*Научная специальность*
*12.00.10 «Международное право; Европейское право»*

УДК 341.1/8

# МЕЖДУНАРОДНАЯ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: ПРАВОВЫЕ АСПЕКТЫ И ДЕЯТЕЛЬНОСТЬ ООН

© **Сидорова Т. Ю., 2020**
Сибирский федеральный университет, г. Красноярск, Россия

Проведен анализ современного состояния работы Организации Объединенных Наций в области создания правового регулирования международной информационной безопасности. Обосновано рассмотрение данных вопросов именно на площадке ООН в связи с тяжестью возможных последствий применения государствами силы в ответ на отражение киберугрозы, исходящей со стороны другого государства. Дан анализ современного подхода ООН к обсуждению и установлению регулирования вопросов международной информационной безопасности. Рассмотрены документы Генеральной Ассамблеи ООН, принятые на третьем этапе развития регулирования организацией международных информационных отношений. Отдельно дан сравнительный анализ двух «киберрезолюций» Генеральной Ассамблеи ООН, принятых в декабре 2018 г. На основе проведенного исследования был поддержан вывод о том, что современное состояние регулирования международной информационной безопасности относится к этапу становления «мягкого права». Опровергнуто утверждение об отсутствии у государств противоречий в понимании пути развития международного права в исследуемой области. Резюмируется, что отсутствие со стороны ООН более решительных действий приведет к укреплению тенденции постепенного снижения роли ООН в регулировании этого вопроса и возможному перехвату инициативы региональными организациями. Предложено расширить механизмы работы, включив в него экспертное сообщество и начав работу над жесткими правовыми нормами.

*Ключевые слова:* кибербезопасность, Организация Объединенных Наций, Группа правительственных экспертов, киберугрозы, «мягкое право».

Вопросы информационной безопасности занимают важное место в международной повестке дня. Если в конце XX в. это воспринималось как новая тенденция в международных отношениях и международном праве, то в XXI в. превратилось в рутину в деятельности внутригосударственных органов по обеспечению безопасности и постоянно включается в вопросы, обсуждаемые на глобальном и региональном международном уровне.

Оборот информации и данных самого различного происхождения плотно вошел в деятельность не только коммерческих, но и государственных и международных структур. Теперь уязвимость или защищенность инфраструктуры информационно-коммуникационных технологий (далее – ИКТ), возможность утечки данных становится условием применения недружественного или откровенно враждебного информационного воздействия на других субъектов международных отношений. По данным интернет-портала «Известия», с 5 января по 5 июня 2020 г. было сделано 14 официальных заявлений о кибератаках на правительственные структуры различных государств и 2 заявления об атаках на Всемирную организацию здравоохранения[1]. В списке пострадавших фигурируют бундестаг ФРГ, оборонные ведомства Японии и России, сайт президента Украины. Среди экономических объектов, по сообщениям «Известий», атакам подвергались системы здравоохранения, энергетики, банки, университеты. Политическая оценка подобных событий в последнее время все чаще стала происходить в риторике обвинений в агрессии, о чем свидетельствует, например, обсуждение Генеральным секретарем НАТО Йенсом Столтенбергом и премьер-министром Великобритании Терезой Мэй 14 мая 2019 г. «продолжающейся российской агрессии», в состав которой включили и предполагаемые кибератаки со стороны подконтрольных России структур и отдельных лиц[2].

[1] Кибератаки. Известия [Электронный ресурс] // Известия. URL: https://iz.ru/tag/kiberataki (дата обращения: 10.06.2020).

[2] Генсек НАТО и британский премьер обсудили «российскую агрессию» [Электронный ресурс] // Известия. URL: https://iz.ru/878105/2019-05-15/gensek-nato-i-britanskii-premer-obsudili-rossiiskuiu-agressiiu (дата обращения: 10.06.2020).

