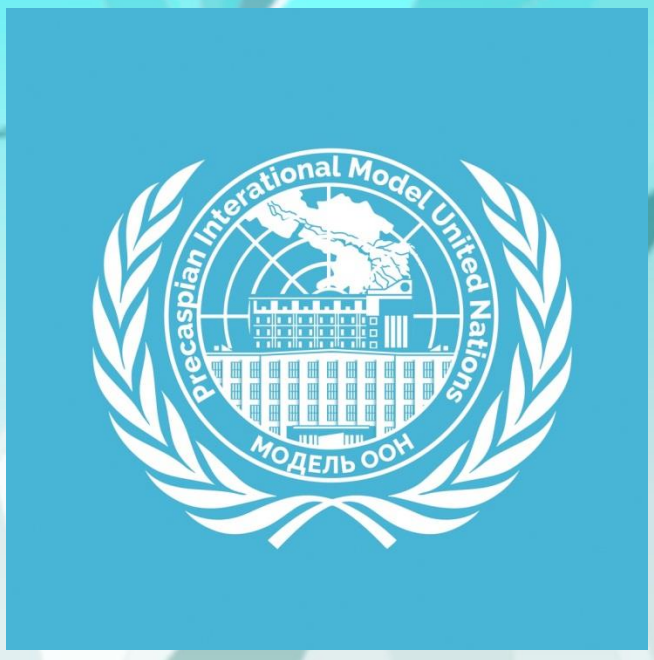
Доклад эксперта
Совет Безопасности
«Угрозы миру и безопасности, создаваемые информационно-коммуникационными технологиями»

PRCIMUN-2022



1. ОСНОВНЫЕ АСПЕКТЫ ПРОБЛЕМЫ

Обмен информацией и возможность ее распространения можно рассматривать в качестве основы существования и функционирования любого типа общества.

На протяжении исторического развития общества можно выделить несколько переломных моментов, связанных с появлением новых форм информационного обмена, так называемых «информационных революций». Первая такая революция была обусловлена изобретением письменности и алфавита, что позволило фиксировать информацию и накапливать знания об окружающем мире и событиях. Вторая информационная революция соотносится с возникновением и развитием книгопечатания, что значительно облегчило процесс фиксации знаний, и увеличило скорость распространения информации. Третья информационная революция, гораздо более грандиозная и стремительная по масштабам и последствиям, была обусловлена технологическими изменениями, открытием электричества, последующим изобретением телеграфа, телефона, радио и телевидения, что значительно повысило скорость распространения информации и сделало ее доступной для широкого круга пользователей. На современном этапе развития общество переживает четвертую информационную революцию, беспрецедентную по своему характеру и масштабам[1]. С середины XX века международное сообщество вступает в новый этап развития – постиндустриальное, или информационное, общество. С 1960-х годов происходит внедрение ЭВМ, первых компьютеров, а впоследствии создание глобальной сети Интернет как важнейшего достижения технологической революции. Все это обусловило переход к новому типу общества – обществу информационному, центральным элементом которого становится практически безграничный доступ к знаниям и информации, их распространение и использование в качестве базового ресурса. Глобальная технологическая инфраструктура Интернета определяет трансграничный характер его функционирования и использования, позволяющий преодолеть временные, пространственные и даже политические границы.

На сегодняшний день можно констатировать, что масштабное распространение в мире ИКТ в совокупности с транснациональной

[1] Рассолов И.М. Право и кибернетическое пространство. Монография.- 2-е изд.-М.: Московское бюро по правам человека, 2016.С.7-10

коммуникационной сетью Интернет создали условия для формирования глобального информационного общества (ГИО). При этом сам процесс становления ГИО и разработки правовой основы его функционирования и устройства занял определенный временной отрезок и проходил в несколько этапов. Первой значимой вехой можно считать состоявшуюся в Миннеаполисе Полномочную конференцию МСЭ, где была выдвинута и поддержана идея Всемирной встречи на высшем уровне по вопросам информационного общества под эгидой «Международного союза электросвязи». Далее в 2000г. «Группой восьми» была принята Окианавская Хартия глобального информационного общества[2]. Данные документ выдвинул ряд важных идей, сформулировал взаимодополняющие цели политического, экономического и социального характера и определил конкретные направления работы, в числе которых проведение экономических и структурных реформ, рациональное управление макроэкономикой, разработка информационных сетей, развитие людских ресурсов, активное использование ИКТ в государственном секторе. В 2002 г. на Полномочной конференции МСЭ были приняты Марракешские соглашения[3], утвердившие принципы построения глобального информационного общества: обеспечение права на информацию и знания, содействие универсальному доступу к ним, укрепление международного сотрудничества и повышение безопасности информационных и коммуникационных сетей. Всемирная встреча на высшем уровне по вопросам информационного общества (ВВУИО) прошла в два этапа – Женевский (2003) и Тунисский (2005)[4]. Эта встреча явилась первым международным форумом, на котором обсуждение вопросов, связанных с глобальными процессами информатизации, было поднято на самый высший политический уровень и состоялось в столь широком геополитическом масштабе в диалоге с представителями деловых кругов и гражданского общества. В саммите участвовало свыше 11 тысяч человек из 176 стран мира, включая представителей международных организаций. В ходе встречи информационная безопасность находилась в центре международного внимания. Одним из основных вопросов, обсуждавшихся на Всемирной встрече, были вопросы доверия и безопасности при использовании информационно-телекоммуникационных технологий. Речь шла о том, что преимущества, которые может предоставить использование информационно-телекоммуникационных технологий, в полной мере могут быть реализованы лишь в случае надежности и безопасности соответствующих технологий и сетей и отказа от их использования в целях, несовместимых с задачами обеспечения международной стабильности и безопасности. Участники

