


Научная статья  
УДК 343.3/7  
DOI: 10.47475/2311-696X-2025-47-4-182-187

С. 182–187

## ПРАВОВОЙ РЕЖИМ КИБЕРОРУЖИЯ В ФОКУСЕ СОВРЕМЕННОГО МЕЖДУНАРОДНОГО ГУМАНИТАРНОГО ПРАВА

Дмитрий Владимирович Лобач

*Дальневосточный юридический институт (филиал) Университета прокуратуры Российской Федерации,  
г. Владивосток, Россия  
dimaved85@mail.ru  
 <https://orcid.org/0000-0002-7229-439X>*

**Аннотация.** В статье предпринята попытка исследования правового режима кибероружия с позиции современного международного гуманитарного права. Рассмотрены два подхода относительно правовой оценки применения кибероружия в практике международных отношений: 1) кибероружие как агрессивное применение информационно-коммуникационных технологий против другого государства, которое не квалифицируется как противоправное применение силы в условиях вооруженного конфликта; 2) кибероружие как средство для проведения кибератак, квалифицируемых как противоправное применение силы в условиях вооруженного конфликта. Делается вывод о том, что современное международное гуманитарное право в контексте своего исторического развития охватывает прежде всего отношения, связанные с традиционным применением вооруженных сил в условиях вооруженного конфликта. Сплошной анализ положений международного гуманитарного права не позволяет констатировать возможность квалификации кибероружия в качестве военных преступлений. Отмечается, что современные военные операции представляют собой не только кинетическое, но также и кибернетическое воздействие на объекты соответствующего противника в условиях вооруженного противостояния. Выдвигается предположение, что к таким операциям должны применяться одни и те же нормы и принципы, включая принципы гуманности, военной необходимости, проведения различия, соразмерности и принятия мер предосторожности.


**Ключевые слова:** преступления против мира и безопасности человечества, кибероружие, военные преступления, информационно-коммуникационные технологии, международное гуманитарное право, вооруженный конфликт

**Для цитирования:** Лобач Д. В. Правовой режим кибероружия в фокусе современного международного гуманитарного права // Правопорядок: история, теория, практика. 2025. № 4(47). С. 182–187. DOI: 10.47475/2311-696X-2025-47-4-182-187

Research article

## THE LEGAL REGIME OF CYBERWEAPONS IN THE FOCUS OF MODERN INTERNATIONAL HUMANITARIAN LAW

Dmitry V. Lobach

*Far Eastern Law Institute (branch) University of the Prosecutor's Office of the Russian Federation, Vladivostok, Russia  
dimaved85@mail.ru  
 <https://orcid.org/0000-0002-7229-439X>*

**Abstract.** The article attempts to study the legal regime of cyber weapons from the standpoint of modern international humanitarian law. Two approaches are considered regarding the legal assessment of the use of cyber weapons in the practice of international relations: 1) cyber weapons as an aggressive use of information and communication technologies against another state, which is not classified as an unlawful use of force in an

armed conflict; 2) cyber weapons as a means of conducting cyber attacks qualified as an unlawful use of force in an armed conflict. It is concluded that modern international humanitarian law in the context of its historical development primarily covers relations associated with the traditional use of armed forces in an armed conflict. A complete analysis of the provisions of international humanitarian law does not allow us to state the possibility of qualifying cyber weapons as war crimes. It is noted that modern military operations represent not only kinetic, but also cybernetic impact on the objects of the corresponding enemy in an armed confrontation. It is suggested that the same rules and principles should apply to such operations, including the principles of humanity, military necessity, distinction, proportionality and precautions.

**Keywords:** crimes against the peace and security of mankind, cyber weapons, war crimes, information and communication technologies, international humanitarian law, armed conflict

**For citation:** Lobach DV. The legal regime of cyberweapons in the focus of modern international humanitarian law. *Pravoporyadok: istoriya, teoriya, praktika* [Legal and Order: History, Theory, Practice]. 2025;(4):182-187. (In Russ.) DOI: 10.47475/2311-696X-2025-47-4-182-187

