RS Global Journals

Scholarly Publisher
RS Global Sp. z O.O.
ISNI: 0000 0004 8495 2390

Dolna 17, Warsaw, Poland 00-773
Tel: +48 226 0 227 03
Email: editorial_office@rsglobal.pl

JOURNAL	International Journal of Innovative Technologies in Social Science
p-ISSN	2544-9338
e-ISSN	2544-9435
PUBLISHER	RS Global Sp. z O.O., Poland

ARTICLE TITLE	INTERNATIONAL LEGAL DOCUMENTS IN THE SPHERE OF ENSURING PEACE AND SECURITY IN THE DIGITAL AGE: CLASSIFICATION AND DEVELOPMENT TRENDS
AUTHOR(S)	Khamdamova Firuza Urazalievna
ARTICLE INFO	Khamdamova Firuza Urazalievna. (2024) International Legal Documents in the Sphere of Ensuring Peace and Security in the Digital Age: Classification and Development Trends. *International Journal of Innovative Technologies in Social Science*. 3(43). doi: 10.31435/rsglobal_ijitss/30092024/8228
DOI	https://doi.org/10.31435/rsglobal_ijitss/30092024/8228
RECEIVED	14 August 2024
ACCEPTED	27 September 2024
PUBLISHED	29 September 2024
LICENSE	This work is licensed under a **Creative Commons Attribution 4.0 International License.**

INTERNATIONAL LEGAL DOCUMENTS IN THE SPHERE OF ENSURING PEACE AND SECURITY IN THE DIGITAL AGE: CLASSIFICATION AND DEVELOPMENT TRENDS

Khamdamova Firuza Urazalievna
Doctoral student of National Center for Human Rights of the Republic of Uzbekistan
Doctor of Philosophy in Legal Sciences (PhD)

DOI: https://doi.org/10.31435/rsglobal_ijitss/30092024/8228

ARTICLE INFO

Received 14 August 2024
Accepted 27 September 2024
Published 29 September 2024

KEYWORDS

International Security Law, Cybersecurity, Cybercrime, Cyber Warfare, Combat Robots, Cyberspace.

ABSTRACT

This article is devoted to the review and analysis of international legal documents in the field of ensuring international security, adopted taking into account the development of digital technologies. The author emphasizes that the rapid development of digital technologies has become an important factor determining the state of international security.

The article provides the author's classification of international legal acts in the field of international security in the context of global digital transformation. Thus, the author distinguishes three groups of documents: 1) international legal acts adopted within the framework of international security law and international information law regarding information security/cybersecurity; 2) international legal acts adopted within the framework of international criminal law against cybercrime and cyberterrorism; 3) international legal acts adopted within the framework of international humanitarian law/law of armed conflict against cyber warfare and rules of warfare in cyberspace.

At the same time, most of the adopted documents are non-binding, which indicates the absence of a universally recognized international consensus on issues of ensuring international security. This is due to the fact that the issue of the legal status of cyberspace has not yet been settled in international law.

The article notes the role of regional organizations in developing international standards in the field of ensuring international security, especially such as the Council of Europe and the SCO.

The article also touches upon issues of the prospects for developing rules for conducting cyber warfare and recognizing the legal personality of combat robots.

Citation: Khamdamova Firuza Urazalievna. (2024) International Legal Documents in the Sphere of Ensuring Peace and Security in the Digital Age: Classification and Development Trends. *International Journal of Innovative Technologies in Social Science*. 3(43). doi: 10.31435/rsglobal_ijitss/30092024/8228

Современное международное право формировалось в рамках ООН. Поэтому современное международное право называют «право ООН». Основные цели ООН и цели современного международного права совпадают. Одна из целей ООН, закрепленных в статье 1 Уставе ООН, - «Поддерживать международный мир и безопасность и с этой целью принимать эффективные коллективные меры для предотвращения и устранения угрозы миру и подавления актов агрессии или других нарушений мира и проводить мирными средствами, в согласии с

принципами справедливости и международного права, улаживание или разрешение международных споров или ситуаций, которые могут привести к нарушению мира».[1]

Проблема безопасности – классическая в Вестфальской политической системе мира. До сих пор обеспечение мира и безопасности остается ключевой задачей международно-правового сотрудничества. Это отражено и в структуре ООН, в которой одним из главных органов является Совет Безопасности ООН. Согласно ст. 39 Устава ООН, Совет Безопасности ООН обладает полномочием определять «существование любой угрозы миру» и решать, какие меры следует предпринять для поддержания или восстановления международного мира и безопасности: меры, не связанные с использованием вооружённых сил (ст. 41 Устава ООН), или меры, связанные с использованием воздушных, морских и сухопутных сил (ст. 42 Устава ООН).

