



ICRC

НАПРАВЛЕНИЕ ДЕЯТЕЛЬНОСТИ 6

ПЕРВАЯ КОНСУЛЬТАЦИЯ С ГОСУДАРСТВАМИ ПО СОБЛЮДЕНИЮ МЕЖДУНАРОДНОГО ГУМАНИТАРНОГО ПРАВА ПРИ ИСПОЛЬЗОВАНИИ ИНФОРМАЦИОННО- КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ ВО ВРЕМЯ ВООРУЖЕННЫХ КОНФЛИКТОВ

СПРАВОЧНЫЙ ДОКУМЕНТ

ВВЕДЕНИЕ.....	2
I. ИСПОЛЬЗОВАНИЕ ИКТ ВО ВРЕМЯ ВООРУЖЕННЫХ КОНФЛИКТОВ И ПРИМЕНЕНИЕ МГП: МЕЖДУНАРОДНЫЕ ДИСКУССИИ И ФОРМИРОВАНИЕ ОБЩЕГО ПОНИМАНИЯ	2
II. ИСПОЛЬЗОВАНИЕ ИКТ В СОВРЕМЕННЫХ ВООРУЖЕННЫХ КОНФЛИКТАХ И ГУМАНИТАРНЫЕ ПОСЛЕДСТВИЯ	4
III. ИСПОЛЬЗОВАНИЕ ИКТ ВО ВРЕМЯ ВООРУЖЕННЫХ КОНФЛИКТОВ: ПРАВОВЫЕ И ГУМАНИТАРНЫЕ ВОПРОСЫ, ВОЗНИКАЮЩИЕ В РАМКАХ МГП	7
I. ЗАЩИТА ГРАЖДАНСКОГО НАСЕЛЕНИЯ И ДРУГИХ ПОКРОВИТЕЛЬСТВУЕМЫХ ЛИЦ И ОБЪЕКТОВ ОТ ОПАСНОСТЕЙ, ВОЗНИКАЮЩИХ В РЕЗУЛЬТАТЕ ДЕЯТЕЛЬНОСТИ В СФЕРЕ ИКТ ВО ВРЕМЯ ВООРУЖЕННОГО КОНФЛИКТА.....	7
II. ЗАЩИТА ГРАЖДАНСКОГО НАСЕЛЕНИЯ И ДРУГИХ ПОКРОВИТЕЛЬСТВУЕМЫХ ЛИЦ ОТ ИНФОРМАЦИИ, РАСПРОСТРАНЯЕМОЙ В НАРУШЕНИЕ МГП ВО ВРЕМЯ ВООРУЖЕННОГО КОНФЛИКТА 12	
III. РИСК ПРИЧИНЕНИЯ ВРЕДА В РЕЗУЛЬТАТЕ ИСПОЛЬЗОВАНИЯ ГРАЖДАНСКОЙ ИКТ- ИНФРАСТРУКТУРЫ В ВОЕННЫХ ЦЕЛЯХ И УЧАСТИЯ ГРАЖДАНСКИХ ЛИЦ В ДЕЯТЕЛЬНОСТИ В СФЕРЕ ИКТ ВО ВРЕМЯ ВООРУЖЕННОГО КОНФЛИКТА	14

ВВЕДЕНИЕ

Всё более широкое использование информационно-коммуникационных технологий (ИКТ) во время вооруженных конфликтов поднимает серьезные гуманитарные и правовые вопросы. Несмотря на то что, по общему мнению, международное гуманитарное право (МГП) налагает ограничения на использование ИКТ в вооруженных конфликтах, особенности среды ИКТ порождают сложности в связи с имплементацией МГП. Государства признали необходимость дальнейшего обсуждения всех этих вопросов. Направление деятельности, посвященное ИКТ, реализуется в рамках непрерывных усилий по выработке общего понимания проблемы.

В продолжение этих дискуссий 15 мая 2025 г. в Женеве в очном и онлайн-формате состоится первая консультация с государствами по данному направлению. Эта встреча положит начало серии консультаций, которые пройдут в 2025 и 2026 гг. и будут способствовать обмену мнениями между государствами и получению информации от соответствующих заинтересованных сторон.

Первая консультация будет посвящена выявлению правовых и гуманитарных вопросов и проблем, возникающих в связи с уникальными особенностями деятельности в сфере ИКТ во время вооруженного конфликта, и изучению путей их решения в целях обеспечения защиты, которую МГП предоставляет гражданскому населению и гражданским объектам в условиях вооруженного конфликта, а также лицам и объектам, пользующимся особой защитой.

I. ИСПОЛЬЗОВАНИЕ ИКТ ВО ВРЕМЯ ВООРУЖЕННЫХ КОНФЛИКТОВ И ПРИМЕНЕНИЕ МГП: МЕЖДУНАРОДНЫЕ ДИСКУССИИ И ФОРМИРОВАНИЕ ОБЩЕГО ПОНИМАНИЯ

Применение международного права, в том числе МГП, к деятельности в сфере ИКТ является предметом многосторонних дискуссий на протяжении почти двух десятилетий. В 2021 г. Группа правительственных экспертов (ГПЭ) по поощрению ответственного поведения государств в киберпространстве в контексте международной безопасности в принятом консенсусом докладе отметила следующее: «...нормы международного гуманитарного права применимы только в ситуациях вооруженных конфликтов. Она напоминает об установленных международно-правовых принципах, включая, где это применимо, принципы гуманности, необходимости, соразмерности и избирательности, которые были отмечены в докладе 2015 года. Группа признаёт необходимость дальнейшего изучения вопроса о том, как и когда эти принципы применяются к использованию ИКТ государствами, и подчеркивает, что напоминание об этих принципах ни в коем случае не узаконивает и не поощряет конфликты»¹. Рабочая группа открытого

¹ Доклад Группы правительственных экспертов по поощрению ответственного поведения государств в киберпространстве в контексте международной безопасности, A/76/135, 2021 г., п. 71(f). См. также

состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021 — 2025 гг. подтвердила этот вывод в своих докладах о проделанной работе².

