УДК 341.3:004.82
DOI: 10.36979/1694-500X-2024-24-3-55-61

ПРИМЕНЕНИЕ МЕЖДУНАРОДНОГО ГУМАНИТАРНОГО ПРАВА К ВООРУЖЕННЫМ КОНФЛИКТАМ В КИБЕРПРОСТРАНСТВЕ

Д.М. Байгазиева, Н.А. Ахматбеков

Аннотация. Рассматриваются и анализируются проблемы применения международного гуманитарного права к вооруженным конфликтам в киберпространстве. Раскрыто основное содержание термина «киберпространство». Рассмотрены содержание государственного суверенитета в киберпространстве и проблемы его реализации. Сформулированы предложения по направлениям адаптации и прогрессивного развития международного гуманитарного права применительно к выполнению гуманитарных задач в ходе вооруженных конфликтов в киберпространстве.

Ключевые слова: международное гуманитарное право; вооруженные конфликты; киберпространство; информационно-коммуникационные технологии; государственный суверенитет; границы; методы и средства ведения войны; правовая защита; адаптация международного гуманитарного права.

КИБЕРМЕЙКИНДИКТЕГИ КУРАЛДУУ КАГЫЛЫШУУЛАРГА ЭЛ АРАЛЫК ГУМАНИТАРДЫК УКУКТУ КОЛДОНУУ

Д.М. Байгазиева, Н.А. Ахматбеков

Аннотация. Макалада кибермейкиндиктеги куралдуу кагылышууларга эл аралык гуманитардык укукту колдонуу маселеси каралат жана талданат. «Кибермейкиндик» терминининн негизги мазмуну ачылды. Кибермейкиндикте мамлекеттик эгемендиктин мазмуну жана аны ишке ашыруу маселелери каралды. Кибермейкиндиктеги куралдуу кагылышуулар учурунда гуманитардык милдеттерди ишке ашырууга карата эл аралык гуманитардык укукту адаптациялоо жана прогрессивдүү өнүктүрүү багыттары боюнча сунуштар иштелип чыккан.

Түйүндүү сөздөр: эл аралык гуманитардык укук; куралдуу кагылышуулар; кибермейкиндик; маалыматтык-коммуникациялык технологиялар; мамлекеттик эгемендик; чек аралар; согуш жүргүзүү ыкмалары жана каражаттары; укуктук коргоо; эл аралык гуманитардык укукту адаптациялоо.

APPLICATION OF INTERNATIONAL HUMANITARIAN LAW TO ARMED CONFLICTS IN CYBERSPACE

D.M. Baigazieva, N.A. Akhmatbekov

Abstract. This article considers the issues of application of international humanitarian law to armed conflicts in cyberspace. The term "cyberspace" is interpreted as well as the concept of state sovereignty in cyberspace and challenges to its implementation. The proposals are made on the areas of adaptation and progressive development of international humanitarian law with regard to carrying out humanitarian tasks in armed conflicts in cyberspace.

Keywords: international humanitarian law; armed conflicts; cyberspace; information and communications technologies; state sovereignty; borders; methods and means of warfare; combatants; legal protection; adaptation of international humanitarian law.

В последние годы киберпространство стало новой сферой развития и конфликтов. Быстрый технологический прогресс и рост интернета привели к возникновению новых угроз для национальной безопасности, в том числе и кибератак. В связи с усилением разработки методов

и подходов к использованию информационно-коммуникационных технологий (ИКТ) для решения военно-политических задач многими государствами становится все более актуальным изучение вопросов применения международного гуманитарного права (МГП) к вооруженным конфликтам в киберпространстве. Согласно докладу Группы правительственных экспертов Организации Объединенных Наций по информатизации и телекоммуникации в контексте международной безопасности (2014–2015 гг.), «понимание, как нормы международного права применимы к использованию ИКТ государствами, играет важную роль для создания открытой, безопасной, устойчивой, доступной и мирной среды в области ИКТ» [1].

Как отмечает Д.М. Байгазиева, «…усиление информационной безопасности и повышение доверия при использовании ИКТ является одним из важных факторов на пути развития информационного общества. В целях совершенствования форм и методов обеспечения информационной безопасности Кыргызской Республики, оценки и прогнозирования угроз информационной безопасности, а также создания эффективной системы противодействия в информационной сфере, постановлением Правительства КР от 3 мая 2019 года № 209 была утверждена Концепция информационной безопасности Кыргызской Республики на 2019–2023 годы» [2, с. 54].

