# ЭКСПЕРТНЫЙ ДОКЛАД
# СОВЕТ БЕЗОПАСНОСТИ ООН

## ПОВЕСТКА: «КИБЕРКОНСЕНСУС: НА ПУТИ К ПОДДЕРЖАНИЮ МИРА И ЦИФРОВОЙ БЕЗОПАСНОСТИ»

ЧЕРНОМОРСКАЯ АССОЦИАЦИЯ МЕЖДУНАРОДНОГО СОТРУДНИЧЕСТВА
THE BLACK SEA ASSOCIATION FOR INTERNATIONAL COOPERATION

МОДЕЛЬ ООН В КРЫМУ

СТУДЕНЧЕСКОЕ НАУЧНОЕ ОБЩЕСТВО
РГУП
КРЫМСКИЙ ФИЛИАЛ

ПРИ ПОДДЕРЖКЕ
ГОСУДАРСТВЕННОГО КОМИТЕТА
МОЛОДЕЖНОЙ ПОЛИТИКИ
РЕСПУБЛИКИ КРЫМ

**МОДЕЛЬ ООН В КРЫМУ (21-23 октября 2022 год)**

**Авторы доклада:**

**Члены организационного комитета**

**Володькин Николай Дмитриевич**

**Лось Владислав Николаевич**

# СОДЕРЖАНИЕ

Введение……..3-5

1. Case study: Случаи применения сферы ИКТ, представляющие угрозу международной безопасности…….6-9

§1. Распространение ложной информации……..6-7

§2. ИКТ и терроризм……..7-8

§3. Хакерские атаки……...8-9

2. Международно-правовые аспекты поддержания мира и безопасности в сфере ИКТ…….10-20

3. Киберпространство и вооруженные конфликты…….21-24

Библиографический список……..25-30

Приложение №1 Рекомендуемые электронные ресурсы.....31

Приложение №2 Рекомендуемые вопросы для составления позиции страны…….32

Приложение №3 Рекомендуемые государства…….33

# ВВЕДЕНИЕ

Статьей 24 Устава Организации объединенных наций[1] на Совет Безопасности ООН (далее – СБ ООН) возложена главная ответственность за поддержание международного мира и безопасности.

Для этих целей СБ ООН уполномочивается расследовать любой спор или любую ситуацию, которые могут привести к международным трениям для определения того, не может ли продолжение этого спора или ситуации угрожать поддержанию международного мира и безопасности (статья 34 Устава ООН).

В случае возникновения любой угрозы миру, любого нарушения мира или акта агрессии, СБ ООН делает рекомендации сторонам спора, требует выполнения временных мер для пресечения возникшей угрозы, а также является единственным органом ООН уполномоченным вводить в отношении стран-агрессоров ограничения (санкции) экономического, политического и военного характера, которые имеют не односторонний субъективно-политический статус, а объективный, будучи выражением воль участников мирового сообщества (статьи 39-51 Устава ООН).

Технологизация современного общества, а равно политических, экономических и социальных отношений, создает для международных организаций новую сферу деятельности, поддержание мира и согласия в которой, как мы это покажем ниже, является чуть-ли не первостепенной задачей в 21-м веке.

Компьютерные технологии поистине стали частью жизни общества. Об этом свидетельствуют и статистические данные[1].

---

[1] Устав Организации Объединенных Наций (Сан-Франциско, 26 июня 1945 г.). // [Электронный ресурс] URL: https://www.un.org/ru/about-us/un-charter/full-text // «Действующее международное право» т. 1. // Ратифицирован Указом Президиума ВС СССР от 20 августа 1945 г. «О ратификации Устава Организации Объединенных Наций» // Сборник законов СССР и указов Президиума Верховного Совета СССР. 1938. 1975, т.2, с. 237.

Однако мирной, бытовой стороной «компьютеризация», к глубокому сожалению, не ограничивается. Опыт последних вооруженных конфликтов показывает, насколько «цифровизованным» – и от того более опасным и смертоносным – стало применяемое оружие[2]. Более того, нечто, что сегодня мы могли бы назвать компьютером, первоначально разрабатывалось именно для военных нужд[3].

Не менее серьезно обстоит вопрос о применении компьютерных технологий террористическими организациями в целях вербовки для совершения, подстрекательства к совершению, финансирования или планирования террористических актов[4].

Тем не менее, угрозы, которые могут настигнуть мировое сообщество, не ограничиваются военными действиями и деятельностью террористических организаций.

Все чаще мы стали слышать о случаях кибератак т.н. «хакерских группировок»[5].

Обозначенное положение дел вызывает серьезную обеспокоенность в вопросах поддержания всеобщего мира и безопасности, что свидетельствует о необходимости выработки основных международно-правовых принципов и норм взаимоотношения государств в сфере информационно-

---

[1] По данным глобального отчета «Digital 2022 April Global Statshot Report (Apr 2022)» аналитической платформы DataReportal на апрель 2022 года около 5 млрд. человек пользуются интернетом, 5.3 млрд. используют мобильные телефоны, а около 4.6 млрд. человек имеют аккаунты в социальных сетях. // [Электронный ресурс] URL: https://www.slideshare.net/DataReportal/digital-2022-april-global-statshot-report-apr-2022-v01).

[2] 102 государства используют беспилотные летательные аппараты (БПЛА) в военных целях, и по меньшей мере сорок из них имеют в своем арсенале такие аппараты, оснащенные оружием. По некоторым данным, 35 государств обладают боевыми беспилотниками с самой высокой поражающей силой.» - Специальный докладчик по внесудебным казням Аньес Калламар. // [Электронный ресурс] URL: https://news.un.org/ru/story/2020/07/1381761

[3] Liivoja R., McCormack T., Leins K. « Emerging Technologies of Warfare» // Routledge Handbook of the Law of Armed Conflic. P. 603. // [Электронный ресурс] URL: https://www.researchgate.net/publication/312173231_Emerging_Technologies_of_Warfare

[4] Кибербезопасность - Контртеррористическое управление ООН. // [Электронный ресурс] URL: https://www.un.org/counterterrorism/ru/cybersecurity

[5] 5 групп киберпреступников, которые вызывают беспокойство. Cyber Policy. // [Электронный ресурс] URL: https://www.cyberpolicy.com/cybersecurity-education/5-cybercrime-groups-making-organizations-uneasy

коммуникационных технологий; разработки основных мер по пресечению актов агрессии, как в сфере ИКТ, так и с помощью них; создание совершенно новых способов и методов разрешения споров между участниками международного сообщества в киберсфере.