На сегодняшний день, насколько нам известно, свои национальные позиции относительно применения норм международного права к кибероперациям опубликовали 33 государства³. Кроме того, свои общие позиции по вопросу применения международного права к использованию ИКТ опубликовали две региональные организации — Африканский союз и Европейский союз, — что ознаменовало собой прогресс в достижении консенсуса на уровне данных регионов и увеличило число государств, выразивших мнение по этому вопросу, до более чем 100. В рамках выработки государствами общего понимания по данной проблематике было подтверждено применение принципов и норм МГП, включая принципы гуманности, необходимости, соразмерности и избирательности (проведения различия), к использованию ИКТ во время вооруженных конфликтов. Всё большее число государств также выражают мнение по поводу защиты от злонамеренных действий в сфере ИКТ, которую МГП предоставляет, в частности, гражданскому населению, гражданской инфраструктуре, данным гражданского назначения, медицинскому персоналу и медицинским учреждениям, а также сотрудникам гуманитарных организаций.

На основе достигнутых результатов в октябре 2024 г. 34-я Международная конференция Красного Креста и Красного Полумесяца, участие в которой приняли все государства и все составные части Международного движения Красного Креста и Красного Полумесяца, утвердила резолюцию «Защита гражданского населения и других покровительствуемых лиц и объектов от потенциальных гуманитарных последствий деятельности в сфере ИКТ во время вооруженного конфликта» (далее — «Резолюция по ИКТ»). В резолюции содержится настоятельный призыв к государствам и сторонам в вооруженном конфликте обеспечивать защиту гражданского населения и других покровительствуемых лиц и объектов, в том числе от рисков, обусловленных злонамеренной деятельностью в сфере ИКТ. Кроме того, резолюция призывает государства и стороны в вооруженном конфликте обеспечивать в соответствии с их международными правовыми обязательствами защиту гражданского населения, объектов гражданской критической инфраструктуры (включая объекты цифровой критической инфраструктуры, такой как подводные кабели и орбитальные коммуникационные сети), медицинского и гуманитарного персонала, а также объектов культуры, в том числе от рисков, обусловленных злонамеренной деятельностью в сфере ИКТ. В резолюции подтверждается запрещение поощрений или подстрекательства к нарушениям МГП, а также рассматриваются вопросы, касающиеся гражданских лиц, осуществляющих деятельность в сфере ИКТ, и частных технологических компаний, предоставляющих услуги ИКТ в условиях вооруженного конфликта.

резолюцию 76/19 Генеральной Ассамблеи Организации Объединенных Наций от 2021 года (пп. 2 и 3), принятую консенсусом, в которой приветствуется консенсусный заключительный доклад ППЭ и содержится призыв к государствам-членам при использовании ИКТ руководствоваться этим докладом.

² См. первый ежегодный доклад о проделанной работе, A/77/275, 2022 г. (п. 15(b)(ii)); второй ежегодный доклад о проделанной работе, A/78/265, 2023 г. (п. 29(b)(ii)); третий ежегодный доклад о проделанной работе, A/79/214, 2024 г. (п. 36(b)(ii)) Рабочей группы открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ.

³ Со всеми национальными позициями отдельных государств и общими позициями, выработанными отдельными регионами, можно ознакомиться на интерактивном портале Cyber Law Toolkit, в разделе «Common and National Positions» по адресу: https://cyberlaw.ccdcoe.org/wiki/List_of_articles#Common_and_national_positions.

Несмотря на отмеченный выше прогресс, было признано, что особенности ИКТ-среды порождают вопросы касательно того, каким образом принципы и нормы МГП применяются к деятельности в сфере ИКТ, и что необходимы дальнейшие дискуссии⁴.

В рамках данного направления деятельности планируется удовлетворить возникшую потребность и предложить специальную площадку для подробного и содержательного обмена мнениями. В свете гуманитарных последствий использования ИКТ в вооруженных конфликтах данное направление деятельности будет способствовать выработке общего понимания того, каким образом МГП ограничивает деятельность в сфере ИКТ во время вооруженных конфликтов, чтобы защитить гражданское население от причинения ему вреда.

II. ИСПОЛЬЗОВАНИЕ ИКТ В СОВРЕМЕННЫХ ВООРУЖЕННЫХ КОНФЛИКТАХ И ГУМАНИТАРНЫЕ ПОСЛЕДСТВИЯ

Стремительная цифровизация общества принесла значительные преимущества, расширив социальные, экономические и коммуникационные возможности. В затронутых конфликтами районах надежные ИКТ имеют решающее значение для обеспечения доступа гражданского населения к основным товарам и услугам, для предоставления услуг государствами, а также для поддержки медицинской и гуманитарной деятельности, в том числе деятельности Международного движения Красного Креста и Красного Полумесяца.

Однако эти преимущества несут в себе и риски, в том числе риски, возникающие в результате более активного использования ИКТ государствами и негосударственными субъектами в вооруженных конфликтах. Некоторые государства работают над расширением потенциала использования ИКТ в военных целях, всё активнее внедряя и применяя ИКТ в качестве средств и методов ведения войны. Хотя наращивание и использование военного потенциала ИКТ может способствовать достижению враждующими сторонами своих целей, не причиняя при этом прямого вреда гражданскому населению и не нанося физического ущерба объектам гражданской инфраструктуры, угроза, которую такая деятельность представляет для гражданского населения и инфраструктуры, по-прежнему вызывает беспокойство. При использовании потенциала ИКТ в военных целях процессы, управляемые компьютерными системами, могут быть запущены, изменены или так или иначе применены такими способами, которые могут причинить значительный вред гражданскому населению.

Использование ИКТ с целью поражения объектов критически важной гражданской инфраструктуры, такой как ядерные объекты, электросети, системы водоснабжения и телекоммуникационные сети, может иметь «потенциально катастрофические

⁴ Доклад Группы правительственных экспертов по поощрению ответственного поведения государств в киберпространстве в контексте международной безопасности, A/76/135, 2021 г., п. 71(f); 34-я Международная конференция Красного Креста и Красного Полумесяца (Женева, 2024 г.). Резолюция 2 «Защита гражданского населения и других покровительствуемых лиц и объектов от потенциальных гуманитарных последствий деятельности в сфере ИКТ во время вооруженного конфликта», 19-й пункт преамбулы.

