С.Г. Тимошков

Кибератака как современная форма совершения акта агрессии

На современном этапе кибератаку следует квалифицировать не только как преступление против информационных ресурсов, но и как современную форму совершения акта агрессии. Осуществляя подобный вид атаки, может быть похищена информация, составляющая государственную тайну, нарушена система жизнеобеспечения государства, а также может быть совершена в том числе и такая серьезнейшая диверсия, как уничтожение системы противоракетной обороны, что представляет собой угрозу для безопасности государства и является нарушением общепризнанных принципов международного права. Установление виновных лиц за совершение подобных атак является проблематичным. Однако необходимо дальнейшее развитие существующей нормативной базы в данной сфере для разработки международных актов, закрепляющих нормы ответственности за это преступление.

Ключевые слова: кибератака, агрессия, международное преступление, суверенитет государств, Устав ООН, Таллиннское руководство.

На современном этапе для совершения такого тяжкого международного преступления, как агрессия, существуют различные виды вооружений, начиная с огнестрельного, заканчивая ядерным оружием. Однако необходимо также рассматривать такой вид атаки, в результате которого может быть нарушена система жизнеобеспечения целого государства и даже подорвана работа системы противоракетной обороны, что является нарушением государственного суверенитета и актом агрессии. Данным видом атаки является кибератака.

В Уголовном кодексе Российской Федерации киберпреступность рассматривается как преступление, совершенное с целью

© Тимошков С.Г., 2017

уничтожения, блокирования, модификации либо копирования компьютерной информации[1]. Однако в кодексе не учитывается тот факт, что данное преступление может быть совершено с территории другого государства для подрыва компьютерной системы безопасности нашего государства, что необходимо квалифицировать как акт агрессии, за который должны нести индивидуальную ответственность отдельные физические лица.

Как указывает в своей научной работе французский автор Д. Вентре, «кибератака является современной формой агрессии, совершаемой отдельными лицами, либо целой группой лиц, целью которой является подрыв информационной системы безопасности, подрыв работы какой-либо инфраструктуры, компьютерной сети и/или подрыв работы персональных компьютеров и других приспособлений, произведенный любыми способами. Кибератаки совершаются злоумышленниками анонимно, что не освобождает лиц, совершивших ее, от ответственности; кибератаки являются нелегальным проникновением в чужую компьютерную систему, что может послужить причиной подрыва национальной системы безопасности. В хакерской атаке (кибератаке) могут принимать участие один или несколько высококлассных специалистов (хакеров)»[2]. Соответственно проблематично определение круга лиц, виновных в данном преступлении.

Кибератаки бывают разных видов, но все они представляют собой большую угрозу. Одним из распространенных видов является кибершпионаж. В своей научной работе профессор Бреннер отмечает, что под кибершпионажем следует квалифицировать деятельность, направленную на получение секретной служебной информации из личных данных индивидуальных лиц, групп, или взлом системы правительственной службы в военных целях, экономических или политических, используя незаконные методы эксплуатации Интернета, компьютерных сетей или программного обеспечения[3]. В результате подобной кибератаки секретная информация, ненадежно обработанная, может быть перехвачена и даже изменена, что делает осуществимым кибершпионаж из любой точки мира. Данная секретная информация, попав в руки потенциального агрессора, может быть использована в противоправной деятельности против других государств, подорвав их государственный и общественный строй, что является непосредственным проявлением агрессии и нарушением международных принципов права. Следует также отметить, что в недавнем времени органами Федеральной службы безопасности Российской Федерации была выявлена попытка совершения кибершпионажа

в целях «заражения» информационных ресурсов государственных органов власти и управления, научных и военных учреждений, предприятий оборонно-промышленного комплекса и иных объектов критически важных частей инфраструктуры страны.

Другим видом кибератаки, представляющим еще большую угрозу для государства, является саботаж – подрыв работы компьютерной системы или систем спутников, выполняющих задачи по поддержанию национальной безопасности государств[4]. В случае совершения киберсаботажа угрозе могут быть подвергнуты спутниковые и компьютерные системы безопасности и жизнеобеспечения целого государства: электростанции, система водоснабжения, топливная система, транспортная инфраструктура – все может быть подвергнуто риску. Профессор Бреннер отмечает, что гражданская сфера также находится под угрозой, поскольку преступная деятельность по подрыву систем безопасности уже вышла за рамки простого воровства номеров кредитных карт, и потенциальной целью могут также стать электрические сети, поезда или фондовый рынок. Кроме гражданской сферы, может быть осуществлен подрыв работы системы обеспечения деятельности Вооруженных сил, чтобы повлечет за собой «обезоруживание» целого государства[5].

Международно-правовая деятельность, направленная на борьбу с кибератаками, имеет множество преград из-за недостаточно разработанной законодательной базы в данной области. Следует отметить, что не существует универсального общепринятого международного акта в области кибербезопасности, и многие юристы-международники считают, что необходимо срочно принять международный договор в сфере борьбы с кибератаками[6]. Они полагают, что международное сообщество должно рассматривать вопрос о кибербезопасности как один из основных, так как это является глобальной угрозой для всего международного сообщества[7].

