DOI: https://www.doi.org/10.36719/2663-4619/65/223-227

**Ильгар Имдат оглу Гасанов**
Бакинский государственный университет
магистрант
ilqar-hesenov-9797@mail.ru

# МЕЖДУНАРОДНО-ПРАВОВЫЕ ОСНОВЫ БОРЬБЫ С КИБЕРПРЕСТУПЛЕНИЕМ

***Ключевые слова:*** *киберпрастранство, киберпреступление, международное право, транснациональные преступления, Совета Европы, ООН, Уголовный Кодекс Азербайджанской Республики, уголовная политика*

## International legal framework for combating cybercrime

**Summary**

The article examines the relevance of cybercrime, their types and possible ways of their fulfillment, the peculiarities of cybercrime, as well as the international legal basis for the fight against this evil. Cyberspace crime is one of the most difficult problems that the international community has faced in recent years with the development of information and communication technologies. International coorperation in the fight against cybercrime is carried out in several directions and involves, first of all, the creation of regulations and the development of general recommendations, as well as the implementation of effective models of organizational interaction between states.

***Key words:*** *cyberspace, cybercrime, international law, transnational crimes, Coucil of Europe, UN, Criminal Code of the Republic of Azerbaijan, criminal policy*

Понятие «*киберпреступление*» и «*киберпространство»* в настоящее время используются достаточно широко в связи с произошедшим в XXI в. информационно-телекоммуникационным прорывом и стали неотъемлемой частью всех сфер жизнедеятельности человека и в целом международного сообщества. Согласно данным Отчета ООН по «Состоянию широкополосной связи» за 2015 г., в настоящее время доступ в Интернет имеют порядка 3,2 млрд человек, по сравнению с 2,9 млрд в 2014 г., что составляет порядка 43 % всего мирового населения. А к 2017 году доступ к мобильному широкополосному Интернету получат уже до 70 % от общей численности населения мира. Одновременно с количеством пользователей увеличивается как потенциальных жертв, так и возможность использовать сеть Интернета для совершения противоправных деяний. По этому, сегодня преступность в киберпространстве считается одна из острейших проблем, с которой столкнулось международное сообщество на протяжении последних десятилетий в связи с развитием информационных технологий.

Как заметил международный эксперт по гармонизации законодательства в сфере киберпреступности Штайн Шольберг *(Stein Schjolberg),* «киберпространство, как пятое общее пространство, после наземного, морского, воздушного и космического, требует координации, сотрудничества и особых мер на международном уровне» (14). Это требования связано с тем, что киберпреступления зачастую выходят за пределы одного государства и носят трансграничный или транснациональный характер (12,p.97-108). Особенно проблема усугубляется тем, что решать ее силами одного государства не представляется невозможным. Угроза киберпреступлений и ее глобализация продолжает расти с каждым днем. Так, уже сейчас кибератаки парализуют работу не только частных структур, но и государственных органов, в мире не существует государства, которое было бы защищено от подобного рода атак. В качестве вероятных источников киберугроз рассматриваются не только хакеры или их группы, но также отдельные государства, террористические, преступные группировки.

Надо отметить, что при выработке средств и методов борьбы с киберпреступлениями следует помнить о латентности данного вида преступлений (13,p.10310-10323). Для большинства преступлений, совершаемых в глобальных компьютерных сетях, характерны следующие *особенности*: а) повышенная скрытность совершения преступления, обеспечиваемая спецификой сетевого информационного пространства (развитые механизмы анонимности, сложность инфраструктуры и т.п.); б) трансграничный характер сетевых преступлений; в) особая подготовленность преступников и интеллектуальный характер преступной деятельности; г) нестандартность, сложность, многообразие и частое обновление способов совершения преступлений и применяемых специальных средств; д) возможность совершения преступления в автоматизированном режиме в нескольких местах одновременно, возможность объединять относительно слабые ресурсы многих отдельных компьютеров в мощное орудие совершения преступления; е) многоэпизодный характер преступных действий при множественности потерпевших; ж) неосведомленность

потерпевших о том, что они подверглись преступному воздействию; дистанционный характер преступных действий в условиях отсутствия физического контакта преступника и потерпевшего; з) невозможность предотвращения и пресечения преступлений данного вида традиционными средствами (10,с.109–110). В настоящее время не существует ни релевантной статистики, отражающей реальную картину состояния киберпреступности, ни надежных методов сбора таких данных. И дело не только в отсутствии единообразия национального уголовного законодательства стран в сфере борьбы с киберпреступностью и разной практике его применения, различиях в формировании уголовной статистики и особенностях правоохранительной системы. До сих пор неясно, до какой степени достоверна статистика об экономических потерях от киберпреступности (5,с.69).