Учитывая характер и важность обозначенных вопросов, принимая во внимание положения Глав V-VII Устава ООН, а также цели деятельности и комплекс полномочий Совета Безопасности ООН, от последнего требуется особо активная роль в их разрешении, поскольку именно от этого зависит сможет ли мировое сообщество предостеречь нашу Планету от надвигающихся угроз миру и безопасности, вызванных развитием сферы ИКТ.

# 1. CASE STUDY: СЛУЧАИ ПРИМЕНЕНИЯ СФЕРЫ ИКТ, ПРЕДСТАВЛЯЮЩИЕ УГРОЗУ МЕЖДУНАРОДНОЙ БЕЗОПАСНОСТИ

## §1. Распространение ложной информации

Информационные технологии дали свободный доступ к колоссальнейшему объему информации, получить которую можно в одно мгновение, но вместе с этим открыли доступ к свободному созданию и распространению этой информации. К сожалению, увеличению объема такой информации коррелируют снижение ее качества и уровня достоверности.

Распространение недостоверной, ложной информации влечет, как негативные последствия для обывателей, к примеру потребитель вводится в заблуждение ложной информацией о товаре, так и для международного сообщества в целом. Рассмотрим несколько ситуаций.

Эпидемия Covid-19 породила огромное количество фейков, как о самом вирусе, так и о вакцине против вируса, что создало значительные трудности в борьбе с пандемией, а равно серьезную угрозу для человечества.

«Население пугали введением военного положения, затем рассказывали о панацее от COVID-19, потом появилась новость о том, что вируса не существует, а больницы на самом деле пустуют. Чтобы фейк выглядел правдоподобно, порой в информацию вплетают немного правды. Например, на фоне дефицита вакцин в ВОЗ призвали не торопиться с ревакцинацией, чтобы жители всех стран могли получить вакцины. Противники вакцин же, ссылаясь на ВОЗ, заявили, что уважаемая организация выступает против вакцинации, умолчав тот факт, что вакцин просто не хватает.»[1]

[1] Оружие против фейков: знания, инновации, партнерство. // [Электронный ресурс] URL: https://news.un.org/ru/story/2022/01/1416312

Имеются и более опасные примеры: «В ответ на фейковую новость Пакистан пригрозил Израилю ядерным оружием»[1]. Один из новостных сайтов опубликовал фейковую новость с цитатой бывшего министра обороны Израиля об угрозах Пакистану в случае вторжение последнего в Сирию. В ответ на это министр обороны Пакистана пригрозил Израилю ядерным оружием. Позднее, возникшее «недоразумение» было улажено, однако в ином случае ситуация могла бы иметь критические последствия для всего человечества.

Как видно на реальных примерах, поддержание достоверности распространяемой информации сегодня является одной из важных задач по поддержанию мира и безопасности на планете.

## §2. ИКТ и терроризм

Применение террористическими организациями средств ИКТ создает новые и усиливает опасность уже существующих угроз.

«Инновация криптовалюты позволяет полностью выйти за пределы легального и создать собственные каналы движения финансовых средств по всему миру. Финансирование терроризма становится теперь полностью независимым от каких бы то ни было форм контроля, а значит и противодействия со стороны государственных и международных структур.»[2]

Значительную угрозу для международного правопорядка и безопасности представляет развитие теневых маркетплейсов. «Так, использование браузера-анонимайзера Tor не представляет сложности даже для рядового пользователя, а на даркнет-площадках этот пользователь может получить ряд нелегальных услуг: наркотические препараты, документы корпоративной и государственной тайны, оружие (в том числе взрывчатку и химическое оружие) …установка

[1] Fake news: дезинформация в медиа: пособие. Н. Муратова, Н. Тошпулатова, Г. Алимова. – Опубликовано в 2020 г. Организацией Объединённых Наций по вопросам образования, науки и культуры и Представительством ЮНЕСКО в Узбекистане. 2020. С.68.

[2] Сальников Е.В., Сальникова И.Н. Криптовалюта как инновация экономики террора. // Интернет-журнал «НАУКОВЕДЕНИЕ». Том 8, №3. (2016). С.5.

вирусного программного обеспечения и взлом вебсайтов, убийство по найму, химические вещества.»[1]

Не менее распространенной является практика применения террористами социальных сетей. «Исламское государство[2]», как известно, использует популярные интернет-сервисы, такие как *«Twitter»* и *«YouTube»*, для размещения видео, на которых боевики демонстрируют казни пленников, террористические атаки (например, теракт в Париже в ноябре 2015 г.) и вербуют новых членов.»[3]

Такое освещение террористической деятельности создает негативные последствия для стабильности общества, а продолжительность и системность такого «информирования» делает восприятие такой информации для общества обыденностью, что может повлечь снижение настороженности и бдительности человека к террористической угрозе.

### §3. Хакерские атаки

Большую озабоченность мирового сообщества вызвало появление т.н. хакерских группировок. Экспертным центром безопасности *Positive Technologies* проведено исследование[4] и сбор информации о нескольких крупных хакерских группировках, причастных к различного рода «киберпреступлениям».

Исследовательская организация в сфере киберпреступности *Cybersecurity Ventures* прогнозирует, что глобальные издержки от киберпреступлений будут

---

[1] Андронова И.В., Гусаков Н.П., Завьялова Е.Б. Финансирование терроризма: новые вызовы для международной безопасности. // Вестник международных организаций. Т. 15. № 1. С. 129.

[2] «Исламское государство/ИГИЛ», «ХАМАС», «Аш-Шабаб», «Twitter», «Facebook». ЗАПРЕЩЕННЫЕ НА ТЕРРИТОРИИ РОССИЙСКОЙ ФЕДЕРАЦИИ ТЕРРОРИСТИЧЕСКИЕ И ЭСКТРЕМИСТСКИЕ ОРГАНИЗАЦИИ.