Одним из факторов, влияющих на международную безопасность, стало бурное развитие цифровых технологий. Современный технический прогресс не стоит на месте, однако все его достижения могут приносить как пользу современному обществу, так и негативно влиять на развитие международного мира и правопорядка.[2]

Роль международного права в создании системы международной безопасности сводится к решению следующих задач:

а) обеспечение функционирования того механизма обеспечения мира, который уже есть у мирового сообщества, и укрепление существующего международного правопорядка;

б) создание новых международно-правовых норм, отвечающих современным реалиям обеспечения безопасности.[3]

Это обуславливает необходимость разработки международно-правовых норм и принятия международно-правовых актов касательно безопасного применения цифровых технологий.

На данный момент международным сообществом принято множество актов касательно обеспечения международной безопасности в условиях цифровой трансформации. Большое количество таких документов обуславливает необходимость их классификации и систематизации. Международные договоры можно классифицировать по различным основаниям.

Так, по юридической природе можно выделить документы императивного и декларативного, или обязательного и рекомендательного характера. По вопросам обеспечения международной безопасности в условиях цифровизации приняты документы как обязательного характера в виде конвенций, так и рекомендательного характера в виде резолюций Генеральной Ассамблеи ООН или деклараций.

По кругу регулируемых вопросов можно выделить общие (посвященные в целом вопросам безопасности и затрагивающие вопросы применения цифровых технологий) и специальные договоры (посвященные именно вопросам международной безопасности в условиях развития цифровых технологий).

По географическому охвату или территориальной сфере действия можно выделить также документы универсального характера (например, в рамках ООН) и регионального характера (в рамках Совета Европы, ШОС, СНГ и так далее).

На основе обзора международно-правовых актов по вопросам обеспечения международной безопасности в условиях цифровой трансформации считаем целесообразным выделить следующие группы актов:

а) международно-правовые акты, принятые в рамках права международной безопасности и международного информационного права касательно информационной безопасности/кибербезопасности.

Еще в декабре 1998 г. Генеральная Ассамблея (ГА) приняла консенсусом (без голосования) резолюцию "Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности" (документ A/RES/53/70). Приняв этот документ, международное сообщество признало сам факт существования проблемы обеспечения информационной безопасности, и эта тема была включена в повестку дня работы ГА ООН. Позже были приняты ряд других резолюций ГА ООН, в частности, Резолюция 57/239 ГА ООН от 20 декабря 2002 года о создании глобальной культуры кибербезопасности, Резолюция 56/121

[1] Устав ООН, 1945 г. Текст документа доступен на https://www.un.org/ru/about-us/un-charter/full-text
[2] Канунникова Н.Г. Современные вызовы и угрозы международной безопасности. // Социально-политические науки 5’2018. – С.231.
[3] Игнатьева И.В. Международная безопасность и актуальные проблемы ее обеспечения // глаголъ правосудия 2(14) / 2017. – С.88.

ГА ООН от 2 декабря 2009 года о борьбе с преступным использованием информационных технологий, Резолюция 55/63 ГА ООН от 22 января 2001 года о борьбе с преступным использованием информационных технологий, Резолюция 68/243 ГАООН от 27декабря 2013 года о достижениях в сфере информатизации и телекоммуникаций в контексте международной безопасности[1] и др.

Дальнейшее обсуждение вопросов информационной безопасности позволило выделить два основных подхода к проблеме информационной безопасности – российский и западный. Россия делала акцент на угрозе информационной войны, а США и Европа считали наиболее важным разработать меры информационной безопасности применительно к угрозам террористического и криминального характера.