Подобные заявления политиков вызывают опасения в связи с тем, что международное право предоставляет каждому государству право на самооборону от агрессии, следовательно, при квалификации кибератак как акта агрессии возможно применение средств самозащиты и других мер в соответствии с Уставом ООН. Хотя в настоящее время ни одного подобного прецедента еще не было, но наращивание угроз информационной безопасности рано или поздно приведет к обсуждению того, какие меры вооруженного характера адекватно применить в данном случае. Именно поэтому является важным оценить, насколько Организация Объединенных Наций как глобальная организация коллективной безопасности способна контролировать ситуацию и предложить государствам адекватные правовые и политические средства поддержания приемлемого уровня информационной безопасности.

При определении понятия информационной безопасности в русскоязычных источниках чаще всего обращаются к Доктрине информационной безопасности, утвержденной Указом Президента РФ от 5 декабря 2016 г. № 646[1]. Если сравнивать это определение с традиционным определением безопасности, то обращает на себя внимание отличие в качестве угроз, они обозначены как информационные и подразделяются на внутренние и внешние. Также следует отметить, что подход к международной составляющей информационной безопасности России осуществляется через реализацию национальных интересов, к числу которых относятся защита прав и свобод человека, устойчивое и бесперебойное функционирование информационной инфраструктуры, развитие IT, отрасли высоких технологий и электронной промышленности, культурные и информационные интересы. Примечательно, что в подп. «д» п. 8 Доктрины также указано содействие формированию системы международной информационной безопасности и защита суверенитета Российской Федерации в информационном пространстве.

Наряду с термином «информационная безопасность» есть термин «кибербезопасность» и другие с использованием именно приставки «кибер». Следует отметить, что терминологические различия обычно подчеркиваются в российских источниках, однако, на наш взгляд, для определенных исследований можно пренебречь различиями в деталях и согласиться с наличием некоего общего значения. Так, проводя исследование вопросов угроз международной информационной безопасности, А. Я. Капустин [2, с. 46] также отмечает наличие двоякой терминологии, причем используемой в различных российских нормативных правовых актах вроде Концепции информационной безопасности и Уголовного кодекса РФ, и приходит к выводу, что сфера применения в России терминов с приставкой «кибер» расширяется. Сам исследователь также пренебрегает некоторыми различиями и использует термин «киберугрозы» применительно к широкому спектру угроз международной информационной безопасности, хотя и подчеркивает нетождественность этих терминов.

На наш взгляд, такой подход вполне оправдан рядом причин. Во-первых, общим употреблением терминов «кибербезопасность» и «киберугрозы» в различных областях знаний. Во-вторых, заимствованием англоязычной терминологии в исследуемой области. В связи с этим для целей настоящей статьи мы также не будем проводить различия между терминами «информационная безопасность» и «кибербезопасность» и прочими парными употреблениями.

Оценивая значимость различных угроз в области международной информационной безопасности, можно обратить внимание на различные классификации, но особо хотелось бы отметить военно-политические угрозы, которые рассматривает в своих работах Н. П. Ромашкина [4, с. 3–5]. В частности, автор выделяет как развитие ИКТ-вооружений, так и применение ИКТ против внутриполитической стабильности государства. Безусловно, что потенциально наиболее тяжелые последствия несут киберугрозы в области стратегических вооружений. Это показывает, что вопрос международной информационной безопасности имеет глобальный характер не только с точки зрения уязвимости любого государства, но и с точки зрения масштаба возможных последствий.

Понимание масштабности угроз есть и в юридической литературе. Так, один из видных ученых в области международного права А. Я. Капустин, анализируя различные киберугрозы, отмечает что ввод таких понятий, как кибератака, кибервойна, в политический и правовой лексикон неизбежно влечет начало дискуссий о применении силы. Критикуя расширительное толкование силы, А. Я. Капустин [2, с. 49] напоминает, что есть уже сложившееся толкование терминов ст. 2 Устава ООН, которое может быть применено и при отражении киберугроз. Рассматривая примеры с атакой на ядерные объекты и информацию, он полагает, что, помимо дискуссии об отличиях кибератак от кибервмешательства, стоит еще помнить о том,

[1] Доктрина информационной безопасности Российской Федерации: утв. указом Президента РФ от 05.12.2016 № 646 [Электронный ресурс] // Президент России. Официальный сайт. URL: http://kremlin.ru/acts/bank/41460 (дата обращения: 10.06.2020).