---

[2] Окинавская хартия Глобального информационного общества 21 июля 2000 года http://www.kremlin.ru/supplement/3170

[3] Министерство связи Российской Федерации ГОСУДАРСТВЕННАЯ КОМИССИЯ ПО ЭЛЕКТРОСВЯЗИ РЕШЕНИЕ от 25 декабря 2002 года N 49 Об итогах Полномочной конференции МСЭ (г.Марракеш, 2002 год) и работе на ней Администрации связи России https://docs.cntd.ru/document/901858785

[4] **Всемирная встреча на высшем уровне по вопросам информационного общества** https://www.un.org/ru/events/pastevents/wsis.shtml

Всемирной встречи выразили опасение относительно того, что информационно-телекоммуникационные технологии могут оказывать негативное воздействие на безопасность государств и признали необходимость предотвращения использования информационных ресурсов или технологий для преступных или террористических целей. В качестве одной из мер, которые можно было бы предложить для решения проблем международной безопасности, участники назвали рассмотрение существующих и потенциальных угроз для безопасности информационных и коммуникационных сетей. Важнейшим итогом первого этапа стало принятие двух документов, впоследствии одобренных Генеральной Ассамблеей ООН: Декларации принципов по вопросам информационного общества[5] и Плана действий Всемирной встречи на высшем уровне по вопросам информационного общества[6].

В ходе второго этапа были приняты Тунисское обязательство по вопросам информационного общества и Тунисская программа для информационного общества[7]. В обозначенных документах было зафиксировано общее понимание того, что использование ИКТ должно сопровождаться соблюдением общепризнанных прав человека, не подрывать свободу доступа к информации, особую значимость приобретает деятельность, направленная на преодоление цифрового разрыва, что позволит развивающимся странам отстоять свое право на доступ к современным ИКТ.

В ходе работы ВВУИО были организованы региональные конференции, на которых был принят ряд деклараций по вопросам информационного общества. Так, одним из принципов информационного общества, зафиксированных в **Бухарестской декларации** Общеевропейской конференции[8], стал принцип укрепления доверия и безопасности при использовании информационно-телекоммуникационных технологий. Он подразумевает разработку «глобальной культуры кибербезопасности», которая должна обеспечиваться путем принятия упреждающих мер и поддерживаться всем обществом при сохранении свободы передачи информации. Государства, принявшие участие в конференции в Бухаресте, пришли к пониманию того, что «информационно-телекоммуникационные технологии могут использоваться в целях, несовместимых с задачами обеспечения международной стабильности и безопасности, а также негативно

---

[5] Документ WSIS-03/GENEVA/DOC/4-R 12 декабря 2003 года Оригинал: английский Декларация принципов Построение информационного общества – глобальная задача в новом тысячелетии https://www.un.org/ru/events/pastevents/pdf/dec_wsis.pdf

[6] Документ WSIS-03/GENEVA/DOC/5-R 12 декабря 2003 года Оригинал: английский План действий https://www.un.org/ru/events/pastevents/pdf/plan_wsis.pdf

[7] Документ WSIS-05/TUNIS/DOC/6(Rev.1)-R 15 ноября 2005 года Оригинал: английский Председатель Подготовительного комитета Тунисского этапа ТУНИССКАЯ ПРОГРАММА ДЛЯ ИНФОРМАЦИОННОГО ОБЩЕСТВА https://www.un.org/ru/events/pastevents/pdf/agenda_wsis.pdf

[8] Документ WSIS/PC-2/DOC/5-R 15 января 2003 года Оригинал: английский Записка Исполнительного секретариата ВВУИО ОТЧЕТ ОБЩЕЕВРОПЕЙСКОЙ РЕГИОНАЛЬНОЙ КОНФЕРЕНЦИИ ВВУИО (Бухарест, 7–9 ноября 2002 года) https://www.itu.int/dms_pub/itu-s/md/03/wsispc2/doc/S03-WSISPC2-DOC-0005!!PDF-R.pdf

воздействовать на целостность инфраструктуры внутри отдельных государств, нарушая их безопасность».