В этой ситуации Россия перенесла центр своей активности на региональный уровень. В октябре 2006 г. состоялось учредительное заседание группы экспертов государств – членов ШОС (председатель А. Крутских), которым было поручено выработать к саммиту в Бишкеке (2007 г.) план действий и определить пути решения проблемы МИБ в рамках компетенции стран-членов. В таком контексте главы государств ШОС договорились о возможных совместных мерах по устранению информационных угроз при соблюдении норм международного права. В ходе Бишкекского саммита был утверждён План совместных действий по обеспечению МИБ, а 16 июня 2009 г. в Екатеринбурге подписано межправительственное Соглашение государств – членов ШОС о сотрудничестве в области обеспечения МИБ. Уникальность этого документа заключалась в том, что он впервые на международно-правовом уровне зафиксировал наличие конкретных угроз в области информационной безопасности, а также определил основные направления, принципы, формы и механизмы сотрудничества в этой сфере. Как в рамках ШОС, так и в широкой международной практике вступившее в силу Соглашение стало первым договорным актом, охватывающим весь спектр проблем МИБ – от противодействия кибирпреступности и кибертерроризму до вопросов разоружения[2]. Это соглашение ратифицировали четыре участника ШОС (Россия, Китай, Казахстан, Таджикистан), и 2 июня 2011 г. оно вступило в силу.

Вышеупомянутые вопросы нашли своё отражение в докладе Генеральному секретарю ООН по вопросам информационной безопасности, представленном на 65-й сессии ГА в июле 2010 г. Документ подготовила группа правительственных экспертов 15-и стран. 12 сентября 2011 г. на 66-й сессии ГА постпреды РФ, Китая, Таджикистана и Узбекистана при ООН предложили совместный проект "Правил поведения в области обеспечения международной информационной безопасности"[3], а 22 сентября 2011 г. на закрытой встрече глав спецслужб и силовых ведомств 52 стран в Екатеринбурге был представлен разработанный Советом безопасности и МИД проект Конвенции об обеспечении информационной безопасности ООН[4]. Эти два документа взаимосвязаны и создают предпосылки для дальнейшего комплексного обсуждения проблемы МИБ на международном уровне. Проект Конвенции опирается на принятые ранее резолюции ГА ООН – "Роль науки и техники в контексте международной безопасности и разоружения" от 20 ноября 2000 г. (A/RES/55/29) и "Создание глобальной культуры кибербезопасности и оценка национальных усилий по защите важнейших информационных инфраструктур" от 21 декабря 2009 г. (A/RES/64/211). Таким образом, проект сохраняет преемственность с принятыми ранее документами ООН[5].

[1] Резолюции ГА ООН касательно ИКТ доступны на https://www.un.org/ru/development/ict/res.shtml

[2] Соглашение стран ШОС о сотрудничестве в области информационной безопасности вступило в силу // ИнфоШОС: интернет-портал. 2011. 16 июня. URL: http:// www.infoshos.ru/ru/?idn=8381

[3] Правила поведения в области обеспечения международной информационной безопасности: Приложение к письму постоянных представителей Китая, Российской Федерации, Таджикистана и Узбекистана при Организации Объединённых Наций от 12 сентября 2011 г. на имя Генерального секретаря: A/66/359: [Подлинный текст на английском, китайском и русском языках] / Генеральная Ассамблея ООН: Шестьдесят шестая сессия. 2011. 14 сентября.

[4] Конвенция об обеспечении международной информационной безопасности ООН (концепция), 21–22 сентября 2011 г. // EXPO IT Security: интернет-проект. URL: http://expo-itsecurity.ru/upload/iblock/a2f/Convention.pdf.

[5]Текст документа доступен на https://docs-library.unoda.org/Open Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/RUS_Concept_of_UN_Convention__on_International_Information_Security_Proposal_of_the_Russian__Federation_0.pdf

Помимо усилий, принимаемые в рамках ООН, подкрепляются мерами на региональном уровне. Так, принят модельный закон СНГ «Об информации, информатизации и обеспечении информационной безопасности»[1].

б) международно-правовые акты, принятые в рамках международного уголовного права против киберпреступности и кибертерроризма.