гуманитарные последствия»⁵. Деятельность в сфере ИКТ может также приводить к сбоям в работе сервисов электронного правительства и субъектов частного сектора, что может иметь социальные и экономические последствия. Эти риски усугубляются характерной для киберпространства взаимосвязанностью его составных элементов. Деятельность в сфере ИКТ, затрагивающая одну систему, может порождать последствия и для различных других систем, независимо от их местонахождения.

Сектор здравоохранения, а также гуманитарные организации особенно уязвимы к деятельности в сфере ИКТ во время вооруженных конфликтов, которая может привести к сбоям в обеспечении жизненно важной деятельности медицинских учреждений, помешать работе беспристрастных гуманитарных организаций и их сотрудников, а также поставить под угрозу оказание необходимой помощи нуждающимся. Так, например, кибероперациям злоумышленников подвергаются и Международный комитет Красного Креста (МККК) и другие составные части Международного движения Красного Креста и Красного Полумесяца⁶.

Кроме того, участились случаи вовлечения гражданских лиц в военную деятельность с использованием ИКТ во время вооруженных конфликтов. Государства терпимо относятся к участию гражданских хакеров в деятельности в сфере ИКТ, затрагивающей или направленной против гражданских лиц и гражданских объектов, связанных с противником, содействуют такому участию или поощряют его. Кроме того, гражданское население призывают сообщать о передвижении вражеских войск, в том числе с помощью приложений для смартфонов. Частные компании всё чаще предоставляют сторонам в вооруженном конфликте услуги в области обеспечения кибербезопасности, а также доступ к другим цифровым сервисам. Чем ближе гражданские лица оказываются к боевым действиям, тем больше они подвергаются опасности. Кроме того, зачастую они не осознают риски, которым подвергаются, и правовые последствия своих действий, а также не знакомы с нормами МГП, которые должны соблюдать.

Еще одним аспектом является использование ИКТ для распространения вредной информации во время вооруженного конфликта. Хотя информационные операции уже давно представляют собой часть военных действий и не являются противозаконными как таковые, использование ИКТ — особенно в социальных сетях или в сочетании с искусственным интеллектом и другими новыми технологиями — увеличивает скорость и масштабы распространения вредной информации, включая, например, подстрекательство к насилию, выставление задержанных лиц на обозрение любопытствующей толпы или подрыв доверия к гуманитарным организациям.

⁵ Рабочая группа открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. Заключительный доклад о проделанной работе, A/AC.290/2021/CRP.2, 2021 г., п. 18.

⁶ Произошедшая в 2022 г. утечка данных и неоднократные хакерские распределенные атаки типа «отказ в обслуживании» на веб-сайт МККК подчеркивают необходимость надежной защиты данных для недопущения разглашения конфиденциальной информации, обеспечения непрерывности работы МККК и поддержания гуманитарного диалога со сторонами в конфликте на условиях конфиденциальности. См.: МККК. Кибератака на МККК: что нам известно, <https://www.icrc.org/ru/document/kiberataka-na-mkkk-chto-nam-izvestno>.

Государства признают эти изменения и сопутствующие им угрозы. Рабочая группа открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности отметила, что государства занимаются развитием потенциала использования ИКТ в военных целях и что их использование в будущих конфликтах становится всё более вероятным и способным иметь потенциально катастрофические гуманитарные последствия⁷. Участники 34-й Международной конференции Красного Креста и Красного Полумесяца отметили вред, который может быть причинен использованием ИКТ сторонами в вооруженных конфликтах гражданскому населению, в частности там, где использование ИКТ направлено против объектов критически важной гражданской инфраструктуры и жизненно важных услуг или случайным образом нарушает их работу, а также потенциальный ущерб для деятельности беспристрастных гуманитарных организаций, затрудняющий их доступ к пострадавшему населению⁸.

ВОПРОСЫ ДЛЯ ПОДГОТОВКИ ДАЛЬНЕЙШЕЙ ДИСКУССИИ

- Какая деятельность в сфере ИКТ во время вооруженного конфликта создает угрозу или риск причинения прямого или косвенного вреда гражданскому населению и гражданским объектам?
- Каким образом информация, распространяемая с использованием ИКТ во время вооруженного конфликта (в частности, в социальных сетях), может нанести физический, длительный психологический, экономический и общественный вред или способствовать его нанесению?
- С практической точки зрения: признаёт ли ваше государство какие-либо значимые различия в том, как деятельность в сфере ИКТ проявляется или создает риски для гражданских лиц в международных и немеждународных вооруженных конфликтах? Выявило ли ваше государство какие-либо особые проблемы или возникающие тенденции в вооруженных конфликтах этих типов?
- Какие меры были приняты вашим государством для оценки и смягчения гуманитарных последствий деятельности в сфере ИКТ во время вооруженного конфликта? Могли бы вы поделиться своим опытом, который может быть полезен другим делегациям?

⁷ Рабочая группа открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. Заключительный доклад о проделанной работе, A/AC.290/2021/CRP.2, 2021 г., пп. 16 и 18.

⁸ Резолюция по ИКТ, 7-й и 14-й пункты преамбулы.

III. ИСПОЛЬЗОВАНИЕ ИКТ ВО ВРЕМЯ ВООРУЖЕННЫХ КОНФЛИКТОВ: ПРАВОВЫЕ И ГУМАНИТАРНЫЕ ВОПРОСЫ, ВОЗНИКАЮЩИЕ В РАМКАХ МГП

Существующие договоры в области МГП и нормы обычного права предоставляют гражданскому населению и гражданским объектам защиту от опасностей, возникающих в результате деятельности в сфере ИКТ во время вооруженного конфликта. Как подтверждается в Резолюции по ИКТ, «в ситуациях вооруженного конфликта, нормы и принципы МГП — включая принцип проведения различия, запрещение неизбирательных и несоразмерных нападений, обязательство обеспечивать защиту гражданского населения, гражданских лиц и объектов от причинения вреда при проведении военных операций и принимать все возможные меры предосторожности, чтобы при любых обстоятельствах избежать или свести к минимуму причинение непреднамеренного вреда таким лицам и объектам, запрещение поощрения или подстрекательства к нарушениям МГП и запрещение актов насилия или угрозы насилием, первоочередной целью которых является терроризирование гражданского населения, — служат цели защиты гражданского населения и других покровительствуемых лиц и объектов, в том числе от рисков, возникающих в результате деятельности в сфере ИКТ»⁹.