Как отмечают специалисты [3], применение принципов и норм МГП (право Гааги и право Женевы) к вооруженным конфликтам в киберпространстве сопряжено с определенными сложностями в трактовке этих принципов и норм. Данные сложности обусловлены, с одной стороны, новизной киберпространства как области применения МГП, а с другой – отсутствием универсальных международных договоров, регулирующих отношения в области использования ИКТ в качестве средства вооруженного насилия.

В настоящее время не существует однозначного определения для термина «киберпространство». Этот термин обычно используется для обозначения виртуального пространства, созданного компьютерными системами и сетями, где происходят цифровые взаимодействия. Киберпространство включает в себя интернет, компьютерные сети, программное обеспечение, данные и всевозможные цифровые технологии. Понятие киберпространства также связано с кибербезопасностью и киберугрозами.

Несмотря на отсутствие универсального определения, многие страны, организации и эксперты всё же используют термин «киберпространство» для обозначения области, где происходят кибератаки, кибершпионаж, киберпреступления и другие цифровые события. Вопросы, связанные с киберпространством, включают в себя вопросы кибербезопасности, норм и правил в цифровой среде, а также вопросы кибервойны и киберконфликтов.

Так, например, в международных договорах Шанхайской Организации сотрудничества и некоторых двусторонних договорах, использование термина «информационное пространство» обозначает сферу деятельности, связанную с обработкой, передачей и использованием информации, а также с ее влиянием на индивидуальное и общественное сознание, информационную инфраструктуру и сами данные [4]. В межправительственном Соглашении Содружества Независимых Государств данное понятие использовано в контексте инновационной деятельности [5, ст. 1]. В этом Соглашении информационное пространство определено как «совокупность информационных ресурсов, систем и технологий, а также информационно-коммуникационной инфраструктуры, обеспечивающих информационное взаимодействие между организациями и гражданами, а также удовлетворение их информационных потребностей».

В свете изложенного имеет смысл согласиться с точкой зрения российских и американских экспертов, специализирующихся в области исследования основной терминологии критической важности в сфере кибербезопасности. По их мнению, «киберпространство» представляет собой составную часть информационной среды, являющейся «электронной средой (включая фотоэлектронную и тому подобное), через которую информация создается, принимается, хранится, обрабатывается и уничтожается» [6].

В национальных законодательствах нередко используется термин «информационно-

коммуникационные технологии», чтобы описать процессы, методы и способы работы с информацией в электронном виде: ее поиск, сбор, хранение, обработку, предоставление и распространение. В англоязычной литературе этот термин понимается более широко и включает в себя все телекоммуникационные средства, компьютеры и, при необходимости, специализированное и общее программное обеспечение, память, системы аудио- и видеовизуализации, которые пользователи используют для хранения, передачи и обработки информации [7].

Одной из ключевых характеристик киберпространства является его глобальность, что позволяет людям и объектам взаимодействовать информационно независимо от нахождения в разных странах. Глобальность киберпространства достигается путем объединения национальных электронных сред в единую среду, где происходит сбор, передача, хранение и обработка информации с использованием единой системы цифровой адресации для всех субъектов и объектов киберпространства.

В современном мире развитие информационных технологий и цифровых коммуникаций привело к возникновению новой сферы противостояния между государствами – киберпространству.

Как отмечает Н. Мельцер в доктрине [8, с. 65], киберпространство является «пятой сферой или пятым доменом ведения военных действий» после суши, моря, воздушного и космического пространств. Данное утверждение не может быть оспорено по той причине, что, в силу уровня развития современных технологий, киберпространство в действительности является потенциальным театром военных действий. Высокая вероятность таких вооруженных конфликтов заставила государства задуматься об их правовом регулировании, и в 2013 году благодаря усилиям юристов и военных специалистов из стран военно-политического блока НАТО, при участии специалистов из Международного Комитета Красного Креста (МККК), было разработано «Таллиннское руководство по международному праву, применимому к кибервооружениям» [9].

Международное гуманитарное право, также известное как право вооруженных конфликтов, регулирует поведение сторон вооруженных конфликтов с целью снижения страданий, предотвращения нарушений прав человека и обеспечения защиты жизни и достоинства граждан. Оно признает необходимость пропорционального использования силы и запрещает неограниченное применение насилия во время военных действий.