Генеральная Ассамблея ООН приняла резолюцию о создании Специального комитета (СК) по разработке Конвенции ООН о противодействии использованию информационно-коммуникационных технологий в преступных целях[2]. Участие в СК в разной степени открыто для всех государств-членов, а также наблюдателей (таких как ЕС и Совет Европы), гражданского общества и неправительственных организаций (НПО). Функции секретариата СК выполняет Управление ООН по наркотикам и преступности (УНП ООН). На данный момент СК обсуждается Сводный переговорный документ (СПД), а также проект текста предлагаемых положений Конвенции, созданный на основе предложений стран-участниц. [3]

Сводный переговорный документ содержит общие положения о криминализации действий, о процессуальных мерах и правоохранительной деятельности. Идея разработать конвенцию о борьбе с использованием информационных технологий в преступных целях получила одобрение в ходе 74-й сессии Генеральной Ассамблеи ООН. Инициатором соответствующей резолюции выступила Россия. В принятой тогда резолюции «Противодействие использованию информационно коммуникационных технологий в преступных целях» было предложено учредить специальный межправительственный комитет для разработки международной конвенции.[4]

В мае 2010 г. благодаря российской инициативе Комиссия ООН по предупреждению преступности и уголовному правосудию приняла решение создать открытую межправительственную группу экспертов для всеобъемлющего изучения проблем киберпреступности.

В настоящее время наиболее авторитетным международно-правовым актом комплексного характера является Конвенция Совета Европы о компьютерных преступлениях от 23 ноября 2001 года [5] . Также был принят Дополнительный протокол к Конвенции о преступлениях в сфере компьютерной информации, об инкриминировании расистских

актов и совершенного ксенофоба при помощи информационных систем.[6]

В СНГ действует Соглашение о сотрудничестве государств–участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий[7].

Отдельное внимание уделяется вопросам борьбы с кибертерроризмом. Контртеррористическое управление Организации Объединенных Наций (КТУ ООН) реализует ряд инициатив в области новых технологий, включая проект по использованию социальных сетей для сбора информации из открытых источников и цифровых доказательств в целях борьбы с терроризмом и насильственным экстремизмом при соблюдении прав человека. Управление делится своими экспертными знаниями по использованию беспилотных летательных аппаратов (БЛА) на международных форумах и будет разрабатывать другие программы в этой области.

Программа по кибербезопасности и использованию новых технологий направлена на укрепление потенциала государств-членов и частных организаций по предотвращению кибератак террористов на важнейшие объекты инфраструктуры. Программа также направлена на смягчение последствий кибератак на отдельные системы и их восстановление после нападения.[8]

Информационный терроризм рассматривается в качестве угрозы информационной безопасности в Соглашении между правительствами государств - членов Шанхайской

[1] Текст документа доступен на http://www.parliament.am/library/modelayin%20orenqner/310.pdf
[2] Текст документа доступен на https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Comments/RF_28_July_2021_-_R.pdf
[3] Хронология обсуждений Конвенции ООН о киберпреступности. https://www.eff.org/ru/deeplinks/2023/04/un-cybercrime-treaty-timeline
[4] В Вене проходят переговоры по разработке конвенции о борьбе с киберпреступностью. [Эл.ресурс]URL: https://news.un.org/ru/story/2023/01/1436692
[5] Текст документа доступен на https://rm.coe.int/1680081580
[6]Текст документа доступен на https://rm.coe.int/123015-rus-conventioncybercrimininalite-1-/1680a59a2b
[7] Текст документа доступен на https://lex.uz/docs/4748982
[8] Текст документа доступен на https://www.un.org/counterterrorism/ru/cybersecurity

организации сотрудничества о сотрудничестве в области обеспечения информационной безопасности[1].

в) международно-правовые акты, принятые в рамках международного гуманитарного права/права вооруженных конфликтов против кибервойн и правил ведения войн в киберпространстве.

