Humanity In War

В рамках Глобальной инициативы по усилению политической приверженности международному гуманитарному праву (Глобальной инициативы в области МГП) **Гана, Люксембург, Мексика, Швейцария и Международный Комитет Красного Креста (МККК)** рады представить следующее мероприятие:

НАПРАВЛЕНИЕ ДЕЯТЕЛЬНОСТИ 6

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

Для работающих в столицах своих государств государственных должностных лиц, специализирующихся в области МГП, кибербезопасности и военных операций с использованием ИКТ, а также сотрудников постоянных представительств в Женеве

ПОНЕДЕЛЬНИК, 24 НОЯБРЯ 2025 Г.
9:00–18:00 (UTC +1)

ФОРМАТ: ОЧНЫЙ (ЦЕНТР МККК «ГУМАНИТАРИУМ» В ЖЕНЕВЕ) И ОНЛАЙН (ZOOM)

Справочная информация

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.

Данное направление деятельности, реализуемое в рамках Глобальной инициативы в области МГП, является продолжением международных дискуссий, посвященных использованию ИКТ, и основывается на достигнутом к настоящему времени прогрессе в этом вопросе, в частности на резолюции 2 «Защита гражданского населения и других покровительствуемых лиц и объектов от потенциальных гуманитарных последствий деятельности в сфере ИКТ во время вооруженного конфликта», принятой на 34-й Международной конференции Красного Креста и Красного Полумесяца. Это направление деятельности реализуется в рамках непрерывных усилий по выработке общего понимания ограничений, налагаемых нормами МГП на деятельность в сфере ИКТ во время вооруженных конфликтов в целях защиты гражданского населения от причинения ему вреда.

Первая консультация в рамках данного направления деятельности, состоялась 15 мая 2025 г. Она была 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, а также иным покровительствуемым лицам и объектам в условиях вооруженного конфликта. Вторая консультация призвана развить результаты состоявшихся обсуждений. Она будет проведена в смешанном формате 24 ноября 2025 г. в Женеве.

Для получения более подробной информации о вопросах, рассматриваемых в рамках данного направления деятельности, участники могут ознакомиться с прилагаемым **справочным документом**.

Цели

В основу второй консультация лягут результаты обсуждений, состоявшихся в ходе первой консультации, и сделанные ее участниками ключевые выводы. Она будет посвящена более детальному обсуждению правовых и гуманитарных вопросов, возникающих в связи с использованием ИКТ во время вооруженного конфликта. Участники консультации попытаются выработать общую позицию и сформулировать потенциальные юридические и практические рекомендации по обеспечению более эффективной защиты гражданского населения и гражданских объектов в условиях военных действий с использованием цифровых технологий.

Цели этой консультации состоят в том, чтобы:

- **предоставить информацию о ходе работы в рамках данного направления деятельности**:

- проинформировать участников о результатах первой консультации, отраженных в промежуточном докладе, а также о выводах, сделанных в ходе последующих дополнительных мероприятий;
- определить дальнейшие действия по выработке окончательных рекомендаций в рамках данного направления деятельности;

- **более детально обсудить выявленные правовые и гуманитарные вопросы для выработки общей позиции по ним:**
  - провести углубленный обмен мнениями по вопросам, выявленным в ходе первой консультации, для их дальнейшего рассмотрения, включая следующие вопросы:
    - последствия (с точки зрения норм МГП) операций в сфере ИКТ, причиняющих иной ущерб, помимо физического (например, утрата той или иной системой своей функциональности);
    - предоставляемая нормами МГП защита данных гражданского назначения и других данных от, например, искажения, повреждения, удаления, несанкционированного получения над ними контроля и их несанкционированной публикации;
    - предоставляемая нормами МГП особая защита определенных категорий лиц, объектов и видов деятельности (в том числе принадлежащих им данных и цифровой инфраструктуры) от последствий деятельности в сфере ИКТ во время вооруженного конфликта;
    - ограничения, налагаемые нормами МГП на информацию, распространяемую в рамках деятельности в сфере ИКТ;
    - последствия (с точки зрения норм МГП) использования гражданской ИКТ-инфраструктуры в военных целях и участия гражданских лиц в осуществлении операций в сфере ИКТ в условиях вооруженного конфликта, а также основанные на нормах МГП меры по минимизации риска причинения вреда гражданским лицам и основным гражданским службам;
  - повысить эффективность практических мер, направленных на обеспечение соблюдения МГП и минимизацию вреда гражданскому населению и гражданским объектам.