что международное сообщество не всегда применяет аналогию. В качестве доказательства он приводит ситуацию, когда в результате террористической атаки на самолет никто не ставит вопроса об автоматическом применении силы [2, с. 49–50].

Это доказывает важность правильного понимания прав и обязанностей государств в отношении вопросов международной информационной безопасности, что должно быть реализовано на универсальном уровне. В поддержку такой позиции можно сослаться на мнение Н. П. Ромашкиной [5, с. 12], которая отмечает, что ООН должна стать единственной глобальной площадкой, на которой необходимо договариваться об общих правилах поведения в киберпространстве, если это затрагивает интересы различных государств.

Говоря об истории вопроса регулирования информационных отношений документами ООН, И. Н. Забара [1, с. 137–140] выделяет три этапа. На первом этапе можно определить фокус внимания государств на вопросах использования информации во враждебных целях, что было осуждено ООН и международным сообществом. Второй этап автор связывает с реализацией идей нового международного информационного порядка, а третий уже касается развития концепции информационного общества. Именно на этом этапе появляются документы, которые относятся к сфере международной информационной безопасности [1, с. 142].

В целом, осуществляя поиск источников среди документов ООН, посвященных вопросам международной информационной безопасности, можно обратить внимание на рост их количества после 1999 г. Именно тогда Генеральным секретарем ООН было признано существование проблемы в сфере международной информационной безопасности и была принята Резолюция Генеральной Ассамблеи ООН 53/70 от 4 января 1999 г. «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности»[1]. В дальнейшем было одобрено несколько резолюций и документов ООН, представлены доклады Группы правительственных экспертов, что и сформировало на сегодняшний день ядро регулирования вопросов международной информационной безопасности в рамках ООН.

Анализируя развитие этого регулирования, В. М. Кулешов и А. А. Тарасенко [3, с. 61–64] отмечают в качестве знаковых ряд документов. Во-первых, они положительно оценивают предложенный в 2004 г. Россией проект «Принципов, касающихся международной информационной безопасности». Во-вторых, отмечают совместную инициативу стран ШОС в 2011 г. – проект «Правил поведения в сфере обеспечения международной информационной безопасности», дополненный в 2015 г. И наконец, неудачную попытку утверждения резолюцией ГА ООН «Правил ответственного поведения государств в информационном пространстве в контексте международной безопасности».

В 2018 г. достижения ООН в этой сфере пополнились еще двумя резолюциями. Рассмотрим их более подробно. Резолюция A/RES/73/27 от 5 декабря 2018 г. «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности»[2] подчеркивает необходимость для государств выполнять свои международные обязательства и в сфере использования информационно-коммуникационных технологий. Если провести корреляцию положений резолюции с принципами Устава ООН, то можно увидеть, что в резолюции в полной мере нашли свое отражение принцип суверенного равенства государств, невмешательства во внутренние дела, сотрудничества, добросовестного исполнения обязательств. Также стоит отметить специально выделенное положение о защите прав человека, в частности неприкосновенности личной жизни. Вместе с тем в резолюции есть два момента, которые выходят за рамки исключительно межгосударственных обязательств. Первый момент связан с п. 1.9 резолюции о каналах поставок, обеспечивающих безопасность продуктов ИКТ, а второй – это п. 1.13, призывающий сотрудничать государства, частный сектор и гражданское общество в области производства и сбыта информационных товаров и информационно-технических услуг.

Рассматривая резолюцию, можно отметить некоторую сложность понимания ряда пунктов. Так, резолюция, как уже было отмечено, исходит из уважения принципа территориального суверенитета (п. 1.2). Государства лишь принимают просьбы пресечь вредоносную деятельность, исходящую с их территории, но при этом имеют право не допускать вмешательство извне (п. 1.8). С другой стороны, п. 1.2 ограничивает толкование правил присвоения противоправ-

[1] Резолюция Генеральной Ассамблеи ООН 53/70 от 4 января 1999 г. «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» [Электронный ресурс] // Организация Объединенных Наций. Официальный сайт. URL: https://www.un.org/ga/search/view_doc.asp?symbol=A/RES/53/70&referer=/english/&Lang=R (дата обращения: 10.06.2020).