Исходя из вышесказанного, ниже предлагаются для дальнейшего обсуждения ключевые правовые вопросы, связанные с наиболее актуальными гуманитарными проблемами.

I. ЗАЩИТА ГРАЖДАНСКОГО НАСЕЛЕНИЯ И ДРУГИХ ПОКРОВИТЕЛЬСТВУЕМЫХ ЛИЦ И ОБЪЕКТОВ ОТ ОПАСНОСТЕЙ, ВОЗНИКАЮЩИХ В РЕЗУЛЬТАТЕ ДЕЯТЕЛЬНОСТИ В СФЕРЕ ИКТ ВО ВРЕМЯ ВООРУЖЕННОГО КОНФЛИКТА

Защита гражданского населения от последствий деятельности в сфере ИКТ во время вооруженного конфликта и понятие нападения в МГП

Деятельность в сфере ИКТ может привести к выходу из строя промышленных объектов, сетей связи и других элементов критически важной инфраструктуры государства или к нанесению им физического ущерба. Такие действия также могут прямо или косвенно причинить вред жизни или здоровью гражданского населения, в том числе в результате нарушения функционирования критически важных систем. Эти риски усугубляются характерной для цифрового пространства взаимосвязанностью его составных элементов. Хотя деятельности в сфере ИКТ, приводящей к нанесению физического ущерба, уделяется особое внимание, недавние случаи использования ИКТ, в том числе в вооруженных конфликтах, показали, что даже в отсутствие физического ущерба действия с использованием ИКТ могут серьезно нарушить функционирование гражданской инфраструктуры и прервать предоставление жизненно необходимых услуг. На самом деле, это один из самых серьезных рисков, связанных с ИКТ, для гражданского населения во время вооруженных конфликтов.

⁹ Резолюция по ИКТ, п. 4.

Цель норм МГП, регулирующих ведение военных действий, заключается в обеспечении уважения и защиты гражданского населения и гражданских объектов¹⁰. Большинство норм, вытекающих из принципов и правил, регулирующих ведение военных действий (в частности, принципов проведения различия, соразмерности и принятия мер предосторожности), которые предоставляют общую защиту гражданским лицам и гражданским объектам, применяются только к операциям или действиям, которые квалифицируются как «нападения» (то есть к операциям или действиям, под которыми согласно МГП понимаются «акты насилия в отношении противника, независимо от того, совершаются ли они при наступлении или при обороне»¹¹). Поэтому вопрос о трактовке понятия «нападение» применительно к использованию ИКТ в ходе вооруженного конфликта, в частности к деятельности в сфере ИКТ, приводящей к выходу из строя гражданских объектов без причинения физического ущерба, является крайне важным. Важность этого вопроса обусловлена тем, что от ответа на него зависит, применяются ли соответствующие нормы МГП и, следовательно, защищены ли гражданское население и другие покровительствуемые лица и объекты от опасностей, возникающих в результате таких операций.

Хорошо известно, что понятие насилия в определении термина «нападение» в МГП может относиться как к используемым средствам, так и к последствиям их использования. Действие, приводящее к последствиям насильственного характера, квалифицируется как нападение, даже если используемые средства сами по себе не являются насильственными¹².

Кроме того, широко признается, что кибероперации, которые, как ожидается, приведут к гибели, ранениям или физическому ущербу, согласно МГП представляют собой нападения¹³. Сюда относятся и кибероперации, которые причиняют вред своими прогнозируемыми прямыми и «непрямыми» (косвенными) последствиями: например, когда пациенты, находящиеся в реанимационном отделении больницы, умирают, потому что больница осталась без электричества в результате кибератаки на электроэнергетическую систему¹⁴.

Кроме того, государствам следует продолжить обсуждение вопроса о том, какие нормы МГП ограничивают кибероперации, влияющие на функциональность систем ИКТ, не обязательно при этом приводя к гибели, ранениям или физическому ущербу, включая вопрос о том, признаются ли такие операции «нападением» согласно МГП.

В условиях современных войн признание киберопераций, приводящих к выходу тех или иных объектов из строя без причинения физического ущерба, нападением

¹⁰ Дополнительный протокол I от 8 июня 1977 года, ст. 48 и заголовки части IV и ее раздела I.

¹¹ Дополнительный протокол I, ст. 49(1). Существует несколько норм МГП, которые применяются ко всем военным операциям, включая те, которые проводятся с помощью ИКТ. См. например: Дополнительный протокол I, ст. 48, ст. 51(1) и ст. 57(1).

¹² Y. Sandoz, C. Swinarski and B. Zimmermann (eds), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*, ICRC, Geneva/Martinus Nijhoff, Leiden, 1987 (далее — ICRC, Commentary on the Additional Protocols). В п. 1881, посвященном ст. 49(1) Дополнительного протокола I, отмечается, что «нападение имеет место всякий раз, когда люди подвергаются непосредственной опасности в результате установки мины». Такое толкование согласуется с подходом, оценивающим последствия. Другим общепризнанным примером является применение химического или биологически активного вещества, которое может представлять собой нападение ввиду вызываемых им последствий насильственного характера, даже если средства доставки таких веществ сами по себе не сопряжены с насилием.

¹³ МККК. Международное гуманитарное право и вызовы современных вооруженных конфликтов, 2015, с. 72—75.

¹⁴ Международное гуманитарное право и кибероперации во время вооруженных конфликтов. Изложение позиции МККК, 2019 г., с. 10. С обзором позиций государств по данному вопросу можно ознакомиться на интерактивном портале Cyber Law Toolkit в разделе «Attack (International Humanitarian Law)» по адресу: [https://cyberlaw.ccdcoe.org/wiki/Attack_\(international_humanitarian_law\)](https://cyberlaw.ccdcoe.org/wiki/Attack_(international_humanitarian_law)).