Дальнейшие действия

На начало 2026 года запланировано проведение третьей консультации с государствами для продолжения обсуждений, состоявшихся в рамках первой и второй консультаций, и закрепления общих позиций, выработанных по их результатам. Эти консультации заложат основу для рекомендаций, которые предстоит выработать в рамках данного направления деятельности. Во втором квартале 2026 года у всех заинтересованных государств будут запрошены отзывы для выработки таких рекомендаций, которые будут дополнительно рассмотрены в ходе будущих консультаций с государствами.

Помимо консультаций с государствами планируется проведение региональных дискуссий и других дополнительных мероприятий, которые будут анонсироваться на сайте Humanity in War.

Участники

- Консультация будет проводиться преимущественно в очном формате в Женеве. Возможно также участие в режиме онлайн.
- К участию в консультации **приглашаются все заинтересованные государства**. Весьма приветствуется участие работающих в столицах своих государств государственных должностных лиц, специализирующихся в области МГП, кибербезопасности и военных операций с использованием ИКТ, а также сотрудников постоянных представительств в Женеве.
- Участие в консультации по приглашению примут также и другие профильные специалисты (представители международных организаций, гражданского общества и научного сообщества).
- Зарегистрироваться можно не позднее 15 ноября 2025 г. по ссылке: https://forms.office.com/e/LuDKik93vY.

Порядок проведения

- Рабочие языки консультации — **английский, арабский, испанский, китайский, русский и французский**, будет осуществляться синхронный перевод.
- Убедительно просим государства ограничить свои выступления **четырьмя минутами**, чтобы всем участникам хватило времени выступить. В конце каждой сессии, после того, как выступят все желающие делегаты, государствам и другим участникам будет предоставлена возможность обсудить высказанные идеи.
- При подготовке своих выступлений просим участников учитывать **вопросы для подготовки**, приведенные в программе мероприятия ниже. Некоторые вопросы для подготовки сопровождаются **наглядными сценариями**, которые необходимо рассматривать во взаимосвязи с конкретными вопросами. К настоящей пояснительной записке прилагается **справочный документ**, призванный помочь организовать и провести обсуждение.
- Ввиду технических трудностей, связанных с проведением встреч в смешанном формате, мы призываем делегации, находящиеся в зале, выступать со своими заявлениями лично и внимательно выслушивать делегации, участвующие в мероприятии в режиме онлайн.
- На протяжении всей консультации будет сохраняться **инклюзивный, конструктивный, неполитизированный и ориентированный на поиск решений** характер обсуждений. В ходе консультаций мы предлагаем участникам ссылаться на национальную практику собственного государства, однако убедительно просим их воздерживаться от обсуждения конкретных ситуаций или практики других государств.
- В целях содействия работе переводчиков просим участников направить копии своих выступлений по электронной почте ihlinitiative@icrc.org до 21 ноября 2025 г., указав в теме письма следующее: «ICT workstream second consultation» («Вторая консультация в рамках направления деятельности, посвященного ИКТ»). Мы также призываем участников по завершении мероприятия направить полный текст своих выступлений

в письменной форме по электронной почте. **Предоставленная информация будет опубликована на сайте МККК, за исключением тех случаев, когда государства попросят обеспечить ее конфиденциальность.**

- Консультация будет записываться, но эти записи не будут выложены для публичного доступа.