В Токио в январе 2003 г. прошла Азиатская конференция, результатом которой стала разработка **Токийской декларации**. В этом документе, который приняли представители 47 стран, 22 международных и 116 неправительственных организаций, а также представители 54 частных компаний, выделены «приоритетные области действий» в области информационно-телекоммуникационных технологий. Важное место в их числе занимает вопрос обеспечения безопасности информационных технологий и средств. Признавая принцип справедливого, равного и адекватного доступа к информационно-телекоммуникационным технологиям для всех стран, особое внимание стороны полагают необходимым уделить угрозе потенциального военного использования ИКТ. Страны - участники также согласились с необходимостью усилить региональное и международное сотрудничество с целью укрепления безопасности инфосферы. Впервые было высказано мнение о том, что эффективное обеспечение информационной безопасности может быть достигнуто не только технологически, но и организационно, для этого потребуются усилия по правовому регулированию вопроса и выработке соответствующих национальных политик.

Таким образом, информационно-коммуникационные технологии в условиях глобальной информационной революции становятся не просто ресурсом, а важнейшим структурным элементом построения глобальной информационного общества. При этом практически с первых попыток обсуждения и понимания роли ИКТ стало очевидно наличие потенциальных вызовов и угроз безопасности как со стороны отдельных пользователей, так и на уровне национальной государственной безопасности, и в конечном итоге международной безопасности. Глобальная информационная революция создала новую среду, в которой формируется мировой правопорядок, что в свою очередь обусловило изменения в структуре международной безопасности и выделение самостоятельной области **международной информационной безопасности (МИБ)**. В этой связи особую актуальность приобретает проблема разработки и совершенствования международно-правовой базы в сфере информационной безопасности, а также принятие специальных юридических норм и правил, непосредственно регулирующих ИКТ. Деятельность по созданию основ международного права в сфере МИБ реализуется на различных форумах в разных форматах дипломатической деятельности, включая двусторонние, региональные и универсальные международные площадки.

2. ДЕЯТЕЛЬНОСТЬ ООН В КОНТЕКСТЕ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.

На площадку ООН вынесено обсуждение глобальной проблемы – обеспечения международной информационной безопасности в различных аспектах, включая вопросы использования ИКТ в военной сфере, возможности

использования ИКТ в преступных или террористических целях, необходимости уважения прав человека и основных свобод в сфере использования ИКТ, вопросы определения статуса и управления Интернет-пространством.

На протяжении 23 лет, начиная с 1998г. на площадке ГА ООН ведется многолетняя и крайне напряженная работа по обсуждению различных аспектов проблемы МИБ. Активную роль в этом процессе принимает РФ, являющаяся автором многих инициатив и проектов Резолюций по повестке «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности».

В 1998 г. в адрес Генерального секретаря ООН было направлено специальное послание по проблеме международной информационной безопасности Министра иностранных дел Российской Федерации. Особый акцент в нем был сделан на необходимости предотвращения появления принципиально новой информационной сферы конфронтации и развязывания принципиально новых военных конфликтов. Практическим развитием этой российской инициативы стало внесение российской стороной в ходе 53-й сессии генеральной Ассамблеи (ГА) ООН проекта резолюции под названием «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», принятой 4 декабря 1998 года в виде резолюции A/RES/53/70[9]. Резолюция содержит предложение в адрес государств-членов ООН продолжить обсуждение вопросов информационной безопасности, дать конкретные определения угроз, предложить свои оценки проблемы, включая разработку международных принципов обеспечения безопасности глобальных информационных систем. О таких оценках страны-члены ООН должны информировать Генерального секретаря ООН, которому было поручено представить соответствующий доклад на следующей сессии ГА ООН [2]. Доклад Генсекретаря был опубликован 10 августа 1999 года (A/54/213)[10] и включил оценки Австралии, Белоруссии, Брунея, Кубы, Омана, Катара, России, Саудовской Аравии, Великобритании и США. Общим для этих оценок стало признание наличия проблемы обеспечения информационной безопасности, однако при этом выявились существенные различия как в расстановке акцентов (военная, правовая, гуманитарная или другие составляющие), так и в методике ее рассмотрения и решения.

Следующие Резолюции ГА ООН 54/49[11], 55/28 [12] во многом подтвердили содержание Резолюции 53/70, дополнив их важными положениями о признании возможности негативного воздействия и использования ИКТ против безопасности государств не только в гражданской, но и в военной сферах. Так впервые была

[9] Резолюция ГА ООН A/RES/53/70 от 4 декабря 1998г. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N99/760/05/PDF/N9976005.pdf?OpenElement

[10] Достижения в области информации и телекоммуникаций в контексте международной безопасности : доклад Генерального секретаря A/54/213 | 1999-08-10 https://digitallibrary.un.org/record/286090?ln=ru

[11] Резолюция ГА ООН A/RES/54/49 от 1 декабря 1999г. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N99/777/15/PDF/N9977715.pdf?OpenElemen t

[12] Резолюция ГА ООН A/RES/55/28 от 20 декабря 2000г. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N00/561/09/PDF/N0056109.pdf?OpenElement

очерчена триада угроз МИД (использование ИКТ в военных, террористических и преступных целях).[13] Резолюция 54/49 еще раз подтверждает целесообразность разработки международных принципов и норм в сфере безопасности ИКТ и борьбы с киберпреступностью. В резолюции A/RES/55/28 отмечается, что целям ограничения угроз в сфере информационной безопасности отвечало бы «изучение соответствующих международных концепций, направленных на укрепление безопасности глобальных информационных и телекоммуникационных систем».