## Введение

Содержание современных вооруженных конфликтов, исторически определяемых в рамках традиционной военной теории как вооруженное противостояние между специально организованными и идентифицируемыми военизированными формированиями, имеющими стабильный состав, единое руководство и подчиненными строгой дисциплине, изменяется в силу широкого применения различных информационно-коммуникационных технологий (далее — ИКТ), используемых в военных целях [6]. В современной военной науке, юридической теории, системе международного гуманитарного права и практике международных отношений подобное применение ИКТ более известно как кибератака, а состояние вооруженного конфликта, сопровождаемого активным использованием ИКТ, получило такое название как кибервойна [5]. Вместе с тем в современном гуманитарном праве пока отсутствует единый подход к пониманию того, что такое кибероружие, и все еще нет устоявшейся политико-правовой оценки критериев использования ИКТ в военных целях в условиях вооруженного конфликта.

## Материал и методы

В статье анализируются нормы международных правовых актов, регулирующие отношения в области информационной безопасности, связанные с вооруженным конфликтом или возникающие в результате совершения международных преступлений. Основу исследования составили общенаучные и частнонаучные методы научного познания, анализ теоретических и нормативных правовых источников. Из специальных методов исследования использовались в основном сравнительно-правовой и формально-юридический методы.

## Описание исследования

### 1. Понятие и общая характеристика кибероружия

В современных международных документах в области обеспечения информационной безопасности (Конвенция Совета Европы «О преступности в сфере компьютерной информации» от 2001 г.; Конвенция Африканского Союза «О кибербезопасности и защите

персональных данных» от 2014 г.; Соглашение о сотрудничестве государств — участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации от 2001 г.; Конвенция Лиги арабских государств «О борьбе с преступлениями в области информационных технологий» от 2010 г.) отсутствует какое-либо упоминание о кибероружии, кибератаках и кибервойне. Однако описание объективной стороны отдельных компьютерных преступлений позволяет увидеть функциональный аспект искомых явлений, который выражается во всем многообразии вредоносных вирусов, троянов, шпионских программ и червей, способных интегрировать поврежденный код в программное обеспечение атакуемого компьютера, заставляя его тем самым выполнять действия и процессы, незапрограммированные его оператором.

Рамочные определения того, что такое кибероружие и кибервойна, раскрываются в Соглашении между Правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности от 2009 г. Данные понятия определяются через указание на их информационную составляющую. В частности, кибероружие определено как информационное оружие, которое представляет собой информационные технологии, средства и методы, применяемые в целях ведения информационной войны. В документе также дается широкое определение информационной войны, которое раскрывается как противоборство между двумя или более государствами в информационном пространстве с целью нанесения ущерба информационным системам, процессам и ресурсам, критически важным и другим структурам, подрыва политической, экономической и социальной систем, массивной психологической обработки населения для дестабилизации общества и государства, а также принуждения государства к принятию решений в интересах противоборствующей стороны.

Из определения видно, что обозначенное понятие отражает в себе два варианта использования ИКТ: 1) информационно-коммуникационные технологии используются в целях нанесения ущерба информаци-

онным системам, процессам и ресурсам, критически важным и другим структурам; 2) информационно-коммуникационные технологии используются в целях психологической обработки населения и воздействия на государственные структуры. Условно говоря, в первом случае речь идет о применении специального программного инструментария (вредоносные вирусы, трояны, шпионские программы) в целях воздействия на компьютеры или компьютерные системы других операторов, а во втором случае — об использовании информационных технологий в целях оказания манипулятивного воздействия на общественное сознание и работу государственных органов. Применительно к целям данной статьи и обозначенной проблематике, в дальнейшем речь пойдет о кибероружии. Это компьютерный инструментарий, то есть все многообразие вредоносного программного обеспечения (вредоносные вирусы, трояны, шпионские программы), которое намеренно создается для нарушения работы компьютера, сервера, клиента или компьютерной сети, утечки личной информации, получения несанкционированного доступа к информации или системам, лишения пользователей доступа к информации или которое неосознанно нарушает компьютерную безопасность и конфиденциальность пользователя [7].