Программа

Соблюдение международного гуманитарного права при использовании информационно-коммуникационных технологий во время вооруженных конфликтов
(направление деятельности, посвященное ИКТ)
Второй раунд консультаций

9:00–18:00, 24 ноября 2025 г.
Центр МККК «Гуманитариум» в Женеве (17 avenue de la Paix, 1202 Geneva)

** Периоды времени, указанные ниже, могут быть изменены в зависимости от количества выступлений.*

Регистрация участников и кофе / Подключение участников в режиме онлайн	8:30–9:00
Открытие мероприятия и вступительное слово	9:00–9:30
Панельная дискуссия. Основные правовые и гуманитарные вопросы, возникающие в связи с использованием ИКТ во время вооруженного конфликта	9:30–10:30
Сессия 1. Практические меры по обеспечению соблюдения МГП и защиты гражданских лиц при использовании ИКТ во время вооруженного конфликта	10:30–11:30
Вопросы для подготовки 1. Какие юридические и оперативные меры ваше государство приняло или планирует принять для обеспечения соблюдения МГП и предотвращения или минимизации вреда гражданским лицам при проведении деятельности в сфере ИКТ во время вооруженного конфликта? Ввиду особенностей операций в сфере ИКТ — чем эти меры отличаются от мер, применяемых при проведении операций с использование кинетического оружия, и как указанные особенности могут быть учтены? 2. Какие меры ваше государство принимает или планирует принять для предотвращения и пресечения нарушений МГП, совершаемых в ходе деятельности в сфере ИКТ или в связи с ней? 3. Какие формы укрепления потенциала или международного сотрудничества были бы наиболее полезны в плане оказания государствам содействия в обеспечении более строгого соблюдения МГП и обмена практическим опытом в этой области?	
Перерыв на кофе	11:30–12:00
Сессия 2. Защита гражданского населения и других покровительствуемых лиц и объектов от опасностей, возникающих в результате деятельности в сфере ИКТ во время вооруженного конфликта	12:00–13:00
Вопросы для подготовки	

1. В чем заключаются гуманитарные последствия (и последствия с точки зрения норм МГП) операций в сфере ИКТ, причиняющих иной ущерб, кроме физического (например, утрата той или иной системой своей функциональности)?

   Рассмотрите следующий сценарий. В условиях вооруженного конфликта проводится операция в сфере ИКТ, направленная на гражданский объект (например, на сервер транспортной компании, интернет-провайдера или банка). На момент проведения операции этот сервер не используется каким бы то ни было образом, который позволил бы признать его военным объектом. В результате операции данный объект утрачивает обычную для него функциональность, но при этом он физически не поврежден. Каким образом ваше государство оценивает законность такой операции в сфере ИКТ? Поменяется ли ваша оценка, если в результате прогнозируемых прямых или косвенных последствий этой операции сервер будет все-таки физически поврежден?

2. Каким образом ваше государство в соответствии с нормами МГП обеспечивает защиту данных гражданского назначения и других данных от, например, искажения, повреждения, удаления, несанкционированного получения над ними контроля и их несанкционированной публикации? Проводит ли ваше государство различия между разными категориями данных (медицинскими, биометрическими, финансовыми и другими данными) при оценке мер по их защите в соответствии с нормами МГП?

   Рассмотрите следующий сценарий. В условиях вооруженного конфликта проводится операция в сфере ИКТ, направленная на удаление определенных данных гражданского назначения (например, медицинских данных, данных органов социального обеспечения, данных банковских счетов, налоговой документации или клиентских баз гражданских компаний). Каким образом ваше государство оценивает законность такой операции в сфере ИКТ? Какие нормы МГП ограничивают операции, направленные на искажение, повреждение или уничтожение данных гражданского назначения или других находящихся под защитой данных во время вооруженного конфликта? Какую защиту предоставляют нормы МГП от несанкционированного копирования данных гражданского назначения или других находящихся под защитой данных, несанкционированного получения над ними контроля и их возможной публикации?