В резолюции A/RES/56/19 от 29 ноября 2001 года[14], принято решение о создании специальной Группы правительственных экспертов государств - членов ООН (ГПЭ) для проведения всестороннего исследования проблемы международной информационной безопасности. Функции этой группы предусматривают рассмотрение существующих и потенциальных угроз в сфере информационной безопасности и возможных совместных мер по их устранению, а также изучение международных концепций, которые были бы направлены на укрепление безопасности глобальных информационных и телекоммуникационных систем. Начало работы ГПЭ ООН в 2004г. определило новый этап многолетней работы ООН, заложив первую институциональную структуру, которая на протяжении нескольких созывов оставалась главной переговорной площадкой по обсуждению проблемы международной информационной безопасности. Вплоть до 2021г. состоялось 6 созывов ГПЭ (ГПЭ 1 2004г., учрежденная в соответствии с A/RES/56/19; ГПЭ 2 2009г., учрежденная в соответствии с A/RES /60/45; ГПЭ 3 2012г., учрежденная в соответствии с A/RES /65/41; ГПЭ 4 2014г., учрежденная в соответствии с A/RES 68/243; ГПЭ 5 2016г., учрежденная в соответствии с A/RES /70/237; ГПЭ 6 2019г., учрежденная в соответствии с A/RES/73/266). Мандат Группы расширялся и конкретизировался, включая такие направления работы, как разработка норм, правил или принципов ответственного поведения государств и мер укрепления доверия и наращивания потенциала, исследование вопросов использования ИКТ в конфликтах и того, как международное право применяется к использованию ИКТ государствами. Необходимо отметить, что только три состава ГПЭ оформили результаты своей в работы в согласованном и утвержденном консенсусом тексте итогового Доклада (2010г., 2013г., 2015г.). Работа других составов ГПЭ позволила осуществить всесторонний обмен мнениями, наилучшими видами практик и документами по вопросу о достижениях в сфере международной информационной безопасности, но не увенчалась достижением консенсуса по окончательному докладу.

Резолюция ГА ООН A/RES/57/53 [15] по международной информационной

[13] **ИНДЕКС БЕЗОПАСНОСТИ № 1 (104), Том 19**

[14] Резолюция ГА ООН A/RES/56/19 от 29 ноября 2001г. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N01/476/30/PDF/N0147630.pdf?OpenElement

[15] Резолюция ГА ООН A/RES/57/53 от 22 ноября 2002г. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N02/541/47/PDF/N0254147.pdf?OpenElement

безопасности развивает положения предыдущих резолюций и указывает на недопустимость использования информационно-телекоммуникационных технологий и средств в целях оказания негативного воздействия на инфраструктуру государств и дестабилизацию обстановки в отдельно взятом регионе.

В резолюции ГА ООН от 8 декабря 2003г. A/RES/58/32[16] выражается обеспокоенность тем, что ИКТ вероятно могут быть применены для задач, несоответствующих обеспечению международной стабильности и безопасности, а также могут критически влиять на единство механизма государств, нарушая их безопасность как в гражданской, так и в военной сферах.

В числе резолюций ГА ООН под титулом «Достижения в сфере информатизации в контексте международной безопасности» стоит отметить Резолюцию A/RES/66/24[17], закрепившую нормы, правила и принципы ответственного поведения государств в области обеспечения МИБ, разработанные ранее Россией совестно партнерами по Шанхайской организации сотрудничества (ШОС). Прорывной стала работа 73-й сессии ГА ООН, в ходе которой были приняты сразу два российских проекта резолюций A/RES/73/27 [18](окончательно утвердившая свод из 13 правил поведения государств в области международной информационной безопасности), A/RES/73/187 [19](«Противодействие использованию ИКТ в преступных целях», включающая в себя представленный ранее российский проект универсальной конвенции ООН о сотрудничестве в сфере противодействия информационной преступности). Стоит также отметить инициативу РФ, направленную на создание в 2019г. нового институционального механизма - Рабочей группы экспертов открытого состава, действующей на основании консенсуса с целью придания переговорному процессу в данной сфере более демократического, инклюзивного и транспарентного характера (A/RES/73/27). Принципиально новым является положение, согласно которому в работе группы смогут участвовать все без исключения государства-члены ООН, а не ограниченное число представителей в составе от 15 до 25 членов Группы правительственных экспертов. Мандат РГОС достаточно обширный и включает весь спектр вопросов, вынесенных на обсуждение в контексте проблемы международной информационной безопасности, включая дальнейшую работу над нормами, правилами и принципами ответственного поведения государств, вопрос применимости международного права к использованию ИКТ государствами, мер укрепления доверия и наращивания потенциала в сфере ИКТ, оценки существующих и потенциальных угроз, а также организацию регулярного