Международный комитет красного креста (МККК) разработал правила ведение войн в киберпространстве. Появление подобного документа происходит впервые — всё больше гражданских лиц вовлекается в вооруженные конфликты с помощью цифровых устройств. Всего насчитывается восемь правил:

1. Не направлять кибератаки на гражданские объекты;
2. Не использовать вредоносное программное обеспечение, которое распространяется автоматически и наносит безразборный ущерб как военным, так и гражданским объектам;
3. Избегать или сводить к минимуму последствия, к которым операция может привести гражданское население;
4. Не проводить никаких кибероперациий против медицинских и гуманитарных объектов;
5. Не проводить никаких кибератак против объектов, необходимых для выживания населения;
6. Не угрожать насилием с целью посеять террор среди гражданского населения;
7. Не провоцировать нарушения МГП;
8. Соблюдать указанные правила, даже если противник этого не делает.

Также уместно упомянуть «Таллиннское руководство по международному законодательству, применимому к кибервойне» (The Tallinn Manual on the International Law Applicable to Cyber Warfare). Это академическое, не имеющее обязательной силы исследование того, как международное право (в частности, jus ad bellum и международное гуманитарное право) применяется к конфликтам и войнам в информационном пространстве. В 2009-2012 гг. «Таллинское руководство» было написано по приглашению расположенного в Таллине Киберцентра НАТО международной группой, состоящей из более чем двадцати экспертов. В апреле 2013 года Руководство было опубликовано издательством Кембриджского университета. Руководство является независимым академическим исследовательским продуктом, представляющим только точку зрения его авторов. Практика подготовки не имеющих обязательной силы руководств по применению международного гуманитарного права не нова — например, по такому же принципу были созданы «Руководство по международному праву, применимому к вооруженным конфликтам на море» Международного института гуманитарного права в Сан-Ремо и «Руководство по международной политике в области гуманитарной помощи и исследованию конфликтов» Гарвардской программы по международному праву, применимому к воздушным и ракетным вооруженным конфликтам.

В феврале 2017 г. был разработан проект под названием «Таллин 2.0» с целью расширения сферы применения «Таллинского руководства». Основное внимание в оригинальном Руководстве уделяется наиболее разрушительным и разрушительным кибернетическим операциям, которые квалифицируются как «вооруженные нападения» и, следовательно, позволяют государствам реагировать в порядке самообороны, а также тем, которые происходят во время вооруженного конфликта. В «Таллин 2.0» говорится об «информационных операциях», а не о «конфликтах».

Помимо правил ведения кибервойны особый интерес представляет вопрос о применении боевых роботов. Касательно применения боевых роботов следует выделить ряд ключевых вопросов.

Первый вопрос – это вопрос понятийного аппарата. В научной литературе встречаются «боевые автономные роботизированные системы» (Lethal autonomous robotics, LARs, «автономные системы вооружения» «смертоносные автономные системы вооружений» (Lethal autonomous weapons systems), «робототехника» и «автономные системы вооружения». Данные термины схожи во многом, но не тождественны[2].

[1] Текст документа доступен на https://lex.uz/ru/docs/2068478

[2] Мохат П.М. К вопросу о соответствии автономных интеллектуальных систем вооружений принципам международного гуманитарного права// Вестник военного права, 2/2018. - С.59

Следующий вопрос – считать ли боевых роботов новым видом оружия или солдатом. Данный вопрос актуален в силу того, что роботы способны осуществлять самостоятельные действия и адаптироваться к окружающей среде. Однако, означает ли это, что робот может быть субъектом права. Одни авторы отмечают, что даже при наличии высокого уровня физической автономии разумный робот не может быть признан субъектом права и на современном этапе даже самые «продвинутые» роботы должны быть признаны «имуществом особого рода»[1]. Другие авторы считают, роботы могут быть субъектом права, ведь они не просто помогают человеку, являясь пассивным инструментом в его руках, а способны заменить человека, действовать самостоятельно и адаптироваться к окружающей среде[2].

Несмотря на аргументы о том, что применение боевых роботов может обеспечить снижение человеческих жертв, возникает ряд вопросов: можно ли обеспечить соблюдение принципов МГП роботами, если даже люди не всегда соблюдают их? Если робот может принимать решение о смерти, не превращает это человека в объект? Именно от способности роботов соблюдать принципы МГП будет зависеть признание его правосубъектности. Главный риск - возрастающая автономность робота несет в себе угрозу постепенного ослабления (возможно утраты) контроля человека за применением силы. Применение боевых роботов ставит под угрозу обеспечение соблюдения важнейших принципов МГП – принципов избирательности и соразмерности. Кроме того, может усилить гонку вооружений между державами-лидерами в борьбе за лидерство в данном направлении[3].