[3] Проблема использования современных информационно-коммуникационных технологий международными террористическими организациями. Абазов К.М. // Вопросы безопасности. 2018. №3. С. 2

[4] Positive Technologies: исследование: Хакерские группировки. // [Электронный ресурс] URL: https://www.ptsecurity.com/ru-ru/research/hacker-groups/

расти на 15% в год в течение следующих пяти лет и к 2025 году достигнут 10,5 трлн долларов США в год по сравнению с 3 трлн долларов США в 2015 году.

Помимо экономических последствий, киберпреступления создают угрозу и для социальной стабильности в обществе в целом.

7 мая 2021 года была совершена кибератака на крупнейшую трубопроводную систему в США. Случившееся, вызвало серьезный дефицит топлива: через 4 дня после инцидента 8,5% заправочных станций в Северной Каролине и 7,7% в Вирджинии не имели бензина, во Флориде, Вирджинии и нескольких других штатах был введён режим чрезвычайного положения[1].

Угроза киберпреступности создала новый вызов для международного сообщества по борьбе с ней. Очевидным является тот факт, что для этих целей необходимо достижение международного консенсуса в сфере применения ИКТ, организация международного сотрудничества для создания и развития правовых механизмов по поддержанию кибербезопасности на планете.

[1] CNN: «Why Americans are panic buying fuel». // [Электронный ресурс] URL: https://edition.cnn.com/us/live-news/us-gas-demand-hack-05-11-21

# 2. МЕЖДУНАРОДНО-ПРАВОВЫЕ АСПЕКТЫ ПОДДЕРЖАНИЯ МИРА И БЕЗОПАСНОСТИ В СФЕРЕ ИКТ

На сегодняшний день международно-правовое регулирование сферы ИКТ находится в активной стадии зарождения, как в части нормативного материала, так и в части доктринальных разработок.

В деятельности ООН вопросы сферы ИКТ, с учетом характера и предмета своих компетенций, разрешаются и разрабатываются Советом Безопасности ООН и Генеральной Ассамблеей ООН, где последняя занимает несколько более активную роль.

Вопрос информационной безопасности был внесен в повестку дня ООН, когда в 1998 году Российская Федерация впервые представила проект резолюции на заседании Первого комитета Генеральной Ассамблеи. На основе этого проекта 4 января 1999 г. была принята Резолюция Генеральной ассамблеи ООН 53/70[1].

Указанной резолюцией странам-участникам было предложено отразить свои позиции по следующим вопросам (п.1-4):

- общая оценка проблемы информационной безопасности;

- определить основные понятия в сфере информационной безопасности;

- целесообразность разработки международных принципов, которые были бы направлены на укрепление безопасности глобальных информационных и телекоммуникационных систем, а также способствовали борьбе с информационным терроризмом и криминалом.

Учитывая позиции государств-участников ООН по указанным в резолюции 53\70 вопросам, Генеральный секретарь ООН ежегодно

[1] Резолюция 53/70, принятая ГА ООН 4 января 1999 года. // [Электронный ресурс] URL: https://undocs.org/A/RES/53/70

представляет доклад по вопросу об ИКТ в контексте международной безопасности[1].

В последнем докладе Генерального секретаря ООН за 2021[2] отмечается ряд достижений стран участников.

К примеру, Австралия в 2021 году представила Международную стратегию взаимодействия с кибернетическими и критически важными технологиями[3]. Стратегия выделяет три основных элемента — ценности, безопасность и процветание — для руководства международным участием Австралии в области кибербезопасности и важнейших технологий.

В Дании функционирует Центр кибербезопасности *(Centre for Cybersecurity)*[4], деятельность которого основана на частно-публичном партнерстве. Целью деятельности центра является консультирование государственных органов по вопросам укрепления кибербезопасности и улучшения обмена знаниями между органами власти, предприятиями и исследователями.

В свою очередь, в 2019 году Агентство по кибербезопасности Сингапура *(Cyber Security Agency of Singapore)* представило генеральный план кибербезопасности операционных технологий[5].

Безусловно, не меньшего внимания заслуживают достижения и других стран, отраженных в рассматриваемом докладе Генерального секретаря ООН.

18 декабря 2003 года на 58-й сессии Генеральной Ассамблеи ООН была принята Резолюция 58/32[6]; на основании 4 пункта этой резолюции была создана

---

[1] Годовые отчеты Генерального секретаря с изложением мнений государств-членов ООН по вопросу об ИКТ в контексте международной безопасности. // [Электронный ресурс] URL: https://www.un.org/disarmament/ict-security/

[2] Advancing responsible State behavior in cyberspace in the context of international security (A/76/187 19.07.2021). // [Электронный ресурс] URL: https://undocs.org/en/A/76/187

[3] Australia's Cyber and Critical Tech Cooperation Program. // [Электронный ресурс] URL: https://www.internationalcybertech.gov.au/our-work/capacity-building

[4] Danish Centre for Cyber Security. // [Электронный ресурс] URL: https://www.cfcs.dk/en

[5] Singapore's Operational Technology Cybersecurity (Masterplan 2019). // [Электронный ресурс] URL: https://www.csa.gov.sg/News/Publications/OT-Cybersecurity-Masterplan

[6] Резолюция 58/32, принятая ГА ООН 4 января 1999 года. // [Электронный ресурс] URL:

группа правительственных экспертов *(Groups of Governmental Experts)*. Группа работала в период с 2004 по 2005 г. Начиная с 2009 года такие группы создавались несколько раз (см. информационный бюллетень работы групп[1]) и представляли свои отчеты.

В докладе за 2012-2013 г.г. 68/98[2] правительственная группа пришла к очень важным вывода о допустимости применения международного права к отношениям, возникающим в сфере ИКТ:

- Международное право, и, в частности, Устав Организации Объединенных Наций, применимо и имеет важное значение для поддержания мира и стабильности и создания открытой, безопасной, мирной и доступной информационной среды.

- Государственный суверенитет и международные нормы, и принципы, вытекающие из принципа государственного суверенитета, распространяются на поведение государств в рамках деятельности, связанной с использованием ИКТ, а также на юрисдикцию государств над ИКТ-инфраструктурой на их территории.

- Предпринимаемые государством усилия по обеспечению безопасности ИКТ должны гармонично сочетаться с уважением прав человека и основных свобод, закрепленных во Всеобщей декларации прав человека и других международных инструментах.