[16] Резолюция ГА ООН A/RES/58/32 от 8 декабря 2003г. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N03/454/85/PDF/N0345485.pdf?OpenElement

[17] Резолюция ГА ООН A/RES/66/24 от 2 декабря 2011г. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N11/460/28/PDF/N1146028.pdf?OpenElemen t

[18] Резолюция ГА ООН A/RES/73/27 от 5 декабря 2018г. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N18/418/07/PDF/N1841807.pdf?OpenElement

[19] Резолюция ГА ООН A/RES/73/187 от 17 декабря 2018г. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N18/450/56/PDF/N1845056.pdf?OpenElement

институционального диалога с широким кругом участников под эгидой ООН. Позиция российской стороны, отраженная в Резолюциях A/RES/74/29[20], A/RES/75/240 [21]«Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» развивает идею работы Рабочей группы открытого состава в 2019г., а также продление ее мандата на 2021-2025гг.

Американская инициативы в области МИБ отражены в Резолюциях A/RES/73/266[22], A/RES/74/28[23], A/RES/75/32[24] «Поощрение ответственного поведения государств в киберпространстве в контексте международной безопасности», отмечает продолжающуюся работу ГПЭ 6 созыва в 2019 – 2021гг., при этом не вносит никаких новых положений или дополнений по мандату группы, да и в целом по вопросу МИБ, оставляя это на рассмотрение ГА ООН на последующих сессиях после рассмотрения итогов работы ГПЭ и РГОС.

В результате анализа проделанной работы в направлении обеспечения международной информационной безопасности можно говорить о формировании международного информационного законодательства. Таким образом, современная ситуация характеризуется появлением нового «измерения» системы международной безопасности.

Между тем угрозы международному миру и безопасности, создаваемые ИКТ, не вынесены на обсуждение в Совете Безопасности ООН в качестве самостоятельной повестки дня. Представляется, что Совет безопасности ООН, являясь универсальной площадкой для обсуждения существующих угроз международному миру и безопасности, может вынести на рассмотрение военно-политические аспекты МИБ. Между тем, военно-политическое использование ИКТ является наиболее политизированной проблемой, влияющей на развитие глобального информационного общества. Данная ситуация во многом обусловлена различиями во взглядах между двумя обозначившимися блоками стран, во главе с РФ и США соответственно, относительно оценки угроз информационной безопасности и ключевого вопроса о возможности отнесения к таким угрозам использования ИКТ в военно-политических целях, а также подходов к регулированию информационного пространства и принципов, по которым оно будет функционировать.

Между тем, активно занимаясь проблемой противодействия террористическим угрозам, Совет Безопасности ООН принял ряд резолюций, отмечающих проблему использования ИКТ, в том числе сети Интернет, для содействия терроризму.

---

[20] Резолюция ГА ООН A/RES/74/29 от 12 декабря 2019г. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N19/410/10/PDF/N1941010.pdf?OpenElement

[21] Резолюция ГА ООН A/RES/75/240 от 31 декабря 2020г. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/000/28/PDF/N2100028.pdf?OpenElement

[22] Резолюция ГА ООН A/RES/73/266 от 22 декабря 2018г. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N18/465/04/PDF/N1846504.pdf?OpenElement

[23] Резолюция ГА ООН A/RES/74/28 от 12 декабря 2019г. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N19/410/03/PDF/N1941003.pdf?OpenElement

[24] Резолюция ГА ООН A/RES/75/32 от 7 декабря 2020г. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N20/354/02/PDF/N2035402.pdf?OpenElement

Так, Резолюция Совета Безопасности 1373 (2001) [25]содержит призыв к государствам-членам по активизации и ускорению обмена оперативной информацией об использовании ИКТ террористическими группами и пресечения вербовки террористов; Резолюция Совета Безопасности ООН 1624 (2005г.)[26], касающаяся запрета террористической деятельности, которая в том числе может осуществляться с использованием Интернета, а именно пропаганды, подстрекательства и оправдания идей терроризма; Резолюция Совета Безопасности 2129 (2013г.)[27] отмечает эволюционирующую взаимосвязь между терроризмом и развитием ИКТ, в частности Интернет, использование таких технологий для совершения террористических актов, а также содействия террористической деятельности путем подстрекательства, вербовки, финансирования или планирования террористических актов, осуществляемых через Интернет, социальные сети; Резолюция Совета Безопасности 2178 (2014г.)[28] об иностранных боевиках-террористах содержит призыв к государствам-членам действовать сообща при принятии национальных мер по недопущению использования террористами технологий, средств связи и ресурсов для подстрекательства к поддержке террористических актов. В 2017 году Совет Безопасности принял Резолюцию 2341 (2017)[29], посвященную вопросам защиты критических объектов инфраструктуры, расширению возможностей государств по предотвращению террористических нападений. Резолюция предлагает государствам-членам рассмотреть возможные превентивные меры при разработке национальных стратегий и политики кибербезопасности. Меры защиты охватывают широкий спектр, включая планирование, координацию и обмен оперативной и разведывательной информацией, скрининг, поиск, обнаружение, безопасность кибернетического пространства и др. К числу критически важных объектов инфраструктуры Резолюция относит, например, такие, которые используются, «для производства, передачи и распределения электроэнергии, воздушного, наземного и морского транспорта, предоставления банковских и финансовых услуг, водоснабжения, распределения продовольствия и общественного здравоохранения». Государства-члены в очередной раз подчеркивают необходимость объединения усилий на уровне государственного и частного сектора посредством проведения предметных консультаций, сотрудничества с операторами критически важных объектов инфраструктуры, должностными лицами