[2] Резолюция Генеральной Ассамблеи ООН 73/27 от 5 декабря 2018 года «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» [Электронный ресурс] // Организация Объединенных Наций. Официальный сайт. URL: https://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/73/27&Lang=R (дата обращения: 10.06.2020).

ного поведения государству. Безусловно, можно согласиться с положением этого пункта о том, что простое происхождение кибератаки с территории конкретного государства еще не создает связи с действиями самого государства. Но вот каким образом следует рассмотреть поведение государства, которое отказывается принимать меры и рассматривать ситуацию? Применение п. 1.2 и 1.8 лишает какого-либо правового инструмента потерпевшее государство и ставит решение проблемы исключительно в зависимость от доброй воли государства, которое обвиняют в поощрении преступной деятельности. Такой подход заводит ситуацию в тупик.

Вторая резолюция A/RES/73/264 от 22 декабря 2018 г. «Поощрение ответственного поведения государств в киберпространстве в контексте международной безопасности»[1] вроде бы должна разрешить противоречия такого рода. Однако анализ резолюции показывает, что ее авторы воздерживаются от провозглашения каких-либо принципов или норм. В первую очередь, подчеркивается необходимость продолжить практику работы Групп правительственных экспертов. Во-вторых, государства призываются следовать положениям докладов Групп правительственных экспертов 2010, 2013 и 2015 гг., проводить и поддерживать совместные меры, чтобы соблюсти баланс безопасности и свободного потока информации. Собственно, резолюция и далее призывает государства обмениваться информацией относительно усилий, предпринимаемых на национальном уровне по обеспечению информационной безопасности, и вопросов международного сотрудничества. В целом можно сказать, что авторы этой резолюции оказались не готовы к формулированию конкретных положений, которые можно было бы адресовать государствам в качестве правил поведения.

Для понимания резолюций важно оценить процесс их принятия. Первая резолюция была выдвинута совместно Россией и еще 32 государствами. За нее проголосовали 119 государств, в основном развивающиеся страны, а также члены ШОС и БРИКС. Против выступили 46 стран, в число которых вошли западные страны. Вторая резолюция была предложена США, за нее проголосовало 139 государств, преимущественно члены ЕС, НАТО, другие союзники США. Против высказались 11 государств. Воздержавшихся по обеим резолюциям было примерно одинаковое количество – 14 и 16 соответственно[2]. Такое распределение голосов показывает, что были страны, которые голосовали за обе резолюции. А. Толстухина насчитала таковых 77. Как она отмечает, эти страны не воспринимают документы как противоположные по содержанию, более того, рассматривают как взаимодополняющие.

Представляется, что голосование этих стран можно объяснить, действительно, отсутствием очевидного противоречия. Но все же анализ резолюций показывает, что если первая устанавливает некий стандарт поведения для всех государств, то вторая скорее говорит о том, что каждое государство само отвечает за свою безопасность, а международная информационная безопасность складывается не из их совместных действий, а из совокупности действий каждого. Также стоит подчеркнуть, что вторая резолюция исходит из уже сложившегося неравенства государств в сфере ИКТ и не стремится его нивелировать. Важно отметить, что именно вторая резолюция делает акцент на свободном потоке информации, которому не должны мешать предпринимаемые государством меры поддержания своей информационной безопасности.

В связи с этим отметим, что голосование за обе резолюции может свидетельствовать не столько о том, что государства не видят в них противоречий, сколько о том, что сами государства пока не выработали собственного подхода к тому, что должно стать основой для обеспечения международной информационной безопасности, и готовы посмотреть на результаты дальнейшей работы в этой сфере, чтобы сформировать собственную позицию.

Применительно к деятельности ООН стоит затронуть и работу Комиссии ООН по международному праву. Обзор документов на сайте Комиссии и поиск привели к тому, что было найдено всего два документа. В первом, Предварительном кратком отчете о 3377-м заседании Комиссии[3], где присутствовал представитель Межамериканского юридического комитета (Организация американских государств), указывается, что ОАГ сотрудничает с Группой правительственных экспертов по предоставлению мнений всех государств организации по вопро-

[1] Резолюция Генеральной Ассамблеи ООН 73/264 от 22 декабря 2018 года «Advancing responsible State behaviour in cyberspace in the context of international security» [Электронный ресурс] // Организация Объединенных Наций. Официальный сайт. URL: https://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/73/266 (дата обращения: 10.06.2020).