3. Какие нормы МГП обеспечивают защиту гражданских лиц и гражданских объектов от операций в сфере ИКТ, которые согласно МГП не квалифицируются как «нападение»? Например, какие практические меры должны приниматься для соблюдения обязательства на постоянной основе обеспечивать защиту гражданского населения, гражданских лиц и гражданских объектов при проведении операций в сфере ИКТ в рамках военных действий?

Обед (не предоставляется)	13:00–14:00

Сессия 3. Внедрение гарантий особой защиты определенных категорий лиц, объектов и видов деятельности от последствий использования ИКТ во время вооруженного конфликта	14:00–15:00
Вопросы для подготовки 1. Какие практические меры ваше государство принимает или планирует принять для того, чтобы деятельность в сфере ИКТ во время вооруженного конфликта не приводила к нарушению функционирования медицинских служб, гуманитарных организаций и объектов, необходимых для выживания гражданского населения, включая принадлежащие им ИКТ-системы и данные? Какие меры предосторожности ваше государство принимает или планирует принять для защиты таких пользующихся особым покровительством объектов от причинения им вреда, включая вред, причиняемый в результате деятельности в сфере ИКТ? 2. Рассмотрите следующий сценарий, связанный с особой защитой медицинских учреждений и их персонала. В условиях вооруженного конфликта одна из сторон проводит операцию в сфере ИКТ, направленную на то, чтобы получить доступ к серверам медицинского учреждения на территории противника. Она получает доступ к медицинским данным военнослужащих, находящихся на лечении в этом учреждении, а затем зашифровывает весь массив данных о пациентах, делая его недоступным для медицинского персонала. В какой степени особая защита медицинских учреждений предусматривает обеспечение конфиденциальности, целостности и доступности данных, к которым такие учреждения имеют доступ и которые они собирают, обрабатывают и хранят для целей своей деятельности? Насколько такая же защита применяется к данным, доступ к которым имеют гуманитарные организации и их персонал и которые они собирают, обрабатывают и хранят для целей своей гуманитарной деятельности? 3. Какие особые риски возникают в связи с деятельностью в сфере ИКТ в части нарушения запрета на сексуальное насилие и/или незаконную вербовку детей или их использования в военных действиях? Какие практические меры ваше государство приняло или планирует принять для предотвращения таких незаконных действий и реагирования на них?	
Сессия 4. Защита гражданского населения и других покровительствуемых в соответствии с нормами МГП лиц от информации, распространяемой в нарушение МГП во время вооруженного конфликта	15:00–16:00
Вопросы для подготовки 1. Какие ограничения налагаются нормами МГП на распространение информации в рамках деятельности в сфере ИКТ во время вооруженного конфликта? Рассмотрите следующий сценарий. Одна из сторон в вооруженном конфликте проводит информационную кампанию, в рамках которой:	

• в интернете размещаются изображения военнопленных, показывающие, как с ними обращаются; • фабрикуются и распространяются в социальных сетях сообщения, нагнетающие напряженность между местными жителями, что повышает риск насилия. Какие гарантии защиты или механизмы контроля ваше государство внедрило или планирует внедрить для предотвращения ситуаций, когда в ходе деятельности в сфере ИКТ лица, лишенные свободы, выставляются на обозрение любопытствующей толпы? Каким образом ваше государство определяет, представляют ли собой информационные операции, проводимые с использованием ИКТ, запрещенные действия, направленные на поощрение нарушений МГП или подстрекательство к ним, либо действия, имеющие своей целью терроризировать гражданское население? 2. Какие меры принимает ваше государство для устранения риска того, что распространение дезинформации с помощью ИКТ может помешать оказанию медицинских услуг или осуществлению гуманитарной деятельности во время вооруженного конфликта? Рассмотрите следующий сценарий. Одна из сторон в вооруженном конфликте проводит в интернете кампанию по распространению сфабрикованных изображений и размещению ложной информации в социальных сетях, заявляя, что некая больница якобы является опорным пунктов комбатантов. Такая дезинформация порождает недоверие у местного населения и затрудняет доступ в больницу медицинского персонала; кроме того, сотрудники, посещающие учреждение, всё чаще становятся объектом провокаций и запугиваний. Какие нормы МГП обеспечивают защиту медицинских служб и гуманитарных организаций от распространения дезинформации с помощью цифровых технологий? Какие юридические или оперативные меры ваше государство приняло или планирует принять для устранения таких рисков? 3. Какие другие меры ваше государство приняло или планирует принять в целях предотвращения использования ИКТ, включая социальные сети, для распространения той или иной информации в нарушение норм МГП?	
Перерыв на кофе	16:00–16:30
Сессия 5. Устранение риска причинения вреда в результате использования гражданской ИКТ-инфраструктуры в военных целях и участия гражданских лиц в деятельности в сфере ИКТ во время вооруженного конфликта	16:30–17:30
Вопросы для подготовки 1. Каковы гуманитарные последствия (и последствия с точки зрения МГП) использования гражданской ИКТ-инфраструктуры в военных целях, и какие меры, основанные на нормах МГП, необходимо принять для минимизации риска причинения вреда гражданским лицам и основным гражданским службам? Рассмотрите следующий сценарий. На территории государства, участвующего в вооруженном конфликте, находится коммерческий	