[25] Резолюция Совета Безопасности ООН S/RES/1373 (2001) https://documents-dds-ny.un.org/doc/UNDOC/GEN/N01/557/45/PDF/N0155745.pdf?OpenElement

[26] Резолюция Совета Безопасности ООН S/RES/1624 (2005) https://documents-dds-ny.un.org/doc/UNDOC/GEN/N05/510/54/PDF/N0551054.pdf?OpenElement

[27] Резолюция Совета Безопасности ООН S/RES/2129 (2013) https://documents-dds-ny.un.org/doc/UNDOC/GEN/N13/624/39/PDF/N1362439.pdf?OpenElement

[28] Резолюция Совета Безопасности ООН S/RES/2178 (2014) https://documents-dds-ny.un.org/doc/UNDOC/GEN/N14/548/01/PDF/N1454801.pdf?OpenElement

[29] Резолюция Совета Безопасности ООН S/RES/2341 (2017) https://documents-dds-ny.un.org/doc/UNDOC/GEN/N17/038/61/PDF/N1703861.pdf?OpenElement

правоохранительных органов и служб безопасности, с владельцами частного бизнеса, в том числе путем проведения совместных учебных мероприятий и применения или создания соответствующих сетей связи или экстренного оповещения (ч. 5). Резолюция призывает государства-члены к введению норм об уголовной ответственности за террористические акты против критически важных объектов инфраструктуры, а также за планирование, подготовку, финансирование и материально-техническую поддержку таких нападений.

3. СУЩЕСТВУЮЩИЕ УГРОЗЫ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.

Эксперты в области международной информационной безопасности выделяют так называемую триаду угроз (использование ИКТ в военных, террористических и преступных целях)[30]. Выделяемые три уровня требуют разных методов регулирования и имеют различные последствия в отношении глобальной информационной безопасности:

- Проблема предотвращения кибервойн относится к уровню международного публичного права и межправительственных отношений;
- Кибертерроризм имеет в своей основе политическую мотивацию и направлен против правительств, государственных органов и общества в целом;
- Киберпреступность – преступления, совершаемые обычными гражданами и пользователями Интернет в киберпространстве, посягающие на безопасность информационных данных, ресурсов и систем.

За последние пять лет отмечаются негативные тенденции, связанные с увеличением масштабов и негативных последствий данных угроз, что свидетельствует о необходимости принятия мер, направленных против незаконного использования ИКТ, и на недопущения их использования с целью подрыва международной безопасности. Стоит отметить, что в практическом плане присутствует смешение обозначенных трех категорий кибератак, поскольку существуют сложности как в плане идентификации пользователя, атрибуции (определение авторства деструктивных действий в информационном пространстве и ответственности за их осуществление), так и в определении четких терминологических, концептуальных, в последствии нормативных границ. Проблематика военно-политического использования ИКТ по-прежнему остается чувствительной для ряда государств и не всегда включается в повестку дня многостороннего международного взаимодействия.

Между тем, глобальное информационное пространство предоставило возможности трансграничного воздействия в

[30] Всестороннее исследование проблемы киберпреступности и ответных мер со стороны государств-членов, международного сообщества и частного сектора. Группа экспертов для проведения всестороннего исследования киберпреступности. Вена, 25-28 февраля 2013г. https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/UNODC_CCPCJ_EG4_2013_2_R.pdf; https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime_Study_Russian.pdf

нарушение национального государственного суверенитета, принципа невмешательства во внутренние дела государств. Это формирует новые вызовы в системе международных отношений, которые требует незамедлительного ответа. Именно в этой связи возникает и развивается концепция цифрового суверенитета государств. Суверенитет государства в ИКТ-среде означает его верховенство в пространстве вычислительных и информационных ресурсов. Концепцию цифрового суверенитета государств поддерживает большинство стран мира, между тем ряд государств-противников данной концепции выдвигают довод о том, что установление государственного контроля над национальным сегментом Интернет и содержанием информационного пространства, в силу его глобальности и трансграничности может повлечь нарушение прав иностранных пользователей на свободный доступ к информации, свободу искать, получать и распространять информацию и идеи любыми средствами и независимо от государственных границ (ст. 19 Всеобщей декларации прав человека[31], п. 3 ст. 19 Международного Пакта о гражданских и политических правах[32]).