С учетом рисков в обеспечении соблюдения роботами принципов МГП, возникает вопрос об ответственности за нарушения норм МГП роботами. Если роботов рассматривать как средство войны, ответственность за нарушения норм МГП лежит на государстве. Но если робот заменяет человека? Среди наиболее популярных: привлечение к юридической ответственности (уголовной и гражданской) оператора, программиста либо самой корпорации изготовителя машин, а также привлечение к международно-правовой ответственности государства, которое направило их для участия в вооруженном конфликте[4].

С учетом вышеуказанных вопросов, на которые пока не имеется однозначного ответа, на международных форумах обсуждаются следующие варианты правового регулирования: - ограничить разработку и применение боевых роботов;- наложить запрет на их разработку и использование[5]. Использование роботов в вооруженных конфликтах может быть разрешено, только если они будут способны соблюдать принципы МГП. В 2013 году специальный докладчик ООН по вопросу о внесудебных казнях, казнях без надлежащего судебного разбирательства или произвольных казнях К. Хейнс рекомендовал ввести национальный мораторий на автономное оружие ввиду отсутствия достоверных данных об их способности действовать в соответствии с нормами МГП. Сегодня это проблема технического характера, решение которой будет влиять на законность присутствия роботов в зоне ведения военных действий[6].

27–31 августа 2018 г. в Женеве под эгидой ООН прошли переговоры Группы экспертов по САС, где признали необходимость сохранить ответственность человека за принятие решений о применении таких систем вооружений. Аналогично, в Заявлении от 18 октября 2018 г. для Первого комитета Генеральной Ассамблеи ООН по разоружению и международной безопасности П. Асаро, представляя Международный Комитет по контролю за роботизированным оружием и Кампанию по остановке роботов, отметил настоятельную необходимость в превентивном запрете роботов[7]. В настоящее время международное

[1] Габов А.В., Хаванова И.А. Автономия боевых роботов и право. [Эд.ресурс] URL: https://cyberleninka.ru/article/n/avtonomiya-boevyh-robotov-i-pravo

[2] Габов А.В., Хаванова И.А. Автономия боевых роботов и право. [Эд.ресурс] URL: https://cyberleninka.ru/article/n/avtonomiya-boevyh-robotov-i-pravo

[3] Хамдамова Ф. Правовой статус роботов в международном гуманитарном праве // Юрист ахборотномаси – Вестник юриста – Lawyer herald. № 2 (2022) С. 131-134

[4] Скуратова А. Ю., Королькова Е. Е. Смертоносные автономные системы вооружений: проблемы международно-правового регулирования. // Российский юридический журнал. – 2019. – №1 (124). – С. 22- 30

[5] Скуратова А. Ю., Королькова Е. Е. Смертоносные автономные системы вооружений: проблемы международно-правового регулирования. // Российский юридический журнал. – 2019. – №1 (124). – С. 22- 30

[6] Скуратова А. Ю., Королькова Е. Е. Смертоносные автономные системы вооружений: проблемы международно-правового регулирования. // Российский юридический журнал. – 2019. – №1 (124). – С. 22- 30

[7] Габов А.В., Хаванова И.А. Автономия боевых роботов и право. [Эд.ресурс] URL: https://cyberleninka.ru/article/n/avtonomiya-boevyh-robotov-i-pravo

сообщество обсуждает данный вопрос, главным образом, в рамках и в увязке с Конвенцией ООН 1980 г. о запрещении или ограничении применения конкретных видов обычного оружия, которые могут считаться наносящими чрезмерные повреждения или имеющими неизбирательное действие (Конвенция о «негуманном» оружии, КНО). Большинство государств придерживаются мнения о недопустимости потери значимого человеческого контроля в отношении роботов. Однако, исследователи отмечают, что полный запрет использования боевых роботов на международном уровне весьма маловероятен.[1]

Вариантом правового регулирования данного вопроса может стать не разработка нового международного договора, а принятие дополнительного протокола к Конвенции о «негуманном» оружии 1980 г.[2] При этом, необходимо полностью запретить их применение в отношении гражданских лиц и объектов. Гражданское население должно иметь возможность быть оповещенным о месте расположения роботов. Боевой робот должен иметь отличительные знаки, позволяющие идентифицировать его как военный объект. При проектировании их внешнего вида не должны применяться какие-либо вероломные способы их маскировки под безопасные объекты. Стороны вооруженного конфликта должны будут уведомлять друг друга о намерении использовать роботов в конкретной военной операции.