Международное сотрудничество в области борьбы с киберпреступлениями осуществляется по нескольким направлениям и предполагает прежде всего создание нормативных актов и выработку общих рекомендаций, а также внедрение эффективных моделей организационного взаимодействия между государствами. При этом следует учитывать, что традиционные механизмы международного сотрудничества, включая запросы, взаимопомощь и другие подобные инструменты, применявшиеся в XX в. и ранее, являются неподходящими в эру, когда преступления могут совершаться из любой точки земного шара со скоростью света (15,p.60). Правовое регулирование вопросов борьбы с киберпреступлениями представляет собой базис всей системы противодействия (универсальный, региональный, субрегиональный и национальный) киберпреступности. Сложность выработки международных актов в целом в рассматриваемой ситуации осложняется еще и тем, что «существующие законы трудно применять, когда речь идет о не поддающихся локализации атаках в планетарных масштабах, доказательства которых разбросаны и виртуальны» (6, с. 144).

Несмотря на этого, международное сообщество на различных уровнях выработало ряд актов, имеющих значение для борьбы с киберпреступностью, при чем особую роль играют региональные акты, поскольку общемировой документ в настоящее время создать затруднительно. Вместе с тем нельзя не отметить попытки государств распространить нормы глобальных международных договоров на борьбу с киберпреступностью или заключить новые договоры. Например, так как в киберпространстве наряду с отдельными лицами могут действовать и организованные преступные группы, существует возможность применения к ним международных договоров, направленных на борьбу с организованной преступностью, в частности Конвенции ООН против транснациональной организованной преступности от 15 ноября 2000 г. Потому, что сегодня киберпреступление приобрела транснациональный характер и создает опасность для стабильности государств.

Правовую основу борьбы с киберпреступлениями образуют следующее международные нормативно-правовые акты, о том числе мягкие правовые нормы – *soft law*, такие как Конвенция ООН против транснациональной организованной преступности 2000 г., Окинавская Хартия глобального информационного общества, принятая 22 июля 2000 г. лидерами стран Большой восьмерки, Женевская Декларация принципов «Построение информационного общества - глобальная задача в новом тысячелетии», принятая в 2003 г., Тунисская программа для информационного общества, принятая в 2005 г., Программа Информация для всех (Information for All Programme), принятая в 2001 г. ЮНЕСКО, Руководство Международного союза электросвязи (ITV): «Понимание киберпреступности: Руководство для развивающихся стран»; среди региональных правовых инструментов можно выделить следующие конвенции Совета Европы: Конвенция о борьбе с киберпреступлениями 2001 г., О взаимной правовой помощи по уголовным делам в том, что касается судебных поручений о перехвате телекоммуникационных сообщений, О борьбе с пиратством в области авторского права и смежных прав, О порядке использования персональных данных полицией», О защите персональных данных в сфере телекоммуникационных услуг, в особенности телефонных услуг, О преступлениях, связанных с компьютерами», По проблемам уголовно-процессуального права, связанным с информационными технологиями»; Бангкокская декларация; в рамках Европейского Союза - Создание безопасного информационного общества посредством повышения защищенности информационной инфраструктуры и борьбы с преступлениями с использованием компьютерных средств» принятая 2001 г.; в рамках СНГ действует Соглашение о сотрудничестве государств-участников СНГ в борьбе с преступлениями в сфере компьютерной информации 2001 г.; на универсальном основе - концепция Конвенции ООН об обеспечении международной информационной безопасности 2011 г., и другие акты в которой отражены основные направления межгосударственного сотрудничества в данной сфере.