По аспекту военно-политического использования ИКТ также стоит отметить, что в международном праве пока не выработаны общепризнанные понятия войны и вооруженной борьбы в информационном пространстве, хотя такие дефиниции содержатся в некоторых международных актах (Соглашение о сотрудничестве в области обеспечения международной информационной безопасности Шанхайской организации сотрудничества 2010 г.[33]). Между тем такие определения необходимы потому, что использование ИКТ в вооруженных конфликтах обладает рядом особенностей, затрудняющих его правовую регламентацию. К ним относятся, в частности, отсутствие предвоенного периода и, следовательно, невозможность определения начала силовых действий военного характера, реальность осуществления агрессивных действий с использованием ИКТ без нарушения границ государства, против которого такие действия направлены. Кроме того, ИКТ сами по себе не являются оружием. Все это затрудняет квалификация информационного воздействия как акта агрессии. Отсюда вытекает важность разработки определения понятия «информационное оружие». Изучению подлежат также следующие вопросы: можно ли рассматривать национальную информационную инфраструктуру как военный объект, против которого в случае киберконфликта может быть применено традиционное оружие; какие информационные инфраструктуры необходимо защищать от возможного противоправного использования ИКТ по

---

[31] **Всеобщая декларация прав человека**
Принята резолюцией 217 А (III) Генеральной Ассамблеи ООН от 10 декабря 1948 года https://www.un.org/ru/documents/decl_conv/declarations/declhr.shtml

[32] **Международный пакт о гражданских и политических правах**
Принят резолюцией 2200 А (XXI) Генеральной Ассамблеи от 16 декабря 1966 года https://www.un.org/ru/documents/decl_conv/conventions/pactpol.shtml

[33] Соглашение между правительствами государств - членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности (Екатеринбург, 16 июня 2009 г.) https://base.garant.ru/2571379/

гуманитарным соображениям; является ли использование ИКТ в целях нарушения стабильности и порядка в другом государстве вмешательством во внутренние дела. Этими и другими вопросами задаются специалисты и ученые при рассмотрении комплекса проблем модернизации действующего международного права.

В числе практических примеров кибератак на ИКТ-сети и инфраструктуру можно назвать применение вирусов Stuxnet, Duqu, Flame, Gauss против информационной инфраструктуры в государствах Ближнего Востока, атаки на сервера госучреждений и компаний частного сектора в Эстонии в 2007г., Грузии в 2008г. и др., которые трактуются рядом экспертов как эпизоды информационной войны[34].

Проведенный анализ международно-правового регулирования МИБ показывает, что на международной площадке взаимодействия. Прежде всего в ООН, идет интенсивная дискуссия, отражающая попытки государств найти действенные международно-правовые механизмы, необходимые для противодействия вызовам и угрозам в информационно-кибернетическом пространстве. Что подтверждает актуальность вынесения данной тематики на повестку дня предстоящего моделируемого заседания Совета Безопасности ООН в рамках Прикаспийской международной модели ООН 2022г.

4. БИБЛИОГРАФИЯ

1. Резолюция Совета Безопасности ООН S/RES/1373 (2001) https://documents-dds-ny.un.org/doc/UNDOC/GEN/N01/557/45/PDF/N0155745.pdf?OpenElement
2. Резолюция Совета Безопасности ООН S/RES/1624 (2005) https://documents-dds-ny.un.org/doc/UNDOC/GEN/N05/510/54/PDF/N0551054.pdf?OpenElement
3. Резолюция Совета Безопасности ООН S/RES/2129 (2013) https://documents-dds-ny.un.org/doc/UNDOC/GEN/N13/624/39/PDF/N1362439.pdf?OpenElement
4. Резолюция Совета Безопасности ООН S/RES/2178 (2014) https://documents-dds-ny.un.org/doc/UNDOC/GEN/N14/548/01/PDF/N1454801.pdf?OpenElement

[34] Олег Демидов ОБЕСПЕЧЕНИЕ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И РОССИЙСКИЕ НАЦИОНАЛЬНЫЕ ИНТЕРЕСЫ https://mail.pircenter.org/media/content/files/10/13559089230.pdf

5. Резолюция Совета Безопасности ООН S/RES/2341 (2017) https://documents-dds-ny.un.org/doc/UNDOC/GEN/N17/038/61/PDF/N1703861.pdf?OpenElement
6. Резолюция ГА ООН A/RES/53/70 от 4 декабря 1998г. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N99/760/05/PDF/N9976005.pdf?OpenElement
7. Резолюция ГА ООН A/RES/54/49 от 1 декабря 1999г. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N99/777/15/PDF/N9977715.pdf?OpenElement
8. Резолюция ГА ООН A/RES/55/28 от 20 декабря 2000г. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N00/561/09/PDF/N0056109.pdf?OpenElement
9. Резолюция ГА ООН A/RES/56/19 от 29 ноября 2001г. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N01/476/30/PDF/N0147630.pdf?OpenElement
10. Резолюция ГА ООН A/RES/57/53 от 22 ноября 2002г. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N02/541/47/PDF/N0254147.pdf?OpenElement
11. Резолюция ГА ООН A/RES/58/32 от 8 декабря 2003г. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N03/454/85/PDF/N0345485.pdf?OpenElement
12. Резолюция ГА ООН A/RES/66/24 от 2 декабря 2011г. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N11/460/28/PDF/N1146028.pdf?OpenElemen t
13. Резолюция ГА ООН A/RES/73/27 от 5 декабря 2018г. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N18/418/07/PDF/N1841807.pdf?OpenElement
14. Резолюция ГА ООН A/RES/73/187 от 17 декабря 2018г. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N18/450/56/PDF/N1845056.pdf?OpenElement
15. Резолюция ГА ООН A/RES/74/29 от 12 декабря 2019г. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N19/410/10/PDF/N1941010.pdf?OpenElement