Отдельного внимания заслуживают доклады экспертных правительственных групп за 2014-2015 г.г. 70/174[3] и 2019-2021 г.г. 76/135[4].

---

https://undocs.org/A/RES/58/32

[1] Информационный бюллетень работы групп правительственных экспертов. // [Электронный ресурс] URL: https://front.un-arm.org/wp-content/uploads/2019/07/Information-Security-Fact-Sheet-July-2019.pdf

[2] Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности 68/98 от 24 июня 2013 года. // [Электронный ресурс] URL: https://undocs.org/A/68/98

[3] Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности 70/174 от 22 июля 2015 года. // [Электронный ресурс] URL: https://undocs.org/A/70/174

[4] Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности 70/174 от 14 июля 2021 года. // [Электронный ресурс] URL:

Генеральная Ассамблея ООН резолюциями 70/237[1] и 76/19[2] призвала государства-члены при использовании информационно-коммуникационных технологий руководствоваться докладами Группы правительственных экспертов 2015 и 2021 года в которых были отмечены довольно важные рекомендации по участию государств в поддержании международной кибербезопасности:

- Разработка процедур взаимопомощи в деле реагирования на инциденты и решения краткосрочных проблем в сфере обеспечения безопасности сетей, включая процедуры оказания оперативной помощи;

- Оказание содействия в сфере проведения необходимых экспертиз или принятия совместных мер по противодействию преступному или террористическому использованию ИКТ;

- Оказание помощи в обеспечении доступа к технологиям, которые считаются существенно важными для обеспечения безопасности ИКТ;

- Уделение особого внимания распространению информации и наращиванию потенциала в сфере обеспечения безопасности ИКТ в национальных планах и государственных бюджетах;

- Создание и укрепление потенциала *CERTs (Computer emergency response team* – компьютерная группа реагирования на чрезвычайные ситуации) и укрепление механизмов сотрудничества по линии *CERTs*.

Стоит отметить, что резолюция 76/19 была принята по совместной инициативе Российской Федерации и Соединенных Штатов Америки. В Резолюции было отмечено о том, что *добровольные*, не имеющие обязательной силы нормы ответственного поведения государств могут снизить риски для международного мира, безопасности и стабильности, и не предусматривают

---

https://undocs.org/A/76/135

[1] Резолюция 70/237, принятая ГА ООН 23 декабря 2015 года. // [Электронный ресурс] URL: https://undocs.org/A/RES/70/237

[2] Резолюция 76/19, принятая ГА ООН 6 декабря 2021 года. // [Электронный ресурс] URL: https://undocs.org/en/A/RES/76/19

ограничения или запрета действий, согласующихся с нормами международного права, однако устанавливают стандарты ответственного поведения государств.

По нашему мнению, акцент на добровольности норм, устанавливающих требования к поведению государств в сфере ИКТ, в некоторой степени соответствует балансу общемеждународных и индивидуально-государственных интересов, ограничивая давление международного права на суверенитеты государств, оставляя вопрос на следование таким нормам на усмотрение каждого государства, но при таком подходе, добровольные правила становится слабоэффективным механизмом международного взаимодействия, который ов такой ситуации основывается на исключительно субъективном видении каждым государством своей ответственности за поведение и действия, совершаемые на международной арене.

Помимо подхода, основанного на добровольности норм международного права, имеется и иной, основанный на обязывающем и предписывающем характере норм об ответственном поведении стран в среде ИКТ.

Конкуренция таких подходов к регулированию сферы ИКТ, особенно явно обозначилась, когда Российская Федерация[1] и Соединенные Штаты[2] представили проекты резолюций к 73 сессии ГА ООН по вопросу безопасности в киберсреде.

Различие проектов сводится к следующему: «Конструктивная часть *[проекта Резолюции, предложенного США – курсив Н.В., В.Л.]* сводится к призыву к правительствам добровольно присоединиться к «правилам ответственного поведения» и «добровольным и необязывающим нормам» поведения в киберпространстве.»[3]; «Предложения России содержат 25 пунктов,

[1] «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» – проект Резолюции ГА ООН к его 73-й сессии, предложенный Российской Федерацией. // [Электронный ресурс] URL: http://undocs.org/ru/A/C.1/73/L.27

[2] «Поощрение ответственного поведения государств в киберпространстве в контексте международной безопасности» проект Резолюции ГА ООН к его 73-й сессии, предложенный Соединенными Штатами Америки. // [Электронный ресурс] URL: http://undocs.org/ru/A/C.1/73/L.27

[3] D-Russia: Генассамблее ООН предстоит выбрать между правилами кибервойны или её предупреждением. //

каждый из которых включает слова «государства должны»…Россия предлагает разработать и кодифицировать международное право специально для киберпространства, описав правила выхода из коллизий, возникновение которых можно предвидеть уже сегодня.»[1]

Однако расхождения имеются не только касательно общего подхода: «Содержательный же раскол можно проследить по целому ряду вопросов регулирования ИКТ: применимость международного права к информационной сфере, применимость гуманитарного права к информационной сфере и в особенности выработка международного договора по МИБ.»[2]

22 октября 2018 года была принята Резолюция 73/27[3] ГА ООН, основой которой стал проект Резолюции, предложенный Российской Федерацией. Отметим основные положения:

- Указания на то, что та или иная деятельность в сфере ИКТ была начата или иным образом происходит с территории или объектов ИКТ-инфраструктуры государства, может быть недостаточным для присвоения этой деятельности указанному государству;

- Государства не должны заведомо позволять использовать свою территорию для совершения международно-противоправных деяний с использованием ИКТ и использовать посредников для совершения международно-противоправных деяний с использованием ИКТ;

- Государства должны удовлетворять соответствующие просьбы об оказании помощи, поступающие от других государств, критически важная инфраструктура которых становится объектом злонамеренных действий в

---

[Электронный ресурс] URL: https://d-russia.ru/genassamblee-oon-predstoit-vybrat-mezhdu-pravilami-kibervojny-ili-eyo-preduprezhdeniem.html

[1] Там же.