согласно МГП имеет решающее значение для защиты гражданских лиц и гражданских объектов от последствий деятельности в сфере ИКТ во время вооруженного конфликта. Узкое толкование понятия нападения, исключающее определенные виды деятельности в сфере ИКТ из сферы защиты, предоставляемой основными нормами МГП, которые касаются ведения боевых действий, с трудом согласуется с объектом и целью МГП, а также с необходимостью обеспечить сохранение эффективности предоставляемой защиты в свете эволюции средств и методов ведения войны. Поэтому для обеспечения защиты гражданского населения и гражданских объектов от последствий вредоносного использования ИКТ во время вооруженных конфликтов крайне важно, чтобы государства согласовали общую позицию относительно понятия «нападение».

Данные гражданского назначения и понятие «гражданские объекты» в МГП

Данные гражданского назначения, такие как медицинские и биометрические данные, данные органов социального обеспечения, налоговая документация, банковские счета, данные, собираемые гуманитарными организациями, клиентские базы компаний или списки избирателей и результаты выборов, — важный элемент общественной жизни в эпоху цифровых технологий. Такие данные имеют ключевое значение для функционирования большинства сфер жизни гражданина как на индивидуальном уровне, так и на уровне всего общества. Защита этих данных становится предметом всё большей озабоченности. Удаление или искажение данных гражданского назначения может быстро привести к полной остановке работы государственных служб и частных предприятий. Подобные действия могут причинить гражданскому населению больше вреда, чем уничтожение физических объектов. Кроме того, кража или утечка данных гражданского назначения может подвергнуть отдельных людей и целые сообщества серьезному риску в плане причинения им вреда.

Что касается данных, относящихся к определенным категориям лиц и объектов, пользующихся в соответствии с МГП особой защитой, то связанные с их защиты нормы носят всеобъемлющий характер. Например, обязательство уважать и обеспечивать защиту медицинского персонала, медицинских учреждений и транспортных средств, гуманитарного персонала и гуманитарных объектов, а также объектов, необходимых для выживания гражданского населения, распространяется и на их данные¹⁵. Однако, помимо этого, необходимо углубить понимание того, в какой степени данные гражданского назначения защищены существующими нормами МГП¹⁶; в частности, являются ли такие данные с точки зрения МГП гражданскими объектами, кибероперации в отношении которых (например, их повреждение или удаление) будут, в частности, регулироваться принципами проведения различия, соразмерности и принятия мер предосторожности.

По этому вопросу некоторые государства придерживаются мнения о том, что защита гражданских объектов распространяется на все виды данных гражданского назначения; ряд государств проводит различие между «содержательными данными» (то есть фактическими данными) и другими данными (например,

¹⁵ См. следующий раздел настоящего документа («Лица и объекты, пользующиеся особой защитой в соответствии с МГП»).

¹⁶ К ним относятся принципы и нормы МГП, регулирующие ведение боевых действий. К числу других норм, касающихся данного аспекта, можно отнести, например, нормы, обеспечивающие защиту культурных объектов, защиту гражданских объектов на оккупированной территории и запрет на мародерство.

метаданными); другие же считают, что цифровые данные в целом не могут считаться гражданскими объектами в соответствии с МГП¹⁷.

Для выработки общего понимания этого важного вопроса государствам необходимо продолжить его обсуждение. С гуманитарной точки зрения утверждение о том, что в нашем мире, зависимом от данных, та или иная операция, имеющая своей целью удаление или искажение данных гражданского назначения или способная привести к подобным последствиям, не запрещается МГП, с трудом согласуется с объектом и целью МГП. Вполне логично, что замещение бумажных документов цифровыми не должно привести к снижению уровня защиты, предоставляемой МГП соответствующим данным.

Лица и объекты, пользующиеся особой защитой в соответствии с МГП

Некоторые нормы МГП предоставляют определенным категориям лиц и объектов особую защиту, выходящую за рамки простого запрета на нападения, в том числе в части деятельности в сфере ИКТ.

Например, воюющие стороны должны при любых обстоятельствах уважать и обеспечивать защиту медицинского персонала и медицинских учреждений¹⁸, что включает требование не вмешиваться необоснованно в работу медицинских служб и принимать возможные меры для их защиты от вредоносных действий и вмешательства со стороны частных лиц, не относящихся к сторонам в вооруженном конфликте¹⁹. Гуманитарный персонал и объекты, используемые в рамках гуманитарной деятельности, также должны пользоваться уважением и защитой²⁰, а стороны в вооруженном конфликте должны разрешать беспристрастную гуманитарную деятельность и содействовать ей во время вооруженного конфликта, сохраняя за собой право на контроль²¹. Как в случае медицинских служб, так и в случае сотрудников гуманитарных организаций и гуманитарных объектов предоставляемая им особая защита распространяется на средства связи и данные²².

Для усиления защиты медицинских служб и гуманитарной деятельности от рисков, связанных с ИКТ, в ходе дальнейшей дискуссии можно сосредоточиться на практических шагах по применению таких гарантий. Одним из направлений является возглавляемая МККК работа по созданию «цифровой эмблемы», то есть средства идентификации цифровой инфраструктуры и данных, принадлежащих организациям и учреждениям, которые имеют право на использование отличительных эмблем, признанных в соответствии с нормами МГП²³. Резолюция

¹⁷ С обзором позиций государств по данному вопросу можно ознакомиться на интерактивном портале Cyber Law Toolkit в разделе «Data as a military objective» по адресу: https://cyberlaw.ccdcoe.org/wiki/Military_objectives#Qualification_of_data_as_a_military_objective_under_IHL.

¹⁸ См., например: Женевская конвенция I от 12 августа 1949 года, ст. 19; Женевская конвенция II от 12 августа 1949 года, ст. 12; Женевская конвенция IV от 12 августа 1949 года, ст. 18; Дополнительный протокол I, ст. 12; Дополнительный протокол II от 8 июня 1977 года, ст. 11; МККК. Исследование «Обычное международное гуманитарное право»: <https://ihl-databases.icrc.org/ru/customary-ihl/rules>, нормы 25, 28 и 29.