Международное гуманитарное право представляет собой систему принципов и норм, установленных в международном праве, которые регулируют отношения между участниками международных конфликтов с целью решения гуманитарных задач, возникающих в связи с вооруженными столкновениями. В частности, МГП имеет применение при вооруженных конфликтах в киберпространстве и обладает несколькими важными аспектами, которые следует учитывать при его использовании:

- территория, на которой осуществляется вооруженное противоборство;
- методы и средства ведения вооруженного противоборства;
- международно-правовой статус участников вооруженного конфликта;
- правовая защита лиц и объектов в ходе вооруженного конфликта;
- ответственность за нарушение МГП.

Рассмотрим выделенные аспекты применения МГП к вооруженным конфликтам в киберпространстве.

Территория вооруженного конфликта ограничена государствами, которые вовлечены в данный конфликт. В киберпространстве возникает вооруженное противостояние, прежде всего, в глобальной электронной среде, позволяющее осуществлять «вооруженное воздействие» на любой объект, который имеет цифровой адрес в едином пространстве цифровых адресов (доменных имен). Важно отметить, что эти адреса не зависят от их соединения с информационной инфраструктурой, расположенной на территории национальных государств. Отсутствие привязки объектов информационной инфраструктуры к объектам общественной инфраструктуры создает значительные трудности для соблюдения

принципов международного гуманитарного права сторонами вооруженного конфликта, таких как различение между гражданскими и военными лицами, запрет нападения на непричастных к военным действиям, запрет причинения излишних страданий, пропорциональность, необходимость и гуманность.

Важным аспектом международного правового регулирования отношений в области вооруженного конфликта является **ограничение методов и средств ведения вооруженной борьбы,** т. е. ограничение видов оружия, иных технических средств поражения противника, а также методов применения оружия и иных технических средств в ходе военных действий.

Известно, что в обычном понимании термин «оружие» означает любое средство, предназначенное для нападения или защиты, а также их совокупность [10, с. 394]. Практически все специалисты согласны с тем, что с точки зрения права ИКТ не являются оружием или техническим средством в общем смысле.

В то же время многие специалисты считают, что злонамеренное использование ИКТ способно нанести серьезный вред, который иногда может быть сравним с применением традиционного оружия, а в некоторых случаях – даже с применением оружия массового уничтожения [11, с. 32]. С этой точки зрения подобное использование ИКТ является серьезной угрозой для международного мира и безопасности, соответственно, в соответствии со статьей 51 Устава ООН, государствами должно признаваться право на самооборону.

В настоящее время не существует норм МГП, ограничивающих использование ИКТ в процессе вооруженного конфликта, несмотря на то что их враждебное применение способно наносить повреждения, «имеющие чрезмерный характер», или оказывающее «неизбирательное воздействие».

Один из ключевых аспектов МГП заключается в **определении международно-правового статуса участников вооруженных конфликтов.** Эта область регулирует отношения, связанные с международно-правовым положением сторон конфликта, включая вооруженные силы и группы, которые применяют оружие и другие технические средства для осуществления насилия.

Применение норм МГП к участникам вооруженных конфликтов в киберпространстве имеет очевидное значение, поскольку использование открытого оружия для насилия становится невозможным. Более того, «виртуальный» характер (ИКТ) как средства для противостояния вооруженным конфликтам позволяет государствам привлекать к участию любых граждан с необходимой квалификацией и доступом к глобальной электронной среде и инфраструктуре.

Таким образом, международно-правовой статус участников вооруженных конфликтов в киберпространстве до сих пор остается неопределенным.

Следующий аспект применения МГП в киберпространстве связан с обеспечением правовой защиты людей и объектов во время вооруженных конфликтов. Это предполагает гарантированное предоставление определенного набора прав всем лицам, которые не участвуют активно в военных действиях и оказываются под контролем противника или на территории конфликта. К правам, предоставляемым в рамках такой защиты, относятся следующие:

- раненые, больные и люди, попавшие в бедственные ситуации, например, кораблекрушение;
- военнопленные;
- женщины;
- дети;
- журналисты;
- гражданское население.

Более общая правовая защита, предоставляемая МГП, также применима к гражданским объектам, включая критически важные инфраструктурные объекты и культурные ценности.