[2] Международная информационная безопасность: подходы России / Крутских А.В., Зиновьева Е.А., .Булва ., В.И., Алборова М.Б., Юдина Ю.А.; под ред. Крутских . А.В., Зиновьева Е.С. — Москва, 2021. — 48 с. — Текст : непосредственный – С.24.

[3] Резолюция 73/27 принятая ГА ООН 5 декабря 2018 года. // [Электронный ресурс] URL: https://undocs.org/ru/A/RES/73/27)

сфере ИКТ;

- Государства должны стремиться предупреждать распространение злонамеренных программных и технических средств в сфере ИКТ и использование скрытых вредоносных функций.

Принимая во внимание высокую ценность позиций, выработанных Генеральной Ассамблеей ООН, все же больший интерес для нашего доклада имеют позиции Совета Безопасности ООН по вопросам поддержания мира в условиях развития ИКТ.

Рассматриваемая нами проблема впервые была отражена в Резолюции СБ ООН 1373 (2001)[1], когда СБ ООН призвал государства найти возможности активизации и ускорения обмена оперативной информацией об использовании террористическими группами коммуникационных технологий.

Позднее СБ ООН в документе Doc. 2015/939[2] распространил и призвал учитывать Руководящие принципы в отношении иностранных боевиков-террористов (Мадридские принципы)[3], которые содержат важные рекомендации по пресечению использования террористическими организациями средств ИКТ:

- Государства, региональные организации, частный сектор и гражданское общество должны наладить эффективные партнерские отношения в целях выработки более совершенных методов отслеживания и изучения террористических материалов, распространяемых через Интернет и с помощью других коммуникационных технологий (принцип №13);

- Государства-члены должны рассмотреть возможность пересмотра национального законодательства для обеспечения того, чтобы доказательства,

[1] Резолюция 1373 (2001) принятая Советом Безопасности 28 сентября 2005 г. // [Электронный ресурс] URL: http://undocs.org/ru/S/RES/1373(2001)

[2] Приложение I к письму Председателя Комитета Совета Безопасности, учрежденного резолюцией 1373 (2001) о борьбе с терроризмом, от 15 декабря 2015 года на имя Председателя Совета Безопасности. // [Электронный ресурс] URL: https://undocs.org/S/2015/939

[3] Мадридские принципы (Madrid guiding principles) – разработаны Комитетом Совета Безопасности ООН, учрежденным Резолюцией СБ ООН 1373 (2001), для контроля за осуществлением этой резолюции.

собранные с помощью средств ИКТ и социальных сетей, в том числе посредством электронного наблюдения, могли признаваться допустимыми в контексте рассмотрения дел, связанных с иностранными боевиками-террористами, и при этом уважать международные стандарты в области прав человека, включая свободу выражения мнения (принцип №25);

- Государства-члены должны создать в национальных правоохранительных органах информационно-коммуникационную и экспертно-криминалистическую базу и укрепить способность правоохранительных органов отслеживать в социальных сетях материалы, связанные с терроризмом, с тем чтобы пресекать поток иностранных боевиков-террористов таким образом, чтобы это не противоречило международным обязательствам государств в отношении прав человека (принцип №26);

В развитии международно-правового противодействия применения террористами средств ИКТ важное значение имеет Крайстчерчский призыв[1], который был подписан после теракта 15 марта 2019 года[2] в Новой Зеландии, и которым подписавшие его стороны призвали мировое сообщество:

- разрабатывать инструменты для предотвращения загрузки контента террористического и насильственного экстремистского содержания;

- повышать информационную открытость при обнаружении и удалении контента;

- следить за тем, чтобы алгоритмы, разрабатываемые и используемые предприятиями, не направляли пользователей на контент насильственного экстремистского содержания, что позволит сократить его вирусное распространение.

[1] Christchurch Call to eliminate terrorist and violent extremist online content adopted from 16 may 2019 – (Доступ URL: https://www.beehive.govt.nz/release/christchurch-call-eliminate-terrorist-and-violent-extremist-online-content-adopted

[2] Стрельба в мечетях Крайстчерча. // [Электронный ресурс] URL: https://ru.wikipedia.org/wiki

Таким образом, СБ ООН рассматривает вопросы кибербезопасности, преимущественно в контексты террористической угрозы.

Представляется, что в настоящее время действительно, именно применение террористами средств ИКТ является наиболее серьезной угрозой для международной безопасности, что и обуславливает внимание СБ ООН именно с этой стороны к рассматриваемому вопросу.

Конвенционное регулирование международной кибербезопасности находится на стадии становления.

В 2001 году Советом Европы была разработана Конвенция о компьютерных преступлениях[1], присоединиться к которой может любое государство планеты. В настоящее время Конвенция ратифицирована 67 странами мира[2].

Конвенцией был обозначен ряд деяний, совершаемых с применением средств ИКТ, и которые государствам-участникам конвенции следует имплементировать в национальное уголовное законодательство:

- Противозаконный доступ к компьютерной системе или ее части;

- Неправомерный перехват данных;

- Воздействие на данные;

- Воздействие на функционирование компьютерной системы;

- Противозаконное использование программ, технических устройств, кодов доступа, разработанных или созданных исключительно для целей совершения указанных выше преступлений.

Конвенция, также содержит международно-правовые предписания для подписавших стран, в части определения неправомерных действий в

[1] Конвенция о преступности в сфере компьютерной информации ETS N 185 (Будапешт, 23 ноября 2001 г.) // Российская Федерация не является участников конвенции. // [Электронный ресурс] URL: https://rm.coe.int/1680081580

[2] Таблица подписаний и ратификаций Конвенции о преступности в сфере компьютерной информации ETS №185 (Будапешт, 23 ноября 2001 г.). // [Электронный ресурс] URL: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185

компьютерной системе и их юридические состав, которые подписавшие страны должны включить в национальное уголовное право или применить иные правовые средства противодействия такого рода деяниям, но обеспечивающим не меньшую эффективность, что уголовно-правовые механизмы.

Конвенцией также определены некоторые процессуальные особенности расследования и рассмотрения дел по такого рода деяниям. Отдельное вниманием уделено вопросам доказательств и доказывания, которые представляют наибольшую сложность, поскольку необходимо обеспечить баланс публичных интересов (предотвращение\расследование общественно опасного деяния) и частных интересов (уважение тайны частной жизни и ее неприкосновенности при сборе и сохранении доказательств).