центр обработки данных, в котором размещаются военные данные и приложения, а также данные гражданского населения и приложения, используемые для предоставления основных гражданских услуг.

- Каким образом ваше государство применяет нормы и принципы МГП (такие как принцип проведения различия, принцип соразмерности и принцип принятия мер предосторожности) при оценке возможности проведения операции в сфере ИКТ в отношении такой ИКТ-инфраструктуры? В случае если какая-либо часть этой ИКТ-инфраструктуры (например, облачный сервер) признаётся военным объектом, каким образом необходимо учитывать последствия проведения в отношении него операции в сфере ИКТ для гражданского населения при планировании и проведении этой операции?
- Какие меры предосторожности может и должно принять государство, проводящее операцию в сфере ИКТ, для защиты гражданского населения и основных гражданских служб, зависящих от ИКТ-инфраструктуры, которая является объектом такой операции?
- Какие меры предосторожности может и должно принять государство, на территории которого располагается центр обработки данных, для защиты гражданского населения и гражданских объектов, находящихся под его контролем, от последствий операций в сфере ИКТ, которые проводятся в отношении этого центра?
- Какие меры предосторожности может и должна принять компания, являющаяся собственником или оператором центра обработки данных, для предотвращения негативных последствий для данных гражданского назначения в результате операций в сфере ИКТ, направленных на военные данные и приложения, которые размещены в этом же центре?

2. Какие опасности могут возникнуть для гражданских лиц в результате их участия в деятельности в сфере ИКТ во время вооруженного конфликта, и какие меры, основанные на нормах МГП, необходимо принять для минимизации рисков для таких лиц?

   Рассмотрите следующий сценарий. В условиях вооруженного конфликта гражданские хакеры на территории одной из воюющих сторон проводят операции в сфере ИКТ, направленные на то, чтобы нарушить функционирование военных коммуникаций или нанести ущерб ИКТ-инфраструктуре частных компаний в целях ослабления экономики вражеского государства и подрыва морального духа его населения.

   - Какие юридические обязательства в соответствии с нормами МГП должны соблюдаться гражданскими хакерами при проведении любых таких операций в сфере ИКТ?
   - Какие меры против таких операций в сфере ИКТ может принять затронутое ими государство?

3. Какие практические меры ваше государство приняло или рассматривает возможность принять для обеспечения того, чтобы гражданские лица, находящиеся на его территории или под его контролем (например,

гражданские хакеры, хакерские группы или сотрудники технологических компаний, занимающиеся деятельностью в сфере ИКТ в связи с вооруженным конфликтом), знали о применимых нормах МГП и соблюдали их, осознавали риски, связанные с их действиями, и были в максимально возможной степени защищены от таких рисков?	
Заключительные слова	17:30–18:00