¹⁹ ICRC, Commentary on the Additional Protocols, para. 517 (ст. 12 Дополнительного протокола I); МККК. Комментарий к Женевской конвенции I: Конвенция об улучшении участи раненых и больных в действующих армиях. МККК, 2021 (далее — Комментарий МККК к Женевской конвенции I»), ст. 19, п. 1799.

²⁰ Дополнительный протокол I, ст. 70(4) и ст. 71(2); МККК. Исследование «Обычное международное гуманитарное право», нормы 31 и 32.

²¹ См.: Женевская конвенция IV, ст. 23; Дополнительный протокол I, ст. 70(2); Дополнительный протокол II, ст. 18(2); МККК. Исследование «Обычное международное гуманитарное право», норма 55.

²² Комментарий МККК к Женевской конвенции I, ст. 19, п. 1804.

²³ Проект «Цифровая эмблема» представляет собой отдельный проект, реализуемый МККК в сотрудничестве с государствами и составными частями Международного движения Красного Креста и

по ИКТ, принимая во внимание текущую работу МККК в сотрудничестве с государствами и составными частями Международного движения Красного Креста и Красного Полумесяца, призывает к дальнейшей работе и консультациям, включая изучение возможных правовых и дипломатических путей для потенциального использования цифровой эмблемы²⁴.

Кроме того, деятельность в сфере ИКТ, в результате которой уничтожаются, вывозятся или приводятся в негодность объекты, необходимые для выживания гражданского населения (такие как сооружения для снабжения питьевой воды и ирригационные сооружения), подпадает под действие норм об особой защите, предоставляемой таким объектам в соответствии с МГП, независимо от того, признается ли подобная деятельность нападением²⁵. Особая защита распространяется и на ИКТ-инфраструктуру, которая сама по себе является «неотъемлемой» для функционирования подобных объектов. Для определения мер по реализации этих гарантий защиты на практике необходимо продолжение дискуссии.

Наконец, нормы МГП предоставляют особую защиту определенным категориям лиц, включая детей, женщин и инвалидов, но не ограничиваясь ими²⁶. Для определения, в частности, практических мер по обеспечению соблюдения норм, требующих особой защиты женщин и детей от сексуального насилия²⁷, в том числе совершаемого с помощью ИКТ, необходимы дальнейшие обсуждения.

Красного Полумесяца. В рамках данного направления деятельности обсуждение этого проекта не предполагается.

²⁴ Резолюция по ИКТ, 15-й пункт преамбулы и п. 12 резолютивной части.

²⁵ Примерами таких объектов являются, в частности, «запасы продуктов питания, производящие продовольствие сельскохозяйственные районы, посевы, скот, сооружения для снабжения питьевой водой и запасы последней, а также ирригационные сооружения». Дополнительный протокол I, ст. 54(2); Дополнительный протокол II, ст. 14; МККК Исследование «Обычное международное гуманитарное право», норма 54. См. также: ICRC, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, 2024, pp. 46—47.

²⁶ МККК Исследование «Обычное международное гуманитарное право», нормы 134, 135 и 138.

²⁷ Женевская конвенция IV, ст. 27(2); Дополнительный протокол I, ст. 76(1) и ст. 77(1).

ВОПРОСЫ ДЛЯ ПОДГОТОВКИ ДАЛЬНЕЙШЕЙ ДИСКУССИИ

- Какие с точки зрения вашего государства ограничения налагают нормы и принципы МГП на деятельность в сфере ИКТ во время вооруженных конфликтов, направленную на защиту гражданского населения от угрозы причинения вреда? В частности, какие ограничения нормы и принципы МГП налагают на деятельность в сфере ИКТ, прямо или косвенно приводящую к выводу из строя гражданских объектов без причинения им физического ущерба?
- Каким образом ваше государство применяет предоставляемые нормами МГП гарантии защиты в отношении медицинских служб, беспристрастных гуманитарных организаций и объектов, необходимых для выживания гражданского населения, от последствий деятельности в сфере ИКТ во время вооруженного конфликта?
- Рассматривало ли ваше государство вопрос о том, защищены ли согласно МГП данные гражданского назначения в целом или их определенные категории от искажения, повреждения или удаления? Какую защиту предоставляют нормы МГП от несанкционированного копирования данных гражданского назначения или данных публичного характера, несанкционированного получения над ними контроля и их возможной публикации?

II. ЗАЩИТА ГРАЖДАНСКОГО НАСЕЛЕНИЯ И ДРУГИХ ПОКРОВИТЕЛЬСТВУЕМЫХ ЛИЦ ОТ ИНФОРМАЦИИ, РАСПРОСТРАНЯЕМОЙ В НАРУШЕНИЕ МГП ВО ВРЕМЯ ВООРУЖЕННОГО КОНФЛИКТА

Государства и негосударственные вооруженные группы распространяют цифровую информацию в самых разных целях, в том числе при проведении информационных или психологических операций. Некоторые операции направлены на снижение риска причинения вреда людям во время вооруженных конфликтов, например путем эффективного заблаговременного предупреждения гражданского населения о нападении или оказания помощи в эвакуации. Другие же направлены на то, чтобы вызвать замешательство или нанести вред, обмануть противника или содействовать достижению одной из сторон в конфликте ее военных или политических целей. В современных вооруженных конфликтах ИКТ используются для распространения информации в нарушение МГП. Информация, распространяемая с помощью ИКТ, может приводить к насилию или поощрять его, причинять длительный психологический вред, создавать непреодолимые препятствия для доступа к жизненно важным услугам и нарушать работу гуманитарных организаций, что может подорвать доверие к ним.

МГП содержит несколько конкретных норм, налагающих ограничения на распространение информации, в том числе с помощью цифровых средств. В частности:

- гражданские и военные должностные лица стороны в вооруженном конфликте не должны поощрять нарушения МГП, в том числе с помощью цифровых платформ²⁸. Резолюция по ИКТ также подтверждает запрещение

²⁸ Женевская конвенция IV, общая статья 1; МККК. Исследование «Обычное международное гуманитарное право», норма 139.