Обеспечения международной информационной безопасности в современном мире является один из актуальных, сложных проблем, которые решения этого вопроса непосредственно зависит от уровня сотрудничества государств. Потому, что информационное пространство по своей природе транснацио-

нально, информационные вызовы и угрозы не ограничиваются пределами отдельных государств. Для обеспечения международной информационной безопасности необходимо сотрудничество, опирающееся на нормы международного права при учете особенностей цифровой среды (7,с.45). Связи с решением этого проблема на универсальном уровне был принят концепция Конвенции ООН об обеспечении международной информационной безопасности 2011 г (8).

Конвенции ООН об обеспечении международной информационной безопасности, которая была представлена международному сообществу в ноябре 2011 г. на конференции по киберпространству в Лондоне и включает преамбулу, 23 статьи, объединенные в основную часть, и заключительные положения. Основная часть документа состоит из пяти глав, содержание которых находится в единой композиционной целостности. Немаловажно, что в ст. 4 Конвенции закреплены основные угрозы международному миру и безопасности в информационном пространстве, из которых выделено 11 базовых и 4 дополнительных.

Среди базовых названы, например, использование информационных технологий и средств для осуществления враждебных действий и актов агрессии; целенаправленное деструктивное воздействие в информационном пространстве на критически важные структуры другого государства; трансграничное распространение информации, противоречащей принципам и нормам международного права, а также национальным законодательствам государств.

В документе не указаны такие реальные угрозы международной безопасности, как совершение киберпреступлений, распространение наркотических и психотропных средств, их аналогов, а также порнографии, в том числе и детской.

Помимо этого, концепция Конвенции 2011 года содержит ст. 5, посвященную основным принципам обеспечения международной информационной безопасности, таких как (их можно разделить на четыре группы) принципы участия государства в системе международной информационной безопасности как члена международного сообщества; принципы, позволяющие государству сохранить свой суверенитет в процессе международного сотрудничества в борьбе с киберпреступностью; принципы обеспечения свободного информационного обмена между странами. Четвертая группа принципов устанавливает характер взаимодействия государства и частных субъектов в рассматриваемых отношениях. Несмотря на это, в концепции Конвенции детально не прописаны принципы международного сотрудничества в борьбе с киберпреступлениями, кроме направленного против действий террористического характера.

Таким образом, положения концепции Конвенции ООН об обеспечении международной информационной безопасности носят достаточно компромиссный характер и ориентированы прежде всего на предупреждение информационных войн, терроризма (11,с. 373).

Нельзя оставить без внимания, представленное в 2013 г. Таллиннское руководство по международному праву, применимому в случае кибервойны (*Tallinn Manual on The International Law Applicableto Cyber Warfare*). Структурно Таллиннское руководство состоит из двух основных частей, закрепляющих 95 правил по ведению кибервойны: 1) часть А – «Международное право кибербезопасности» (International Cyber Security Law), включающая в себе две главы и 19 правил, регламентирующие права сторон конфликта на ведение кибервойны (*jus ad bellum*); 2) часть В – «Право киберконфликтов» (*The Law of Cyberarmed Conflict*), состоящая из 5 глав и 76 правил, регулирующие поведение сторон в ходе кибервойны (*jus in bellum*) (16). Цель Таллиннского руководства – оценить нормативную и правовую базу в области информационной безопасности и проанализировать их эффективность в современных условиях. Руководство содержит важное положение: каждое государство обязано понимать и осознавать результаты разработки, внедрения и применения новых видов вооружения, включая кибероружия, в рамках международного гуманитарного права.

Как отмечает исследователь М.Б.Касенов, «Таллиннское руководство следует рассматривать именно в контексте «стремления к нормативной определенности» применимости нормы современного международного права к «киберугрозам» (9,с.117). Тем не менее, руководство не дает четко определенного толкования киберпреступления, также как и на международном уровне.

Первым международно-правовым актом, предусматривающим межгосударственное сотрудничество в борьбе с киберпреступлениями, является Конвенция Совета Европы о борьбе с киберпреступлениями, принятая в 2001 году. Хотя Конвенция является региональным соглашением по территориальным критериям, несмотря на этого она приобрела принцип субрегионального действия. Это связано с тем, что настоящее время не существует международного соглашения, регулирующего универсальные основы борьбы с киберпреступлениями. Конвенция вступила в силу в 2004 г., ее подписали более 40 государств - членов Совета Европы, а также государства, не входящие в Совет Европы, такие как США, Канада, Япония, ЮАР и другие государств, которые сильно страдает от киберпреступности. Азербайджанская Республика присоединилась к этой Конвенции в 2009 г., и взял на себя соответствующие обязательства.