В 2003 году был принят Первый протокол о ксенофобии и расизме к Конвенции о компьютерных преступлениях[1]. Указанным протоколом были обозначены меры, которые следует принять государствам, присоединившимся к протоколу, для пресечения любых форм ксенофобии и расизма в компьютерной среде.

В частности, каждая сторона Протокола:

- Принимает соответствующие законодательные меры для квалификации в качестве уголовных преступлений деяния по распространению и обеспечению общего доступа через компьютерные системы к материалу расистского и ксенофобского содержания, угроз и оскорблений, совершенных на почве расизма и ксенофобии, когда такие деяния совершены умышлено и противоправно.

По нашему мнению, большинство национальных уголовных законодательств признает обозначенные деяния в качестве преступных, однако

[1] Первый протокол о ксенофобии и расизме (Страсбург, 28 января 2003 года) от к Конвенции о преступности в сфере компьютерной информации ETS №185 (Будапешт, 23 ноября 2001 г.). // [Электронный ресурс] URL: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189 // Неофициальный перевод на русский. // [Электронный ресурс] URL: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=189

отмечается, что «единое терминологическое закрепление понятия киберпреступности и правовое регулирование отношений в киберпространстве должны быть достигнуты только путем создания и ратификации универсальной Конвенции по борьбе с киберпреступностью. ООН обладает единственным потенциалом для реализации такой универсальной меры.»[1]

[1] Талипова Л.Р. Международно-правовая регламентация киберпреступности. // Гуманитарные, социально-экономические и общественные науки. 2016. №4 – С.122.

## 3. КИБЕРПРОСТРАНСТВО И ВООРУЖЕННЫЕ КОНФЛИКТЫ

Отдельный вопрос, который стоит рассмотреть – это киберпространство и вооруженные конфликты. Выше мы обозначили доклады правительственных групп за 2013 г. и 2015 г, которыми было отмечено, что нормы международного права, в частности Устав ООН, применимы к информационной среде.

В практическом плане указанный тезис вызывает сложности правоприменения норм международного гуманитарного права (далее - МГП) к вооруженным конфликтам с применение средств ИКТ.

Международным комитетом красного креста (далее - МККК) была представлена позиция[1] по вопросу применимости МГП к «кибероперациям» во время вооруженных конфликтов, которая содержит следующие тезисы:

- МГП ограничивает применение кибероружия во время вооруженного конфликта так же, как любого другого оружия, средств и методов ведения войны — и новых, и старых;

- В ситуации вооруженного конфликта объекты гражданской инфраструктуры защищены от кибератак существующими принципами и нормами МГП, в частности принципами проведения различия, соразмерности и принятия мер предосторожности во время нападения. МГП также предоставляет особую защиту больницам и объектам, необходимым для выживания гражданского населения;

- Во время вооруженных конфликтов запрещено применение киберсредств, которые распространяются неизбирательно и при этом наносят неизбирательный ущерб;

- Толкование государствами существующих норм МГП определит, в какой степени МГП защищает от последствий кибероперациий.

[1] Международное гуманитарное право и кибероперации во время вооруженных конфликтов - позиционный документ МККК. // [Электронный ресурс] URL: https://www.icrc.org/en/document/international-humanitarian-law-and-cyber-operations-during-armed-conflicts

Как представляется, одной только констатации факта применения МГП к вооруженным конфликтам с киберэлементом недостаточно, поскольку имеются некоторые практические трудности такого применения, вызванные техническими особенностями киберсреды, как таковой.

Указанные проблемы были обозначены и рассмотрены в работе сотрудников МККК: «Двадцать лет спустя: международное гуманитарное право и защита гражданских лиц от последствий кибероперациий во время вооруженных конфликтов»[1], где были отмечены следующие тезисы:

- Выражение «кибероперации во время вооруженных конфликтов» МККК понимает как означающее операции против компьютерной системы, или сети, или иного подключенного к сети устройства через поток данных, когда такие операции применяются в качестве средства или метода войны в контексте вооруженного конфликта;

- Если использование кибероперациий в отношениях между государствами приводит к последствиям, схожим с последствиями использования более традиционных средств и методов войны, МГП может быть применимо независимо от того используются ли в конфликте традиционные средства. Позиции государств по данному вопросу неоднозначны.

Многие нормы МГП, регулирующие ведение военных действий, применяются только к военным операциям, которые являются «нападениями» по определению МГП, поэтому необходимо определить, когда кибероперации являются нападением по смыслу норм МГП. МККК занял такую позицию: операция, предназначенная для выведения из строя компьютера или компьютерной сети во время вооруженного конфликта, является нападением по определению МГП, независимо от того, выведен ли объект из строя

[1] Жизель Л., Роденхойзер Т., Дёрман К. «Двадцать лет спустя: международное гуманитарное право и защита гражданских лиц от последствий кибероперациий во время вооруженных конфликтов». // Международный журнал Красного Креста, № 913 (2021 г.) Цифровые технологии и война. С.367-425. // [Электронный ресурс] URL: https://international-review.icrc.org/ru/articles/twenty-years-ihl-effects-of-cyber-operations-during-armed-conflicts-913

в результате уничтожения или каким-либо иным способом. Позиции государств по данному вопросу, также неоднозначны.

Защита гражданских данных от вредоносных кибероперациий во время вооруженных конфликтов, должна признаваться такой же необходимой, как и защита гражданских объектов, поскольку данные — это важнейший компонент цифровой сферы и краеугольный камень жизни во многих обществах: личные медицинские данные, данные органов социального обеспечения, налоговые сведения, банковские счета, файлы клиентов компаний и списки избирателей крайне важны для функционирования большинства систем гражданской жизни.

Как видно, технические особенности киберсреды влекут сообразные трудности в применении норм международного права. В условиях все большего распространения использования киберсредств в вооруженных конфликтах, вопросы применения и применимости норм МГП должны быть разрешены первостепенно, однако мировому сообщество еще только предстоит достигнуть консенсуса по решению этих вопрос.