В случае признания ИКТ в качестве возможного оружия в условиях вооруженного конфликта возникает юридическая возможность: во-первых, квалифицировать отдельные бесчеловечные деяния, совершаемые через использование ИКТ, в качестве военных преступлений; во-вторых, отграничивать правомерное применение силы одним государством против суверенитета, территориальной целостности и политической независимости другого государства от его неправомерного проявления, которое при определенных обстоятельствах может быть квалифицировано как вооруженная агрессия (преступление агрессии). Не следует забывать и тот факт, что возможное признание кибератаки в качестве акта агрессии может спровоцировать ответные действия обороняющегося государства на основании своего права на самооборону, предусмотренного ст. 51 Устава ООН, что может привести к осложнению международных отношений.

Учитывая современные тренды развития международных отношений, практику межгосударственного сотрудничества в сфере обеспечения международной и национальной информационной безопасности, состояние правовой науки и развитие международного гуманитарного права, представляется возможным предложить два подхода к рассмотрению правовой природы кибероружия и связанных с ним кибератак: 1) кибероружие и кибератаки, которые не квалифицируются как противоправное применение силы в условиях вооруженного конфликта; 2) кибероружие как инструмент для проведения кибернетических атак, квалифицируемых как противоправное применение силы в условиях вооруженного конфликта.

В свою очередь, раскрытие данного феномена

в контексте правовой регламентации отношений, регулируемых современным международным гуманитарным правом и правом международной безопасности, с учетом оценочного понимания концепта «кибератака», следует рассматривать как методологическую основу данного исследования.

## **2. Кибератаки как агрессивное применение информационно-коммуникационных технологий против другого государства, которые не квалифицируются как противоправное применение силы в условиях вооруженного конфликта**

Исторически международное гуманитарное право возникает и развивается как отрасль международного публичного права для защиты прав, свобод и законных интересов участников вооруженного конфликта и лиц, не являющихся таковыми, но находящихся в эпицентре вооруженного конфликта. При этом вооруженный конфликт традиционно воспринимается как вооруженное противостояние между двумя и более государствами вне зависимости от того, признают ли все стороны состояние войны, а также как длительное вооруженное противостояние между государственными вооруженными силами и организованными военизированными группировками или между самими такими группировками, которые находятся под ответственным командованием, осуществляют контроль над частью территории, что позволяет им проводить непрерывные и согласованные военные действия в пределах территории одного государства. Обязательным условием вооруженного конфликта является присутствие вооруженных сил, под которыми следует понимать всех лиц, которые принимают участие от имени стороны в конфликте и подчиняются ее командованию. В основе понятия «вооруженный конфликт» положен концепт «вооруженное противостояние», что свидетельствует о применении особых средств и методов силового противоборства. Под средствами ведения боевых действий следует понимать любые виды оружия, боеприпасов, веществ и военной техники, которые применяются вооруженными силами воюющих сторон для нанесения вреда и поражения сил противника в целях подавления сил и способности к сопротивлению. Методы ведения военных действий представляют собой порядок, практику и сочетание всевозможных способов применения разных видов средств ведения войны в указанных целях.

Внимательное изучение норм Женевских конвенций от 1949 г. (далее — Женевское право) позволяет увидеть, что во всех случаях, где говорится об использовании оружия в контексте вооруженного конфликта, имеется в виду исключительно только обычное вооружение (ст. 3, 13, 19, 32 Женевской конвенции об улучшении участи раненых и больных в действующих армиях от 12 августа 1949 г., ст. 3, 13, 35 Женевской конвенции об улучшении участи раненых, больных и лиц, потерпевших кораблекрушение, из состава вооруженных сил на море от 12 августа 1949 г., ст. 4, 18, 42 Женевской конвенции об обращении с военнопленными от 12 августа

1949 г., ст. 3 и 19 Женевской конвенции о защите гражданского населения во время войны от 12 августа 1949 г., ст. 13, 28, 44, 56, 65, 67 Дополнительного протокола к Женевским конвенциям от 12 августа 1949 года, касающегося защиты жертв международных вооружённых конфликтов (Протокол I).