Международным сообществом достигнут консенсус по поводу сохранения «значимого человеческого контроля» при применении роботов[3]. Данный принцип должен быть закреплен во всех правовых документах касательно боевых роботов.

До принятия международно-правового документа об основных принципах использования боевых роботов и создания механизмов его контроля, важно решить концептуальные вопросы касательно правосубъектности роботов, а также ответственности и мер наказания за нарушения норм МГП. Следует четко обозначить конкретные случаи, когда применение боевых роботов допустимо. Вопрос должен решаться с учетом всех рисков, которые несут роботы человеческой жизни. После достижения консенсуса по ключевым вопросам, целесообразно принять документ юридически обязательного характера «Основные принципы применения боевых роботов», состоящий из следующих разделов: 1. Основные понятия; 2. Правовой статус боевых роботов; 3. Основные принципы применения боевых роботов (заблаговременное уведомление об их применении, значимый человеческий контроль, предупреждение рисков); 4. Условия для применения боевых роботов; 5. Основания и виды ответственности в случае нарушения норм МГП; 6. Механизмы контроля и гарантии. 7. Международное сотрудничество и координация[4]. При этом, договор не должен допускать оговорок (аналогично договорам по борьбе с терроризмом или ядерным вооружениям). В рамках договора следует создать эффективный контрольный механизм и предусмотреть процедуру регулярной отчетности. Таким образом, при решении данного вопроса следует исходить из того, что одна из важнейших целей МГП – минимизация негативных последствий войны и защита человеческой жизни[5].

Таким образом, на сегодняшний день принято множество международно-правовых актов на универсальном и региональном уровне, как обязательного, так и рекомендательного характера, в целях обеспечения международной безопасности в условиях стремительного развития цифровых технологий.

В данном исследовании предлагается их разграничить на документы, принятые в рамках права международной безопасности, международного гуманитарного права и международного уголовного права. Данные акты признают, что цифровые технологии могут нести угрозу безопасности и призывают к применению цифровых технологий только в мирных целях. Они также направлены на правовое регулирование киберпространства и разработку правил

[1] Мохат П.М. К вопросу о соответствии автономных интеллектуальных систем вооружений принципам международного гуманитарного права// Вестник военного права, 2/2018. - С.59.

[2] Скуратова А. Ю., Королькова Е. Е. Смертоносные автономные системы вооружений: проблемы международно-правового регулирования. // Российский юридический журнал. – 2019. – №1 (124). – С. 22- 30

[3] Jarna Petman, LL.D. Autonomous weapons systems and international humanitarian law: ‘out of the loop’? Helsinki 2017.Available at https://um.fi/documents/35732/48132/autonomous_ weapon_systems_an_international_humanitarian_law__out_of_the/c0fca818-3141-b690-0337 7cfccbed3013?t=1525645981157

[4] Хамдамова Ф. Правовой статус роботов в международном гуманитарном праве // Юрист ахборотномаси – Вестник юриста – Lawyer herald. № 2 (2022) С. 131-134.

[5] Хамдамова Ф. Правовой статус роботов в международном гуманитарном праве // Юрист ахборотномаси – Вестник юриста – Lawyer herald. № 2 (2022) С. 131-134

поведения в киберпространстве. Большая часть документов носит рекомендательный характер вследствие отсутствия общепризнанного консенсуса по ряду вопросов и нуждается в дальнейшем совершенствовании.

Как было показано выше, ключевыми вопросами обеспечения международной безопасности в условиях цифровизации являются вопросы правового регулирования киберпространства, от чего в цифровую эпоху зависит безопасность как целых государств, так и отдельно взятого человека, разработка правил ведедения кибервойн, применения боевых роботов.