[2] Толстухина А. Лучше две киберрезолюции, чем ни одной. [Электронный ресурс] // Российский совет по международным делам. URL: Режим доступа: https://russiancouncil.ru/analytics-and-comments/analytics/luchshe-dve-kiberrezolyutsii-chem-ni-odnoy/ (дата обращения: 10.06.2020).

[3] Provisional summary record of the 3379th meeting [Электронный ресурс] // Организация Объединенных Наций. Официальный сайт. URL: https://legal.un.org/ilc/documentation/english/summary_records/a_cn4_sr3379.pdf#xml=https://legal.un.org/dtSearch/dtisapi6.dll?cmd=getpdfhits&DocId=4629&Index=D%3a%5csites%5clegal%5cilc%5cdtSearch%5cIndexes%5cDocuments%2dEnglish&HitCount=2&hits=1bfd+20af+&.pdf (дата обращения: 10.06.2020).

сам информационной безопасности. Во втором, Предварительном кратком отчете о 3379-м заседании Комиссии[1], кибербезопасность также упоминается в контексте визита представителя Межамериканского юридического комитета, который представил результаты обсуждения планов их работы с Генеральным секретарем ОАГ. В числе этих вопросов оказалось и противодействие киберспреступности. Других упоминаний о вопросах международной информационной безопасности в работе Комиссии нет. Также нет этой темы и среди тех, по которым Комиссия разрабатывает проекты статей и конвенций.

В исследовании В. П. Талимончик [6, с. 106] обосновывается, что в рамках ООН сформировалась концепция международной информационной безопасности, а также создан институционный механизм сотрудничества по этим вопросам. Вместе с тем, описывая различные киберугрозы, от кибероружия до киберпреступности, автор не может акцентировать внимание на тех документах ООН, которые охватывают правовое регулирование отношений в сфере международной информационной безопасности в ее всеобъемлющем подходе. В работе анализируются отдельные конвенции, имеющие отношение к противодействию киберугрозам в основном в сфере уголовных преступлений.

В свою очередь, в исследованиях политического характера отмечается слабая адаптация существующих норм международного права к отношениям в области информационной безопасности. Как пишет Н. П. Ромашкина [5, с. 11], лишь в докладе Группы правительственных экспертов в 2013 г. было заявлено о применении Устава ООН к киберпространству, а в Докладе 2015 г. уже определены ключевые положения: территориальный суверенитет государства над информационно-телекоммуникационной инфраструктурой; распространение на эти отношения принципов Устава ООН; отказ от использования посредников и предоставления своей территории для создания угроз информационной безопасности; ответственность государств. Пожалуй, только одно положение вызывает сомнение с точки зрения его реализации – это признание за государствами права на применение мер, которые не уточняются в Докладе.

«Мягкую» природу большинства норм относительно регулирования международных информационных отношений отмечает и И. Н. Забара [1, с. 142], объясняя это сложностью проблем правового регулирования данных отношений. Примечательно, что автор подчеркивает вовлечение в процесс все большего количества международных организаций, но оставляет координирующую роль за ООН.

По мнению Н. П. Ромашкиной [5, с. 12], в отношении Правил ответственного поведения государств у ведущих держав, в частности у России и США, есть ряд разногласий как по их содержанию, так и по характеру действия. Так, Россия склонна рассматривать их в качестве политической договоренности, а возможно, и придать им действие акта «мягкого права». США, в свою очередь, рассматривают документ более утилитарно, полагая, что туда необходимо включить только технические аспекты.

А. Я. Капустин отмечает, что этап «мягкого права» является важной частью процесса создания юридически обязательных правил поведения для государств в киберпространстве [2, с. 51].