Режим запрещения отдельных видов вооружения установлен в ряде международных конвенций, принятых в разное время под эгидой ООН. К таким документам, в частности, можно отнести Конвенцию ООН по конкретным видам обычного оружия от 1980 г. (включая 5 дополнительных протоколов к Конвенции), Оттавскую конвенцию о запрещении противопехотных мин от 1997 г., Дублинскую конвенцию о запрещении касетных боеприпасов от 2008 г., Договор о принципах деятельности государств по исследованию и использованию космического пространства, включая Луну и другие небесные тела от 1967 г., Конвенцию о запрещении разработки, производства и накопления бактериологического (биологического) оружия и токсинов и его уничтожении от 1975 г., Конвенцию о запрещении военного или любого иного враждебного использования средств воздействия на природную среду от 1978 г., Конвенцию о запрещении разработки, производства, накопления и применения химического оружия и его уничтожении от 1997 г.

Однако в современных условиях развития международного права все еще нет специальной конвенции, которая бы устанавливала юридические параметры кибернетического оружия (кибероружия), позволяющие отграничивать его от других видов угроз в информационном пространстве, и закрепляла бы запрет (или ограничение) на его применение в условиях вооруженного конфликта. В то же время об ограниченном действии Женевского права в части возможного расширения его регулятивного действия в отношении новых видов оружия сделана оговорка в ст. 36 Дополнительного протокола к Женевским конвенциям от 12 августа 1949 года, касающегося защиты жертв международных вооружённых конфликтов (Протокол I), в которой закреплено, что при разработке и принятии новых видов оружия, средств и методов ведения войны государства должны определиться, подпадает ли их применение под нормы международного гуманитарного права.

Кроме того, также необходимо обратить внимание на то, что, несмотря на расширение в рамках Римского статута Международного уголовного суда от 1998 года группы военных преступлений за счет криминализации применения оружия, использующего микробиологические или другие биологические агенты или токсины, каково бы ни было их происхождение или способ производства, оружия, основным действием которого является ранение осколками, не обнаруживаемыми рентгеновскими лучами в человеческом теле, а также ослепляющего лазерного оружия<sup>1</sup>, кибероружие и кибе-

<sup>1</sup> Amendment to article 8 of the Rome Statute of the International Criminal Court (Weapons which use microbial or other biological

ратаки все еще не являются предметом регулятивного действия норм данного документа в части установления ответственности за военные преступления.

Исходя из всего вышесказанного, следует признать, что в рамках данного подхода кибероружие и связанные с ним кибератаки могут быть определены только как агрессивное применение ИКТ против интересов другого государства безотносительно наличия или отсутствия вооруженного конфликта, так как современное состояние международного гуманитарного и уголовного права, выраженное в действующих документах, не содержит конкретных норм, регламентирующих запрет и, соответственно, ответственность за применение ИКТ в качестве запрещенного оружия.

### 3. Кибероружие как инструмент для проведения кибернетических атак, квалифицируемых как противоправное применение силы в условиях вооруженного конфликта

В рамках данного подхода обосновывается позиция, в соответствии с которой применение ИКТ в агрессивных целях в условиях вооруженного конфликта при определенных условиях может быть квалифицировано как противоправное действие с позиции международного гуманитарного права. Такое допущение основывается на обычно-правовом характере международного гуманитарного права, в соответствии с которым нормы, регламентирующие поведение участников вооруженного конфликта, закреплены не только в актах договорного права, но и в правовых обычаях и связанных с ними требованиях общечеловеческой гуманности<sup>2</sup>. Несмотря на то, что договорное право в силу своей формальной определенности является наиболее очевидным источником международного гуманитарного права, что делает его применение более вероятным и эффективным с позиции механизма правового регулирования отношений, связанных с вооруженным конфликтом, отдельные нормы и принципы содержатся в обычаях, нашедших свое отражение в общей практике государств, которая является констатацией признания субъектами правотворчества (субъектами международного права) соответствующих правил поведения в качестве норм права (*opinio juris*).

agents, or toxins) // United National Treaty Collection. URL: [https://translated.turbopages.org/proxy\\_u/en-ru.ru.18b29799-62e0d196-40df20a4-74722d776562/https/treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg\\_no=XVIII-10-d&chapter=18&clang=en](https://translated.turbopages.org/proxy_u/en-ru.ru.18b29799-62e0d196-40df20a4-74722d776562/https/treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XVIII-10-d&chapter=18&clang=en) (дата обращения: 30.09.2025).