Учитывая сказанное, руководствуясь главой II Временных правил процедуры СБ ООН (S/96/Rev.7)[1], делегатам-участникам рекомендуется представить позиции стран по следующим вопросам повестки дня:

1. Общая оценка внутригосударственных угроз кибербезопасности;

2. Предпринимаемые представляемым государством усилия по обеспечению безопасности в сфере ИКТ, в частности:

- Борьба с распространением фейков;

- Меры по исключению доступа к недопустимому контенту;

- Борьба с активным применением средств ИКТ террористическими организациями;

[1] Временные правила процедура Совета Безопасности ООН. (S/96/Rev.7). // [Электронный ресурс] URL: https://www.un.org/securitycouncil/ru/content/provisional-rules-procedure

3. Применяются ли в представляемых странах принципы, изложенные в докладах экспертных правительственных групп за 2014-2015 г.г. (A/RES/68/243) и 2019-2021 г.г. (A/RES/73/266);

4. Позиция представляемых государств о применимости норм международного гуманитарного права к вооруженным конфликтам с применением средств ИКТ;

5. Позиция представляемых государств, касательно целесообразности создания в Совете Безопасности ООН специального комитета по вопросу поддержания международного мира и безопасности в сфере применения средств ИКТ, в частности, предложения (позиции) о структуре, предмете ведения такого комитета;

# БИБЛИОГРАФИЧЕСКИЙ СПИСОК

***Конвенции и иные международно-правовые акты:***

1. Устав Организации Объединенных Наций (Сан-Франциско, 26 июня 1945 г.). // [Электронный ресурс] URL: https://www.un.org/ru/about-us/un-charter/full-text // «Действующее международное право» т. 1 // Ратифицирован Указом Президиума ВС СССР от 20 августа 1945 г. «О ратификации Устава Организации Объединенных Наций». // Сборник законов СССР и указов Президиума Верховного Совета СССР. 1938 - 1975, т. 2, с. 237.

2. Конвенция о преступности в сфере компьютерной информации ETS №185 (Будапешт, 23 ноября 2001 г.). // Российская Федерация не является участников конвенции. // [Электронный ресурс] URL: https://rm.coe.int/1680081580

3. Первый протокол о ксенофобии и расизме (Страсбург, 28 января 2003 года) от к Конвенции о преступности в сфере компьютерной информации ETS №185 (Будапешт, 23 ноября 2001 г.). // [Электронный ресурс] URL: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=189)

***Резолюции Генеральной Ассамблеи ООН:***

1. Резолюция 53/70, принятая ГА ООН 4 января 1999 года. // [Электронный ресурс] URL: https://undocs.org/A/RES/53/70

2. Резолюция 58/32, принятая ГА ООН 4 января 1999 года. // [Электронный ресурс] URL: https://undocs.org/A/RES/58/32

3. Резолюция 70/237, принятая ГА ООН 23 декабря 2015 года. // [Электронный ресурс] URL: https://undocs.org/A/RES/70/237

4. Резолюция 73/27 принятая ГА ООН 5 декабря 2018 года. // [Электронный ресурс] URL: https://undocs.org/ru/A/RES/73/27

5. Резолюция 76/19, принятая ГА ООН 6 декабря 2021 года. // [Электронный ресурс] URL: https://undocs.org/en/A/RES/76/19

6. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» – проект Резолюции ГА ООН к его 73-й сессии, предложенный Российской Федерацией. // [Электронный ресурс] URL: http://undocs.org/ru/A/C.1/73/L.27

7. «Поощрение ответственного поведения государств в киберпространстве в контексте международной безопасности» проект Резолюции ГА ООН к его 73-й сессии, предложенный Соединенными Штатами Америки. // [Электронный ресурс] URL: http://undocs.org/ru/A/C.1/73/L.27

***Резолюции и иные акты Совете Безопасности ООН:***

1. Резолюция 1373 (2001) принятая Советом Безопасности 28 сентября 2005 г. // [Электронный ресурс] URL: http://undocs.org/ru/S/RES/1373(2001)

2. Приложение I к письму Председателя Комитета Совета Безопасности, учрежденного резолюцией 1373 (2001) о борьбе с терроризмом, от 15 декабря 2015 года на имя Председателя Совета Безопасности. // [Электронный ресурс] URL: https://undocs.org/S/2015/939

***Доклады и отчеты Генерального секретаря ООН, правительственных и иных экспертных групп:***

1. Глобальный отчет «Digital 2022 April Global Statshot Report (Apr 2022)» аналитической платформы. // [Электронный ресурс] URL: https://www.slideshare.net/DataReportal/digital-2022-april-global-statshot-report-apr-2022-v01

2. Бесконтрольное использование беспилотников – выдержка из отчета независимого докладчика ООН по внесудебным казням Аньес Калламар. //

[Электронный ресурс] URL: https://news.un.org/ru/story/2020/07/1381761

3. 5 групп киберпреступников, которые вызывают беспокойство. Cyber Policy. // [Электронный ресурс] URL: https://www.cyberpolicy.com/cybersecurity-education/5-cybercrime-groups-making-organizations-uneasy

4. Positive Technologies: исследование: Хакерские группировки. // [Электронный ресурс] URL: https://www.ptsecurity.com/ru-ru/research/hacker-groups/

5. Годовые отчеты Генерального секретаря с изложением мнений государств-членов ООН по вопросу об ИКТ в контексте международной безопасности. // [Электронный ресурс] URL: https://www.un.org/disarmament/ict-security/

6. Информационный бюллетень работы групп правительственных экспертов. // [Электронный ресурс] URL: https://front.un-arm.org/wp-content/uploads/2019/07/Information-Security-Fact-Sheet-July-2019.pdf

7. Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности 68/98 от 24 июня 2013 года. // [Электронный ресурс] URL: https://undocs.org/A/68/98

8. Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности 70/174 от 22 июля 2015 года. // [Электронный ресурс] URL: https://undocs.org/A/70/174

9. Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности 70/174 от 14 июля 2021 года. // [Электронный ресурс] URL: https://undocs.org/A/76/135

10. Advancing responsible State behavior in cyberspace in the context of international security (A/76/187 19.07.2021). // [Электронный ресурс] URL:

https://undocs.org/en/A/76/187

11. Australia's Cyber and Critical Tech Cooperation Program. // [Электронный ресурс] URL: https://www.internationalcybertech.gov.au/our-work/capacity-building