поощрений или подстрекательства к нарушениям МГП с помощью цифровых средств²⁹;

- военнопленные и другие лица, пользующиеся защитой МГП, должны быть защищены от любопытства толпы³⁰. Публичное распространение властями данных, изображений и видеозаписей военнопленных и других лиц, лишенных свободы (за некоторыми исключениями) будет являться нарушением этой нормы; государства должны обеспечивать защиту от распространения такой информации также и со стороны частных субъектов³¹;
- угрозы насилием, имеющие основной целью терроризировать гражданское население, запрещены МГП³²;
- ложная информация, распространяемая сторонами в вооруженном конфликте с целью воспрепятствовать медицинской или гуманитарной работе, несовместима с обязательствами уважать сотрудников медицинских и гуманитарных организаций и их деятельность и обеспечивать им защиту³³;
- пропаганда, направленная на вербовку детей или покровительствуемых лиц на оккупированных территориях в вооруженные силы, является незаконной³⁴.

Учитывая вышеупомянутые риски причинения вреда гражданскому населению и другим лицам, пользующимся защитой в соответствии с МГП, необходимо продолжить обсуждение для выработки общего понимания относительно того, как нормы МГП применяются к распространению информации, обеспечивая эффективную защиту всех пользующихся защитой лиц и объектов.

ВОПРОСЫ ДЛЯ ПОДГОТОВКИ ДАЛЬНЕЙШЕЙ ДИСКУССИИ

- Какая деятельность в сфере ИКТ, по мнению вашего государства, подпадает под запрет на поощрение нарушений МГП или подстрекательство к ним? Какие меры были приняты вашим государством для предотвращения такой деятельности?
- Каким образом лица, лишенные свободы, защищены от любопытства толпы, вызванного распространением информации с помощью ИКТ / средств цифровой коммуникации? Какие меры принимаются для предотвращения подобных ситуаций и реагирования на них?
- Принимало ли или рассматривало ли ваше государство принятие каких-либо мер по предотвращению использования информационных операций в нарушение МГП? Можете ли вы поделиться теми или иными полезными наработками?

²⁹ Резолюция по ИКТ, п. 4.

³⁰ См., например: Женевская конвенция III от 12 августа 1949 года, ст. 13; Женевская конвенция IV, ст. 27.

³¹ Для ознакомления с более подробной информацией по этому вопросу см., например: ICRC, *Commentary on the Third Geneva Convention: Convention (III) relative to the Treatment of Prisoners of War*, 2nd ed., ICRC, Geneva, 2020 (далее — ICRC, *Commentary on the Third Geneva Convention*, 2020), paras 1623—1632.

³² Дополнительный протокол I, ст. 51(2); Дополнительный протокол II, ст. 13(2); МККК. Исследование «Обычное международное гуманитарное право», норма 2.

³³ Речь, конечно, не идет о критике или выражении гнева со стороны властей или получателей услуг в адрес медицинских служб или гуманитарных организаций, что само по себе не является противозаконным.

³⁴ По вопросу вербовки детей см.: МККК. Исследование «Обычное международное гуманитарное право», норма 136, а также обязательства по Факультативному протоколу к Конвенции о правах ребенка, касающемуся участия детей в вооруженных конфликтах, от 25 мая 2000 года. По вопросу вербовки покровительствуемых лиц в условиях оккупации см.: Женевская конвенция IV, ст. 51.

III. РИСК ПРИЧИНЕНИЯ ВРЕДА В РЕЗУЛЬТАТЕ ИСПОЛЬЗОВАНИЯ ГРАЖДАНСКОЙ ИКТ-ИНФРАСТРУКТУРЫ В ВОЕННЫХ ЦЕЛЯХ И УЧАСТИЯ ГРАЖДАНСКИХ ЛИЦ В ДЕЯТЕЛЬНОСТИ В СФЕРЕ ИКТ ВО ВРЕМЯ ВООРУЖЕННОГО КОНФЛИКТА

Использование гражданской ИКТ-инфраструктуры в военных целях и влияние такого использования на ее защиту в соответствии с МГП

За исключением некоторых военных сетей, киберпространство является преимущественно гражданским. Однако взаимосвязанность гражданских и военных сетей и использование гражданской ИКТ-инфраструктуры военными порождают ряд проблем в связи с ее защитой.

В случае использования гражданской ИКТ-инфраструктуры (в том числе инфраструктуры, предоставляемой технологическими компаниями) в военных целях (в этом случае такую инфраструктуру иногда называют инфраструктурой «двойного назначения») она рискует стать военным объектом согласно МГП и утратить защиту от нападения³⁵. В подобных случаях гражданские лица и гражданские объекты, находящиеся вблизи такой инфраструктуры, подключенные к ней или зависящие от нее, могут подвергнуться непреднамеренному ущербу.

Однако не каждое использование гражданского объекта в военных целях превращает его в военный объект согласно МГП; это происходит только тогда, когда способ использования отвечает критериям военного объекта, определенным в МГП. При этом, даже если воюющая сторона считает, что гражданское лицо или гражданский объект утратили защиту вследствие участия в деятельности в сфере ИКТ, на любое нападение на них по-прежнему распространяются запрет на неизбирательные и несоразмерные нападения и обязательство принимать все возможные меры предосторожности. Кроме того, некоторые пользующиеся особой защитой объекты, даже если они соответствуют определению военного объекта, не могут подвергаться нападению вообще — либо на нападение на них могут распространяться более строгие ограничения.

Для обеспечения защиты гражданского населения и основных гражданских служб, функционирование которых зависит от ИКТ-инфраструктуры, необходимы дальнейшие обсуждения. Это позволит определить, в каких случаях использование объектов преимущественно гражданской ИКТ-инфраструктуры в военных целях превращает их в военные объекты, а также определить и реализовать другие возможные меры защиты. Например, МККК призвал государства по возможности физически или технически отделить ИКТ-инфраструктуру (или ее части), используемую в военных целях, от гражданской ИКТ-инфраструктуры³⁶. Не менее

³⁵ Объекты двойного назначения могут быть признаны военными, если при существующих в данный момент обстоятельствах они будут удовлетворять определению, приведенному в ст. 52(2) Дополнительного протокола I: «Что касается объектов, то военные объекты ограничиваются теми объектами, которые в силу своего характера, расположения, назначения или использования вносят эффективный вклад в военные действия и полное или частичное разрушение, захват или нейтрализация которых при существующих в данный момент обстоятельствах дает явное военное преимущество».