Нисколько не умаляя значение «мягкого права» в регулировании международных отношений, тем не менее, следует отметить, что утрата ООН первенства в области создания норм по обеспечению международной информационной безопасности может привести к куда более негативным последствиям – правотворчеством могут заняться региональные организации. Так, в российской науке с деятельностью НАТО связывают разработку и публикацию Таллинского руководства – Tallin Manual on the International Law Applicable to Cyber Warfare[2], хотя данный документ лишь опосредованно связан с НАТО тем, что его разработал и опубликовал аккредитованный при НАТО экспертный центр – The NATO Cooperative Cyber Defence Centre of Excellence[3]. Как отмечают В. М. Кулешов и А. А. Тарасенко, данный документ рассматривает возможность вооруженного ответа против киберугроз [3, с. 66]. Действительно, Таллинское руководство анализирует применение к кибербезопасности норм и принципов международного права в области суверенитета, использования силы и самообороны, ответственности государства и др. Центр продолжает работать над этой темой и в 2017 г. опубликовал вторую редакцию Руководства.

Подводя итог, можно обратить внимание на ряд факторов, которые свидетельствуют о сни-

[1] Provisional summary record of the 3379th meeting [Электронный ресурс] // Организация Объединенных Наций. Официальный сайт.URL: https://legal.un.org/ilc/documentation/english/summary_records/a_cn4_sr3379.pdf#xml=https://legal.un.org/ dtSearch/dtisapi6.dll?cmd=getpdfhits&DocId=4629&Index=D%3a%5csites%5clegal%5cilc%5cdtSearch%5cIndexes%5cDocuments%2dEnglish&HitCount=2&hits=1bfd+20af+&.pdf (дата обращения: 10.06.2020).

[2] Tallin Manual on the International Law Applicable to Cyber Warfare [Электронный ресурс] // Центр стратегических оценок и прогнозов URL: http://csef.ru/media/articles/3990/3990.pdf (дата обращения: 10.06.2020).

[3] The NATO Cooperative Cyber Defence Centre of Excellence [Электронный ресурс] // The NATO Cooperative Cyber Defence Centre of Excellenceю URL: https://ccdcoe.org/ (дата обращения: 10.06.2020).

жении роли ООН в разработке международных норм в области обеспечения международной информационной безопасности. Во-первых, использование, по существу, только одного механизма – докладов Группы правительственных экспертов. За годы работы над этой проблемой ООН не смогла предложить другого механизма, который бы способствовал более быстрому формированию консенсуса государств с постепенным закреплением достижений хотя бы в резолюциях Генеральной Ассамблеи ООН. Противоречивость подходов резолюций 2018 г. демонстрирует, что выработанный механизм способен завести ООН в тупик.

Во-вторых, ООН не может перевести обсуждение вопросов международной информационной безопасности в правовую сферу. С этим связаны утвердившиеся в российской доктрине подходы к пониманию правовой основы регулирования международной информационной безопасности как «мягкого права». Вместе с тем к уже оформленному в ООН институционному механизму можно добавить и экспертный механизм по толкованию норм международного права, включая принципы Устава ООН, нормы jus cogens, нормы существующих универсальных конвенций применительно к вопросам международной информационной безопасности. Такая работа может быть востребована и международными судебными органами, и государствами для формирования своей позиции.

В-третьих, обсуждение вопросов международной информационной безопасности наталкивается на неравномерность экономического развития государств мира, и, как следствие, большой разрыв в финансовых и технологических возможностях в этой сфере. К сожалению, единства государств и в этом в рамках ООН добиться не удается.

Дальнейшее снижение роли ООН может привести к тому, что основная инициатива по урегулированию вопросов международной информационной безопасности перейдет на региональный уровень, что может в итоге подорвать доверие к ней как к организации глобальной коллективной безопасности.

### СПИСОК ЛИТЕРАТУРЫ

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

2. Капустин А. Я. К вопросу о международно-правовой концепции угроз международной информационной безопасности // Журнал зарубежного законодательства и сравнительного правоведения. 2017. № 6. С. 44–51.

3. Кулешов В. М., Тарасенко А. А. Международная информационная безопасность как вектор развития национальной безопасности России и Германии // Социально-экономические явления и процессы. 2019. Т. 14, № 105. С. 60–73.