Однако соблюдение сторонами вооруженного конфликта, ведущих боевые действия в киберпространстве, данных прав и обеспечение защиты указанных объектов в значительной степени затруднено из-за трудности их идентификации в электронной среде. Это обусловлено отсутствием международно-правовых норм, регламентирующих классификацию объектов электронного пространства и других объектов информационной инфраструктуры

противостоящих государств, связанных с предоставлением гарантированных прав согласно МГП или обеспечением соответствующей правовой защиты.

Важным аспектом международного правового регулирования отношений в области вооруженных конфликтов в киберпространстве является ответственность за нарушение МГП. Согласно международным договорам, сторона, которая нарушает положения Женевских конвенций 1949 года или дополнительных протоколов к ним [12, ст. 91], должна компенсировать причиненные убытки, если на то есть основания. Государство несет политическую и материальную ответственность в форме реституции и компенсации [13, с. 315].

Для проведения расследования нарушений в международном гуманитарном праве в киберпространстве необходимо выполнить следующие действия:

- обнаружить признаки нарушения международного гуманитарного права;
- установить идентичность тех, кто использует информационно-коммуникационные технологии в киберпространстве и является противниками государств (государства), виновными в нарушении норм международного гуманитарного права;
- обнаружить, документировать и проанализировать цифровые следы участников вооруженного конфликта в киберпространстве, причастных к нарушению международного гуманитарного права, а также выявить информационно-коммуникационные технологии, использование которых является объективным правонарушением международного права;
- определить, принадлежат ли те, кто использует информационно-коммуникационные технологии в киберпространстве, к вооруженным силам государств, участвующих в вооруженном конфликте, или они являются неправительственными вооруженными силами, другими организованными вооруженными группами, участвующими в конфликте;
- классифицировать нарушения международного гуманитарного права и привлечь виновных к ответственности.

Указанные меры являются необходимыми для эффективного расследования и борьбы с нарушениями международного гуманитарного права в киберпространстве.

Определенный опыт осуществления соответствующих оперативно-следственных действий в национальных киберпространствах уже накоплен национальными правоприменительными и правоохранительными органами многих государств мира в рамках применения национального законодательства и региональных международно-правовых актов в области противодействия киберпреступлениям. В то же время, возможность использования этого опыта в деятельности Международной комиссии по установлению фактов представляется весьма ограниченной. Это обусловлено, в первую очередь, незаинтересованностью государств, участвующих в вооруженном конфликте, в проведении таких исследований, в возможности манипулирования информацией, содержащей «следы» активности в киберпространстве со стороны как государств-участников конфликта, так и других заинтересованных государств.

Международная гуманитарная правовая защита (МГП) может быть адаптирована и развита в контексте киберпространства через несколько направлений:

1) закрепление государственного суверенитета в национальном киберпространстве включает в себя установление норм и принципов управления адресным пространством как в глобальном киберпространстве, так и на национальном уровне;
2) определение процедур для разграничения границ национальных киберпространств и закрепление этих границ в соответствующих международных договорах;
3) определение объектов информационной инфраструктуры общества, включая критически важные объекты, и обеспечение им правовой защиты в рамках МГП;
4) создание и поддержание актуальных «карт» объектов национальной информационной

инфраструктуры, которые будут защищены в соответствии с принципами МГП;

5) уточнение условий использования и международно-правового статуса бойцов, осуществляющих враждебное использование информационно-коммуникационных технологий (ИКТ) вооруженными силами государств и другими вооруженными группами во время вооруженных конфликтов;
6) уточнение критериев для классификации враждебного использования ИКТ в отношении противника, граждан и объектов, которые находятся под защитой МГП;
7) усовершенствование процедур и условий расследования нарушений принципов МГП международной комиссией по установлению фактов;
8) определение необходимости создания международной системы фиксации событий, связанных с использованием ИКТ во время вооруженных конфликтов, чтобы обеспечить выполнение задач, возложенных на международную комиссию по установлению фактов;
9) разработка и расширение международных соглашений о кибербезопасности и кибернормах, которые устанавливают правила и принципы поведения в киберпространстве;
10) содействие международной сотрудничеству и обмену информацией между государствами, правительственными и неправительственными организациями, а также частным сектором для предотвращения и пресечения кибератак и нарушений МГП;
11) создание международного механизма для рассмотрения и обсуждения киберпреступлений, включая нарушения МГП, и принятия согласованных международных мер по их пресечению и наказанию;
12) обеспечение доступности международного правосудия и механизмов разрешения споров для жертв киберпреступлений и нарушений МГП;
13) повышение осведомленности и образования в области кибербезопасности и МГП, включая развитие программ и обучающих материалов для государств, организаций и населения;
14) ограничение использования кибероружия, включая запрет на разработку и применение кибероружия, которое может нанести значительный ущерб гражданскому населению и инфраструктуре во время вооруженных конфликтов;
15) содействие техническому развитию и инновациям в области кибербезопасности для защиты информационной инфраструктуры и предотвращения нарушений МГП.

