nost' OON v razvitii mezhdunarodno-pravovogo regulirovaniya informacionnyh otnoshenij [Activities of the United Nations in the development of international legal regulation of information relations]. *Vestnik RUDN* [Bulletin RUDN], 2013, vol. 1, pp. 136-143. (in Russian)

3. Ignatenko G.V. *Mezhdunarodnoe pravo: Uchebnik dlya vuzov* [International law: Textbook for universities]. Moscow, Norma, 2005, 624 p. (in Russian)

4. Kolosov U.M. *Mezhdunarodnoe pravo: uchebnik* [International law: textbook]. Moscow, Yurait, 2007, 1026 p. (in Russian)

5. Molchanov N.A., Matevosova E.K. Konceptual'no-politicheskij i formal'no-yuridicheskij analiz Parizhskogo prizyva k doveriyu i bezopasnosti v kiberprostranstve... i rossijskie iniciativy v oblasti mezhdunarodnogo prava [Conceptual, political and formal legal analysis of the Paris Call for Trust and Security in Cyberspace and Russian initiatives in the field of international law]. *Aktual'nye problemy rossijskogo prava* [Current problems of Russian law], 2020, vol. 1, pp. 133-141. https://doi.org/10.17803/1994-1471.2020.110.1.133-141. (in Russian)

6. Romashkina N.P. Problema mezhdunarodnoj informacionnoj bezopasnosti v OON [The problem of international information security at the UN]. *Mirovaya ekonomika i mezhdunarodnye otnosheniya* [World economy and international relations], 2020, vol. 64, pp. 25-32. (in Russian)

Confidence-building Measures in the Field of Information Security as a Basis for International Cooperation

© Kolosov A. V., 2021

The features of confidence-building measures in the field of information security are studied. It is noted that international peace and security are of global importance in modern conditions and one of the ways to ensure the stability of international relations is an equal partnership of states on the basis of generally recognized principles and norms of international law. The article analyzes the current issue of international law-the creation of confidence-building measures in the field of information security. Special attention is paid to the analysis of the international legal framework for cooperation in information relations. The work of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the context of international security was studied, and one of the most important achievements of the Working Group was the Final Report of March 12, 2021. It is established that the capabilities of modern technical devices are constantly expanding and evolving, such technologies can be used by attackers to make society more vulnerable and create large-scale negative consequences for most countries, because no state is protected from possible threats. It is argued that in order to solve such problems, it is necessary to make common efforts on the part of all countries to strengthen mutual cooperation and achieve large-scale results in the field of creating a secure information environment. It is concluded that one of the forms of cooperation between states is confidence-building measures in the field of information security. The classification of measures is proposed and a conclusion is made about the fundamental importance of measures for the successful cooperation of states in order to ensure the international information security of each state.

Keywords: confidence-building measures, information security, Open-ended Working Group on Developments in the field of Information and Telecommunications in the context of international security, cyber policy, cybersecurity.