16. Резолюция ГА ООН A/RES/75/240 от 31 декабря 2020г. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/000/28/PDF/N2100028.pdf?OpenElement
17. Резолюция ГА ООН A/RES/73/266 от 22 декабря 2018г. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N18/465/04/PDF/N1846504.pdf?OpenElement
18. Резолюция ГА ООН A/RES/74/28 от 12 декабря 2019г. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N19/410/03/PDF/N1941003.pdf?OpenElement
19. Резолюция ГА ООН A/RES/75/32 от 7 декабря 2020г. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N20/354/02/PDF/N2035402.pdf?OpenElement
20. Всеобщая декларация прав человека

Принята резолюцией 217 А (III) Генеральной Ассамблеи ООН от 10 декабря 1948 года *https://www.un.org/ru/documents/decl_conv/declarations/declhr.shtml*

21. Международный пакт о гражданских и политических правах

Принят резолюцией 2200 А (XXI) Генеральной Ассамблеи от 16 декабря 1966 года

https://www.un.org/ru/documents/decl_conv/conventions/pactpol.shtml

22. Соглашение между правительствами государств - членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности (Екатеринбург, 16 июня 2009 г.) https://base.garant.ru/2571379/
23. Достижения в области информации и телекоммуникаций в контексте международной безопасности : доклад Генерального секретаря A/54/213 | 1999-08-10 https://digitallibrary.un.org/record/286090?ln=ru
24. Всемирная встреча на высшем уровне по вопросам информационного общества

https://www.un.org/ru/events/pastevents/wsis.shtml

25. Окинавская хартия Глобального

информационного общества 21 июля 2000 года http://www.kremlin.ru/supplement/3170

26. Документ WSIS-03/GENEVA/DOC/4-R 12 декабря 2003 года Оригинал: английский Декларация принципов Построение информационного общества – глобальная задача в новом тысячелетии https://www.un.org/ru/events/pastevents/pdf/dec_wsis.pdf
27. Документ WSIS-03/GENEVA/DOC/5-R 12 декабря 2003 года Оригинал: английский План действий https://www.un.org/ru/events/pastevents/pdf/plan_wsis.pdf
28. Документ WSIS-05/TUNIS/DOC/6(Rev.1)-R 15 ноября 2005 года Оригинал: английский Председатель Подготовительного комитета Тунисского этапа ТУНИССКАЯ ПРОГРАММА ДЛЯ ИНФОРМАЦИОННОГО ОБЩЕСТВА https://www.un.org/ru/events/pastevents/pdf/agenda_wsis.pdf
29. Документ WSIS/PC-2/DOC/5-R 15 января 2003 года Оригинал: английский Записка Исполнительного секретариата ВВУИО ОТЧЕТ ОБЩЕЕВРОПЕЙСКОЙ РЕГИОНАЛЬНОЙ КОНФЕРЕНЦИИ ВВУИО (Бухарест, 7–9 ноября 2002 года) https://www.itu.int/dms_pub/itu-s/md/03/wsispc2/doc/S03-WSISPC2-DOC-0005!!PDF-R.pdf
30. Всестороннее исследование проблемы киберпреступности и ответных мер со стороны государств-членов, международного сообщества и частного сектора. Группа экспертов для проведения всестороннего исследования киберпреступности. Вена, 25-28 февраля 2013г. https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/UNODC_CCPCJ_EG4_2013_2_R.pdf; https://www.unodc.org/documents/organized-

crime/cybercrime/Cybercrime_Study_Russian.pdf
31. Министерство связи Российской Федерации ГОСУДАРСТВЕННАЯ КОМИССИЯ ПО ЭЛЕКТРОСВЯЗИ РЕШЕНИЕ от 25 декабря 2002 года N 49 Об итогах Полномочной конференции МСЭ (г.Марракеш, 2002 год) и работе на ней Администрации связи России https://docs.cntd.ru/document/901858785
32. Рассолов И.М. Право и кибернетическое пространство. Монография.- 2-е изд.-М.: Московское бюро по правам человека, 2016.С.7-10
33. Олег Демидов ОБЕСПЕЧЕНИЕ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И РОССИЙСКИЕ НАЦИОНАЛЬНЫЕ ИНТЕРЕСЫ https://mail.pircenter.org/media/content/files/10/13559089230.pdf
34. ИНДЕКС БЕЗОПАСНОСТИ № 1 (104), Том 19