Статистические данные показывает, что одной из стран, наиболее пострадавших от киберпреступности, является Российская Федерация. Тем не менее Россия не участвует в данной Конвенции. По мнению противников присоединения России к Конвенции, ст. 32 Конвенции противоречит российскому законодательству и нарушает суверенитет государства, так как предусмотренные в ней действия могут совершаться без предварительного уведомления и согласия стороны, на территории которой эти действия совершаются. Кроме того, в УК РФ отсутствуют нормы, устанавливающие уголовную ответственность юридических лиц за преступления в сфере компьютерной информации (3, с. 27).

В преамбуле к Конвенции Совета Европы государства-участники обозначили *цель* ее принятия: выработка в приоритетном порядке общей политики в сфере уголовного права, ориентированной на защиту общества от киберпреступление, в том числе посредством принятия соответствующих законодательных актов и укрепления международного сотрудничества; сдерживание действий, направленных против конфиденциальности, целостности и доступности компьютерных систем и сетей и компьютерной информации, а также против злоупотребления такими системами, сетями и информацией, путем обеспечения уголовной наказуемости таких деяний и предоставления полномочий, достаточных для эффективной борьбы с данными уголовными преступлениями, путем содействия выявлению и расследованию таких уголовных преступлений и судебному преследованию за их совершение как на внутригосударственном, так и на международном уровне и путем разработки договоренностей относительно оперативного и надежного международного сотрудничества (4).

Профессор А.Г.Волеводз высоко оценить роль Конвенции 2001 г, в борьбе с киберпреступлениями и потом автор отмечает, что Конвенция Совета Европы представляет собой комплексный документ, содержащий нормы, призванные оказать существенное влияние на различные отрасли права: уголовное, уголовно-процессуальное, авторское, гражданское, информационное. Она базируется на основных принципах международного права: уважения прав человека, сотрудничества и добросовестного выполнения обязательств. Нормы Конвенции направлены на регулирование трех основных блоков вопросов: **1)** сближение уголовно-правовой оценки преступлений в сфере компьютерной информации; **2)** сближение национальных уголовно-процессуальных мер, направленных на обеспечение собирания доказательств при расследовании таких преступлений; **3)** международное сотрудничество в уголовно-процессуальной деятельности, направленной на собирание доказательств совершения таких преступлений за рубежом (1,с.17-18).

В Конвенции 2001 года *киберпреступления* классифицируются следующим образом:

**1**) преступления против конфиденциальности, целостности и доступности компьютерных данных и систем (offences against the confi dentiality, integrity and availability of computer data and systems): противозаконный доступ (illegal access); неправомерный перехват (illegal interception); воздействие на данные (data interference); воздействие на функционирование системы (system interference); противозаконное использование устройств (misuse of devices);

**2**) правонарушения, связанные с использованием компьютерных средств (computer-related offences): подлог с использованием компьютерных технологий (computerrelated forgery); мошенничество с использованием компьютерных технологий (computerrelated fraud);

**3**) преступления, связанные с содержанием данных (content-related offences) - преступления, связанные с детской порнографией (offences related to child pornography);

**4**) правонарушения, связанные с нарушением авторского права и смежных прав (offences related to infringements of copyright and related rights).

Дополнительный протокол к Конвенции о киберпреступности (2) включает в указанный перечень следующие виды преступлений:

**1**) распространение расистских и ксенофобских материалов посредством компьютерных систем (dissemination of racist and xenophobic material through computer systems);

**2**) мотивированная угроза расизма и ксенофобии (racist and xenophobic motivated threat);

**3**) расистское и ксенофобское мотивированное оскорбление (racist and xenophobic motivated insult);

**4**) отрицание, чрезвычайная минимизация, одобрение или оправдание геноцида или преступлений против человечности (denial, gross minimisation, approval or justifi cation of genocide or crimes against humanity).

Таким образом, можно сделать следующие выводы.

1) Международное сотрудничество в борьбе с киберпреступлением осложняется особенностями данного вида преступности. Для оптимизации борьбы с киберпреступлением необходимо в первую очередь участие всех государств, поскольку киберпреступления имеет транснациональный характер.