<sup>2</sup> Великий вклад в развитие международного гуманитарного права в части регулятивного расширения действия его норм был внесен в конце XIX в. российским юристом-международником Ф. Мартенсом, который сделал оговорку, вошедшую в преамбулу II Гаагской конвенции 1899 года, о том, что в случаях, не предусмотренных международными соглашениями, гражданские лица и комбатанты остаются под защитой и действием принципов международного права, проистекающих из установившихся обычаев, принципов гуманности и требований общественного сознания. Данное положение стало уникальным юридическим приемом, демонстрирующим эффективное и адаптивное действие морального регулирования в сфере отношений, которые не в полной мере урегулированы позитивным правом.

В юридической литературе отмечается, что в современных условиях развития информационных технологий происходят изменения в тактических и операционных сферах военного дела, а как следствие, меняется и облик вооруженного конфликта [1; 4]. Современные вооруженные конфликты, более известные как гибридные войны, охватывают не только традиционные формы применения вооруженной силы (авиация, флот, сухопутные силы, разведка, тыловое обеспечение, космические войска, блокада портов и городов), но и нетипичные для вооруженного конфликта методы, формы, практики и средства противоборства (например, терроризм, организованная преступность, пропаганда в информационной сфере, «цветные революции», наемничество, теневая экономика, политическая дестабилизация в обществе и др.) [3]. В свою очередь, развитие и активное применение информационных технологий приводит к появлению нового театра политического и военного противостояния — киберпространства, в котором также могут совершаться действия, порождающие реальные последствия в физическом мире [9].

Кибероперации можно понимать как операции против или через компьютер или компьютерную систему, через поток данных, с помощью вирусов, червей, вредоносных программ и т. д., приводящие к причинению материального вреда физическим или юридическим лицам, а также конкретным объектам. При этом причиненный вред должен выходить за рамки компьютерной программы или атакуемых данных, а последствия должны оцениваться как значительные и соотносимые с последствиями, которые могут наступить от применения запрещенных средств и методов ведения войны. Примером такого нападения можно считать враждебное применение ИКТ, приводящее к открытию шлюза плотины, что приводит к гибели людей, затоплению района, нарушению работы транспортной инфраструктуры и выводу из строя систем жизнеобеспечения целых населенных пунктов [8].

Кроме того, если в практике международных отношений допускается расширение понятия «применение вооруженной силы» за счет включения в него различных видов оружия массового поражения (биологического, химического, радиологического), которые, как правило, действуют неочевидным и неизбирательным образом, но способны порождать серьезные негативные последствия для разных сфер жизни общества, то возникает закономерный вопрос о причинах, препятствующих признанию ИКТ, используемых в агрессивных целях в условиях вооруженного конфликта, в качестве кибероружия и кибератак, запрещенных международным гуманитарным правом.

Не без интереса будет отметить, что возможное признание кибероружия и связанных с ним кибератак в качестве противоправного применения вооруженной силы одним государством против другого также может вытекать из расширенного толкования резолюции Генеральной Ассамблеи ООН 3314 (XXIX) от 14 декабря

1974 года «Определение агрессии» [2]. В ст. 3 данного документа закреплена перечень типичных для практики международных отношений и истории вооруженных конфликтов актов применения силы, которые, независимо от объявления войны, с учетом и в соответствии с положениями статьи 2, могут быть квалифицированы в качестве акта агрессии. Однако уже в ст. 4 рассматриваемой резолюции говорится, что указанный перечень актов не является исчерпывающим и Совет Безопасности ООН может определить, что и другие акты также могут представлять собой агрессию согласно положениям Устава ООН. Несмотря на то, что сама резолюция является информационно-декларативным документом для Совета Безопасности ООН и что в истории пока нет примеров признания Советом Безопасности ООН кибератак в качестве акта агрессии или противоправного применения вооруженной силы против другого государства, определяемого как угроза миру, представляется возможным сделать допущение о возможном признании кибератак в качестве нетипичного акта применения вооруженной силы в случае, если в результате такой атаки будет нарушен международный мир (возникнет открытое вооруженное противостояние между государствами) или произойдет осложнение международных отношений до состояния, определяемого как угроза миру.