Закрепление соответствующих правовых новаций по каждому из выделенных направлений в универсальных международных договорах будет способствовать выполнению задачи обеспечения применимости норм международного права к использованию ИКТ на основе принципа суверенного равенства. Это также способствует укреплению общего понимания и повышению стабильности и безопасности в мировом киберпространстве, формированию единообразной практики применения международного гуманитарного права к вооруженным конфликтам в киберпространстве, а также разработке методологии оценки законности использования информационно-коммуникационных технологий в качестве средств насилия в ходе военных действий в традиционных сферах применения вооруженных сил.

Поступила: 01.12.23; рецензирована: 15.12.23;
принята: 19.12.23.

Литература

1. Доклад группы правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникации в контексте международной безопасности. Представлен Генеральным Секретарем ООН 70-й сессии Генеральной Ассамблеи ООН 22 июля 2015 г. URL: https://base.garant.ru/401457662/ (дата обращения: 10.12.2023).
2. *Байгазиева Д.М.* Теоретико-правовые аспекты формирования информационного общества в Кыргызской Республике / Д.М. Байгазиева, А.З. Сариева // Вестник КРСУ. 2022. Т. 22. № 3.
3. Материалы Международной конференции экспертов по компьютерным сетевым атакам и применимости международного

гуманитарного права. 17–19 ноября 2004. Стокгольм, Швеция.
4. Соглашение между правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности. 16 июня 2009 года. Екатеринбург. URL: https://base.garant.ru/2571379/ (дата обращения: 11.12.2023); Соглашение между Правительством Российской Федерации и Правительством Республики Беларусь о сотрудничестве в области обеспечения международной информационной безопасности, 25 декабря 2013 года. Москва. URL: https://base.garant.ru/70593484/ (дата обращения: 11.12.2023); Соглашение между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности. 8 мая 2015 года. Москва. URL: https://base.garant.ru/71032852/ (дата обращения: 11.12.2023).
5. Соглашение о создании инфраструктуры инновационной деятельности государств-участников СНГ в форме распределенной информационной системы и портала СНГ «Информация для инновационной деятельности государств-участников СНГ». 19 мая 2011 года. Минск. URL: https://base.garant.ru/70164896/ (дата обращения: 11.12.2023).
6. Российско-американская двусторонняя конференция по кибербезопасности. Основы критической терминологии // Всемирная инициатива по кибербезопасности Института Востока и Запада / Институт информационной безопасности МГУ. 2013. URL: http://wiki.informationsecurity.club/lib/exe/fetch.php?media=-documents_all:russia-u_s_bilateral_on_terminology_rus.pdf (дата обращения: 11.12.2023).
7. *Роуз М.* Информационные и коммуникационные технологии (ИКТ) / М. Роуз. URL: https://www.techopedia.com/definition/24152/information-and-communications-technology-ict (дата обращения: 11.12.2023).
8. *Мельцер Н.* Международное гуманитарное право: всеобъемлющее введение / Н. Мельцер // Международный комитет Красного Креста. 2017.
9. Tallinn Manual on the International Law Applicable to Cyber Warfare. Schmitt, 2013. URL: https://d-russia.ru/wpcontent/uploads/2013/08/tallinnmanual.pdf (дата обращения: 10.12.2023).
10. *Ожегов С.И.* Словарь русского языка / С.И. Ожегов. М.: Русский язык, 1986.
11. *Hoizington M.* Cyberwarfare and the use of Force Giving Rise to the Right of self-Defense / M. Hoizington // 32 B.C. Int'l & Comp. L. Rev. 432. 2009. V. 32.
12. Дополнительный протокол № 1 к Женевским конвенциям 1949 года. 8 июня 1977 г. URL: https://constitution.garant.ru/act/right/megdunar/2540377/ (дата обращения: 09.12.2023).
13. *Соколова Н.А.* Международное гуманитарное право / Н.А. Соколова // Международное право. М.: Проспект, 2015.