2) Угроза киберпреступлений и ее глобализация продолжает расти с каждым днем. По этому сегодня преступность в киберпространстве считается одна из острейших проблем, с которой столкнулось международное сообщество на протяжении последних десятилетий в связи с развитием информационных технологий.

3) Правовое регулирование вопросов борьбы с киберпреступлениями представляет собой базис всей системы противодействия киберпреступности (универсальный, региональный, субрегиональный и национальный) киберпреступности.

4) Конвенция Совета Европы о борьбе с киберпреступлениями является единственным признанным международным договором которые содержит нормы материального и процессуального права в целях противодействия киберпреступности и защиты свободы, безопасности и прав человека в Интернете и других социальных сетях. Тем не менее, Конвенция не гарантирует полностью безопасность виртуального пространства.

5) Данная Конвенция весьма значима не только в рамках Совета Европы, но и на глобальном уровне (до сих пор единого универсального акта, регламентирующего порядок противодействия киберпреступлениям, не выработано). Она является одним из основополагающих документов в сфере противодействия киберпреступности. Конвенцию подписали не только страны Европы, но также США, Аргентина, Австралия, Израиль, Япония, Южная Корея, в общей сложности более 50 государств.

## References

1. Volevodz AG Convention on Cybersecurity: innovations in legal regulation // Legal issues of communication. № 2. 2007, p. 17-25
2. Additional Protocol to the Convention on Cybercrime in relation to the criminalization of racist and xenophobic acts, carried out with the assistance of computer systems (signed in Strasbourg on January 28, 2003). URL: http://mvd.gov.by/ mainaspx? Guid = 4593
3. Evdokimov KN Current issues of crime prevention in the field of computer information in the Russian Federation // Academic Juridical Journal. № 1 (59). 2015, p. 21–31
4. European Convention on Cybercrime: concluded in Budapest on 23 November. 2001 URL: http: //conventions.coe. int / Treaty / RUS / Treaties / Html / 185.htm
5. Zhuravlenko NI, Shvedova LE Problems of struggle with cybersecurity and perspective directions of international cooperation in this sphere // Society and Law. № 3 (53), 2015, p. 66-70
6. Zhilina I.Yu. Cybersecurity and struggle with it // Social and humanitarian sciences. Domestic and foreign literature. Series 2, Economics: abstract journal. № 1.2003, p. 144–148
7. Zinovyeva E. International cooperation in the field of information security // Law and Management. XXI century. №4 (33). 2014, pp.44-52
8. Convention on the Provision of International Information Security (Concept). URL: http: // www.scrf.gov.ru/documents/6/112.html.
9. Kasenov MB International cooperation and management of the use of the Internet. Documents and materials. SPb .: Gerda, 2013
10. Osipenko AL Network computer crime. Theory and practice of wrestling. Omsk, 2009
11. Yakimova EM, Narutto S.V. International cooperation in the fight against cyber-ambiguity // Criminological Journal of Baikal State University of Economics and Law. T. 10, № 2. 2016, p. 369-378
12. Podgor E.S. Cybercrime: National, Transnational, or International? // 50 Wayne Law Review. 97. 2004, p.97-108
13. Quisumbing L.A. Global Perspectives on Cyber security Using Latent Dirichlet Allocation Algorithm // International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 20. 2017 / p. 10310-10323
14. Schjolberg S.A cyberspace treaty: A United Nations convention or protocol on cybersecurity and cybercrime / Stein Schjolberg // Twelfth United Nations Congress on Crime Prevention and Criminal Justice. Salvador, Brazil, 12–19 April 2010. Mode of access: http://cybercrimelaw.net/documents/UN_ 12th_Crime_Congress.pdf.
15. Smith R.G. Criminals on Trial / R.G.Smith, P.Grabosky, G.Urbas. Cambridge. Cambridge University Press, 2004
16. The Tallinn administration on the international law applicable in the case of cyberwar (Tallinn Manual on The International Law Applicable to Cyber Warfare). of URL: http: // www. Cambridge.org/ 97811- 07024434

**Рецензент: доц.Р.Мамедов**

Göndərilib: 12.04.2021 Qəbul edilib: 13.04.2021