12. Danish Centre for Cyber Security. // [Электронный ресурс] URL: https://www.cfcs.dk/en

13. Singapore’s Operational Technology Cybersecurity (Masterplan 2019). // [Электронный ресурс] URL: https://www.csa.gov.sg/News/Publications/OT-Cybersecurity-Masterplan

***Иные источники:***

1. Liivoja R., McCormack T., Leins K. « Emerging Technologies of Warfare» // Routledge Handbook of the Law of Armed Conflic - P. 603. // [Электронный ресурс] URL: https://www.researchgate.net/publication/312173231_Emerging_Technologies_of_Warfare

2. Оружие против фейков: знания, инновации, партнерство. // [Электронный ресурс] URL: https://news.un.org/ru/story/2022/01/1416312

3. Fake news: дезинформация в медиа: пособие. Н. Муратова, Н. Тошпулатова, Г. Алимова. – Опубликовано в 2020 г. Организацией Объединённых Наций по вопросам образования, науки и культуры и Представительством ЮНЕСКО в Узбекистане. 2020. – С.68.

4. Сальников Е.В., Сальникова И.Н. Криптовалюта как инновация экономики террора. // Интернет-журнал «НАУКОВЕДЕНИЕ» Том 8, №3 (2016) – С.5.

5. Андронова И.В., Гусаков Н.П., Завьялова Е.Б. Финансирование терроризма: новые вызовы для международной безопасности. // Вестник международных организаций. Т. 15. № 1. С. 129.

6. Абазов К.М. Проблема использования современных информационно-

коммуникационных технологий международными террористическими организациями. // Вопросы безопасности. 2018. №3. С. 2.

7. D-Russia: Генассамблее ООН предстоит выбрать между правилами кибервойны или её предупреждением. // [Электронный ресурс] URL: https://d-russia.ru/genassamblee-oon-predstoit-vybrat-mezhdu-pravilami-kibervojny-ili-eyo-preduprezhdeniem.html

8. Международная информационная безопасность: подходы России / Крутских А.В., Зиновьева Е.А., Булва В.И., Алборова М.Б., Юдина Ю.А.; под ред. Крутских А.В., Зиновьева Е.С. — Москва, 2021. — 48 с. — Текст : непосредственный – С.24.

9. Стрельба в мечетях Крайстчерча. // [Электронный ресурс] URL: https://ru.wikipedia.org/wiki

10. Таблица подписаний и ратификаций Конвенции о преступности в сфере компьютерной информации ETS №185 (Будапешт, 23 ноября 2001 г.). // [Электронный ресурс] URL: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185

11. Талипова Л.Р. Международно-правовая регламентация киберпреступности. // Гуманитарные, социально-экономические и общественные науки. 2016. №4 С.122.

12. Международное гуманитарное право и кибероперации во время вооруженных конфликтов - позиционный документ МККК. // [Электронный ресурс] URL: https://www.icrc.org/en/document/international-humanitarian-law-and-cyber-operations-during-armed-conflicts

13. Жизель Л., Роденхойзер Т., Дёрман К. «Двадцать лет спустя: международное гуманитарное право и защита гражданских лиц от последствий кибероперaций во время вооруженных конфликтов». // Международный журнал Красного Креста, № 913 (2021 г.). Цифровые технологии и война – с.367-425. // [Электронный ресурс] URL: https://international-review.icrc.org/ru/articles/twenty-

years-ihl-effects-of-cyber-operations-during-armed-conflicts-913

**ПРИЛОЖЕНИЕ №1**

## РЕКОМЕНДУЕМЫЕ ЭЛЕКТРОННЫЕ РЕСУРСЫ

1. Официальный интернет-сайт ОНН. // [Электронный ресурс] URL: https://www.un.org/ru/

2. Кибербезопасность - Контртеррористическое управление ООН. // [Электронный ресурс] URL: https://www.un.org/counterterrorism/ru/cybersecurity

3. Официальный интернет-сайт СБ ООН. // [Электронный ресурс] URL: https://www.un.org/securitycouncil/ru

4. Официальный интернет-сайт, где размещены резолюции СБ ООН. // [Электронный ресурс] URL: https://www.un.org/securitycouncil /ru/content/resolutions

5. Официальный интернет-сайт Генеральной Ассамблеи ООН. // [Электронный ресурс] URL: https://www.un.org/ru/ga/

6. Официальный интернет-сайт, где размещены резолюции Генеральной Ассамблеи ООН. // [Электронный ресурс] URL: https://www.un.org/ru/ga/documents/gares.shtml

7. Официальный интернет-сайт Международного комитета красного креста. // [Электронный ресурс] URL: https://www.icrc.org/ru

8. Официальный интернет-сайт Африканского союза. // [Электронный ресурс] URL: https://au.int/

**ПРИЛОЖЕНИЕ №2**

**Рекомендуемые** вопросы, которые делегаты могут отразить в позиции представляемых стран (выбирать стоит наиболее актуальные для представляемой страны):

- Общая оценка внутригосударственных угроз кибербезопасности;
- Предпринимаемые представляемым государством усилия по обеспечению безопасности в сфере ИКТ, в частности:
- Борьба с распространением фейков;
- Меры по исключению доступа к недопустимому контенту;
- Борьба с активным применением средств ИКТ террористическими организациями;
- Применяются ли в представляемых странах принципы, изложенные в докладах экспертных правительственных групп за 2014-2015 г.г. (A/RES/68/243) и 2019-2021 г.г. (A/RES/73/266);
- Позиция представляемых государств о применимости норм международного гуманитарного права к вооруженным конфликтам с применением средств ИКТ;
- Позиция представляемых государств, касательно целесообразности создания в Совете Безопасности ООН специального комитета по вопросу поддержания международного мира и безопасности в сфере применения средств ИКТ, в частности, предложения (позиции) о структуре, предмете ведения такого комитета.

**Приложение №3**

## РЕКОМЕНДУМЫЕ ГОСУДАРСТВА

| | |
|---|---|
| Албания | Мексика |
| Бразилия | Норвегия |
| Габон | Объединенные Арабские Эмираты |
| Гана | Российская Федерация |
| Индия | Соединенное Королевство Великобритании и Ирландии |
| Ирландия | США |
| Кения | Франция |
| Китай | |