4. Ромашкина Н. П. Глобальные военно-политические проблемы международной информационной безопасности: тенденции, угрозы, перспективы // Вопросы кибербезопасности. 2019. № 1(29). С. 2–9.

5. Ромашкина Н. П. Проблемы международной информационной безопасности: компромисс между Россией и Западом // Европейская безопасность: события, оценки, прогнозы. 2016. Вып. 41 (57). С. 9–12.

6. Талимончик В. П. Информационная безопасность в контексте всеобъемлющей системы международной безопасности // Правоведение. 2008. № 2. С. 103–110.

### REFERENCES

1. Zabara I.N. Deyatelnost OON v razvitii mezhdunarodno-pravovogo regulirovaniya informatsionnykh otnosheniy [UN activities in the development of international legal regulation of information relations]. *Vestnik RUDN, seriya Yuridicheskiye nauki* [Herald of RUDN University, series Legal Science], 2013, no. 1, pp. 136-143. (in Russian)

2. Kapustin A.YA. K voprosu o mezhdunarodno-pravovoy kontseptsii ugroz mezhdunarodnoy informatsionnoy bezopasnosti [About the international legal concept of threats to international information security]. *Zhurnal zarubezhnogo zakonodatelstva i sravnitel'nogo pravovedeniya* [Journal of Foreign Legislation and Comparative Law], 2017, no. 6, pp. 44-51. (in Russian)

3. Kuleshov V.M. Mezhdunarodnaya informatsionnaya bezopasnost' kak vektor razvitiya natsional'noy bezopasnosti Rossii i Germanii [International information security as a vector for the development of national security of Russia and Germany]. *Sotsialno-ekonomicheskiye yavleniya i protsessy* [Socio-economic phenomena and processes], 2019, vol. 14, no. 105, pp. 60-73. (in Russian)

4. Romashkina N.P. Globalnyye voyenno-politicheskiye problemy mezhdunarodnoy informatsionnoy bezopasnosti: tendentsii, ugrozy, perspektivy [Global military-political problems of international information security: trends, threats, prospects]. *Voprosy kiberbezopasnosti* [Issues of Cybersecurity], 2019, no. 1(29), pp. 2-9. (in Russian)

5. Romashkina N.P. Problemy mezhdunarodnoy informatsionnoy bezopasnosti: kompromiss mezhdu Rossiyey i Zapadom [Problems of international information security: a compromise between Russia and the West]. *Yevropeyskaya bezopasnost: sobytiya, otsenki, prognozy* [European Security: Events, Assessments, Predictions], 2016, no. 41 (57), pp. 9-12. (in Russian)

6. Talimonchik V.P. Informatsionnaya bezopasnost v kontekste vseob"yemlyushchey sistemy mezhdunarodnoy bezopasnosti [Information Security in the Context of a Comprehensive System of International Security]. *Pravovedeniye* [Jurisprudence], 2008, no. 2, pp. 103-110. (in Russian)

## International Information Security: Legal Aspects and UN Activities

**© Sidorova T. Yu., 2020**

The article is devoted to the analysis of the United Nations current work in the field of creating legal regulation of international information security. The article substantiates the consideration of these issues namely at the UN platform which is connected with the severity of possible consequences of the use of force by states in response to the reflection of a cyber threat emanating from another state. The article provides an analysis of the current UN approach to the discussion and establishment of regulation of international information security issues. The article discusses the documents of the UN General Assembly adopted at the third stage of the organization's regulatory development of international information relations. A comparative analysis of the two "cyber resolutions" of the UN General Assembly, adopted in December 2018, is given separately. The conducted research proves the conclusion that the current state of regulation of international information security refers to the stage of "soft law" formation. At the same time, the argument that states have no contradictions in their understanding of the development of international law in the study area is refuted. As a result, the article infers that the lack of more decisive actions on the part of the United Nations will strengthen the tendency towards its gradually declining role in regulating this issue and will probably lead to intercepting the initiative by regional organizations. To solve this problem, it was proposed to expand the working mechanisms by including an expert community in this process and starting work on "hard law".

*Keywords:* cybersecurity, United Nations, Group of Governmental Experts, cyber threats, soft law.