³⁶ Например, при решении вопроса о том, где хранить военные данные — в не отделенном от гражданской ИКТ-инфраструктуры коммерческом облаке, в выделенном сегменте коммерческого облака или в выделенной военной цифровой инфраструктуре, — специалисты, отвечающие за планирование и реализацию военных операций, не должны использовать первый из этих вариантов. См.: ICRC, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, 2024, pp. 53—54.

важно также обеспечить реализацию любых особых мер защиты, предусмотренных МГП.

Участие гражданских лиц в деятельности в сфере ИКТ во время вооруженного конфликта

В современных вооруженных конфликтах наблюдается несколько тенденций, которые создают угрозу для гражданского населения: гражданские хакеры всё чаще проводят кибератаки на гражданские объекты; стороны в вооруженном конфликте поощряют гражданских лиц собирать сведения военного характера с помощью цифровых средств, подвергая тем самым этих лиц нападениям; а гражданские технологические компании, предоставляющие ИКТ-услуги и инфраструктуру вооруженным силам, рискуют утратить предоставленную им правовую защиту.

В основе МГП лежит важнейший принцип проведения различия. Всё более частые случаи участия гражданских лиц в деятельности в сфере ИКТ и использование гражданской ИКТ-инфраструктуры военными создают угрозу для применения гарантий защиты, которую этот основополагающий принцип призван обеспечить гражданскому населению, в том числе защищая его от ошибочного определения в качестве законных военных целей.

Отдельные лица и группы лиц, включая хакеров и сотрудников технологических компаний, осуществляющие деятельность в сфере ИКТ в условиях вооруженных конфликтов, должны соблюдать ограничения, налагаемые МГП на такую деятельность³⁷, и осознавать связанные с ней риски. В исключительных случаях участие гражданского населения в деятельности в сфере ИКТ может быть приравнено к «непосредственному участию в военных действиях»; это означает, что гражданские лица утрачивают защиту от нападения лишь в подобных ситуациях. Однако в соответствии с нормами МГП при наличии сомнений лица должны считаться гражданскими и подлежать защите в качестве таковых³⁸.

Обязанность государств распространять информацию об МГП, а также предотвращать и пресекать нарушения МГП

Что касается участия гражданского населения в деятельности в сфере ИКТ во время вооруженного конфликта, то следует отметить, что государства обязались соблюдать и обеспечивать соблюдение МГП. Если гражданские хакеры, частные компании или другие частные лица или образования действуют по указаниям либо под руководством или контролем государства, то это государство несет международно-правовую ответственность за любое поведение таких лиц, не соответствующее

³⁷ Что касается гражданских хакеров, действующих в условиях вооруженных конфликтов, то эти ограничения были обобщены в публикации МККК «Восемь правил для „гражданских хакеров” во время войны и четыре обязательства по их сдерживанию для государств» (Eight rules for 'civilian hackers' during war, and four obligations for states to restrain them, доступна на англ. языке по адресу: <https://www.icrc.org/en/article/8-rules-civilian-hackers-during-war-and-4-obligations-states-restrain-them>).

Более подробную информацию по вопросу об актуальности МГП для частных предприятий см.: ICRC, *Private Businesses and Armed Conflict: An Introduction to Relevant Rules of International Humanitarian Law*, 2024.

³⁸ Дополнительный протокол I, ст. 50(1). В случае угрозы вовлечения детей в военные действия посредством их участия в деятельности в сфере ИКТ, в результате чего они будут считаться непосредственными участниками военных действий, воюющие стороны несут дополнительное обязательство по предотвращению вовлечения в такие действия детей младше 15 или 18 лет, в зависимости от применимого законодательства.

международно-правовым обязательствам государства, включая обязательства по МГП³⁹.

Даже если поведение гражданских лиц не присваивается стороне в вооруженном конфликте, государства тем не менее обязаны обеспечить соблюдение МГП. Как минимум стороны в вооруженном конфликте не должны поощрять гражданских лиц, участвующих в деятельности в сфере ИКТ, нарушать МГП, а также помогать или содействовать им в совершении таких нарушений⁴⁰ (например, поощрять их проводить кибероперации против гражданских объектов). Кроме того, государства должны распространять информацию об МГП, предотвращать и пресекать нарушения МГП, а также расследовать военные преступления (в том числе совершенные гражданским населением) и преследовать лиц, виновных в их совершении⁴¹.

ВОПРОСЫ ДЛЯ ПОДГОТОВКИ ДАЛЬНЕЙШЕЙ ДИСКУССИИ

- Каким образом ваше государство оценивает риски для гражданского населения и основных гражданских служб в тех случаях, когда ИКТ-инфраструктура выполняет как гражданские, так и военные функции? Каким образом применяются принципы проведения различия, соразмерности и принятия мер предосторожности при рассмотрении возможности осуществления деятельности в сфере ИКТ в отношении инфраструктуры «двойного назначения»?
- Какие, по мнению вашего государства, существуют риски в тех случаях, когда гражданским лицам предлагается или разрешается осуществлять деятельность в сфере ИКТ в связи с вооруженным конфликтом, и какие меры следует принять для снижения таких рисков?
- Какие меры следует принимать государствам, с тем чтобы гражданские лица, участвующие в деятельности в сфере ИКТ во время вооруженного конфликта, были осведомлены о своих обязательствах по МГП и соблюдали их? Существует ли в вашем государстве законодательство, регулирующее этот вопрос и направленное на предотвращение и пресечение возможных нарушений МГП?

³⁹ Согласно международному публичному праву государство несет ответственность за поведение частных лиц, групп или образований (включая гражданских хакеров или хакерские группы), если они уполномочены «правом этого государства осуществлять элементы государственной власти» или «фактически» действуют «по указанию либо под руководством или контролем этого государства». См.: *Комиссия международного права*. Ответственность государств за международно противоправные деяния, 2001 г., ст. 5 и 8.

⁴⁰ ICRC, Commentary on the Third Geneva Convention, 2020, Article 1, para. 191.

⁴¹ ICRC, Commentary on the Third Geneva Convention, 2020, Article 1, para. 183.