#### **Заключение и выводы**

Безусловно, нельзя игнорировать тот факт, что современные информационно-коммуникационные технологии вносят свой вклад не только в развитие социальных отношений, но также приводят к трансформации определенных социокультурных явлений, имеющих отрицательное значение. К таким явлениям, помимо прочего, относится и политическое насилие между государствами, более известное как межгосударственный вооруженный конфликт.

Современное международное гуманитарное право в контексте своего исторического развития охватывает прежде всего отношения, связанные с традиционным применением вооруженных сил в условиях вооруженного конфликта. Сплошной анализ положений международного гуманитарного и уголовного права (жневские конвенции 1949 г. и дополнительные протоколы к ним, а также Римский статут МУС) не позволяет установить юридическую возможность признания применения кибероружия (кибератак) в качестве военных преступлений. В то же время не следует забывать, что международное гуманитарное право — это не только нормы, отраженные в системе договорного регулирования, но и обычаи, сложившиеся в межгосударственной практике и ставшие в дальнейшем, в силу широкого признания, нормами общего характера (*opinio juris*). В этой связи следует согласиться с позицией, неоднократно высказываемой в юридической науке, что военные операции в современных условиях представляют собой не только кинетическое, но также и кибернетическое воздействие на объекты

соответствующего противника в вооружённом конфликте. Соответственно, к таким операциям должны применяться одни и те же нормы и принципы, включая принципы гуманности, военной необходимости, проведения различия, соразмерности и принятия мер предосторожности.

#### Список источников

1. Белоус А. И. Кибероружие и кибербезопасность. О сложных вещах простыми словами: монография / А. И. Белоус, В. А. Солодуха. Москва, 2020. 692 с.
2. Дзейтова Р. Б. Ответственность за киберагрессию по международному уголовному праву: основание и условия наступления // Вестник Московского университета. Серия 11. Право. 2021. № 6. С. 89–101.
3. Калдор М. Новые и старые войны: организованное насилие в глобальную эпоху / пер. с англ. А. Апполонова, М. Дондуковского; ред. перевода А. Смирнов, В. Софронов. Москва, 2015. 416 с.
4. Старкин С. В. Кибербезопасность и киберреволюция: критический анализ базовых концептов // Вестник московского университета. Серия 12. Политические науки. 2015. № 1. С. 35–53.
5. Clarke R. A., Knake R. K. Cyber War. New York: HarperCollins, 2010. 194 p.
6. Ophardt J. A. Cyber warfare and the crime of aggression: the need for individual accountability on tomorrow's battlefield // Duke Law & Technology Review. 2010. No. 3. URL: <https://scholarship.law.duke.edu/dltr/vol9/iss1/2/>
7. Hathaway O., Crootof R., Levitz Ph. Nix H., Nowlan A., Perdue W. & Spiegel J. The Law of Cyber-Attack // California Law Review. 2012. Vol. 100. P. 817–886.
8. The Rome Statute of the International Criminal Court. A Commentary / Triffterer O., Ambos K. Beck/Hart, 2016. P. 355–356.
9. Gisel L., Rodenha T., Dormann K. Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts // International Review of the Red Cross. 2020. No. 102 (913). P. 287–334.

#### СВЕДЕНИЯ ОБ АВТОРЕ

##### Лобач Дмитрий Владимирович

Кандидат юридических наук, доцент кафедры теории и истории государства и права, Дальневосточный юридический институт (филиал) Университета прокуратуры Российской Федерации  
Россия, 690091, г. Владивосток, ул. Суханова 8  
E-mail: dimaved85@mail.ru  
ORCID: 0000-0002-7229-439X

#### INFORMATION ABOUT THE AUTHOR

##### Dmitry V. Lobach

Candidate of Legal Sciences, Associate Professor of the Department of Theory and History of State and Law, Far Eastern Law Institute (branch), University of the Prosecutor's Office of the Russian Federation  
8 Sukhanova str., Vladivostok 690091, Russia  
E-mail: dimaved85@mail.ru  
ORCID: 0000-0002-7229-439X

#### КОНФЛИКТ ИНТЕРЕСОВ

Конфликт интересов отсутствует.

#### CONFLICT OF INTEREST

There is no conflict of interest.

Дата поступления статьи / Received: 01.10.2025.

Дата рецензирования статьи / Revised: 07.10.2025.

Дата принятия статьи к публикации / Accepted: 15.10.2025.