Например, в своей статье И.М. Рассолов отмечает, что «среди множества проблем судебной практики по этим делам можно выделить две ключевые: 1) сложность определения круга лиц, привлекаемых к юридической ответственности...; 2) фиксация (собирание, представление) доказательств, их допустимость и достоверность»[8].

Главной проблемой в сфере выработки единого акта о запрещении кибератак является тот факт, что независимо от вида атаки почти никогда нельзя точно выяснить, кто именно выступает организатором данной атаки: хакеры-одиночки, организованные хакерские группы либо государственные структуры. Как пишет профессор Томас Рид: «Разносторонний характер кибератак означает, что трудно определить мотивацию нападающей стороны,

а это означает, что неясно, когда конкретный акт следует рассматривать как акт агрессии»[9].

Однако необходимо отметить, что в данной сфере произошел положительный сдвиг. В 2015 г. Группа правительственных экспертов ООН подготовила Доклад о международной информационной безопасности, в котором говорится о договоренности 20 крупнейших мировых держав, в том числе России, США и Китая, использовать кибертехнологии в мирных целях и не атаковать объекты критически важной инфраструктуры[10].

При этом страны обязуются противостоять попыткам хакеров вести незаконную деятельность против других государств с их территории. Все указанные в Докладе договоренности носят рекомендательный характер, и он был предоставлен на рассмотрение Генеральному секретарю ООН Пан Ги Муну и на обсуждение в Генеральную Ассамблею ООН[11].

Стоит отметить, что данный итоговый Доклад является одним из важнейших политико-правовых актов на современном этапе, устанавливающим универсальные рамки для взаимных действий государств в киберпространстве. В нем подтверждается общая заинтересованность государств в мирном применении «информационно-коммуникационных технологий»[12] и необходимость в усилении действий международного сообщества, направленных на предотвращение конфликтов в киберпространстве. Также группа утвердила суверенное право государств распоряжаться информационно-коммуникационными технологиями на своей территории и определять свою политику в сфере международной информационной безопасности[13].

Следует отметить, что Доклад 2015 г. развивает положения докладов Группы правительственных экспертов за 2010 и 2013 гг., закрепивших суверенное право государств на мирное использование компьютерных технологий и верховенство Устава ООН в разрешении конфликтов, связанных с данной сферой. Следует отметить, что нововведением Доклада 2015 г. является положение о том, что обвинение в планировании и осуществлении кибератак не должно быть беспочвенным[14]. Таким образом, ни одно государство не имеет права обвинять другое государство в совершении кибератак без имеющихся на то неопровержимых доказательств.

Следующим важным моментом является то, что данным Докладом признаются нормы международного права, применимые к сфере использования информационно-коммуникационных технологий, но при этом эти нормы могут быть развиты за счет принятия новых принципов и соответствующих норм. Стоит отметить, что

в Докладе отведено особое внимание вопросу разработки норм, правил и принципов, устанавливающих ответственность государств в киберпространстве[15]. Также важным моментом является пункт Доклада, который посвящен инициативе Шанхайской организации сотрудничества (ШОС). Данная инициатива касается «Правил поведения в области обеспечения международной информационной безопасности», обновленный проект которых был направлен от имени государств – членов ШОС Генеральному секретарю ООН в январе 2015 г.[16]

Одним из важных итогов работы данной Группы правительственных экспертов стало то, что она инициировала созыв новой группы в 2016 г., которой необходимо будет продолжить работу в целях выработки правовых норм по определению существующих и потенциальных угроз в сфере информационной безопасности и возможных совместных мер по их устранению. Также в документ включены основные рекомендации по наращиванию международного сотрудничества в области международной информационной безопасности, отмечена значимость мер укрепления доверия, преодоления «цифрового разрыва». Предусматривается изучение способов увеличения объемов технической помощи, возможностей по реагированию на инциденты, связанные с использованием информационно-коммуникационных технологий, ускорение передачи соответствующих знаний и технологий прежде всего развивающимся странам[17].

Таким образом, несмотря на то что доклад Группы правительственных экспертов ООН по международной информационной безопасности носит рекомендательный характер, он имеет огромное значение по становлению современных норм, которые в перспективе будут закреплены в международном акте, направленном на предотвращение кибератак как современной формы совершения акта агрессии.

В том числе в недавнем времени стало известно, что Россия под эгидой ООН подпишет пакт об электронном ненападении. Об этом было сделано заявление начальником Восьмого управления Генерального штаба Вооруженных сил Российской Федерации Юрием Кузнецовым. По его словам, этот пакт предусматривает запрет на кибератаки на информационные ресурсы других стран в мирное время[18]. Этим фактом следует отметить, что наше государство вносит огромный вклад в развитие норм международного права в сфере ответственности за кибератаки и тем самым выполняет ряд задач по поддержанию международного мира и безопасности, которая закреплена Уставом ООН.

Восьмое управление Генерального штаба Вооруженных сил Российской Федерации отвечает за режим секретности в воинских частях и соединениях, скрытое управление войсками и оружием, защиту информации от несанкционированного доступа, работу систем сертификации средств защиты информации и работу с информацией, составляющей государственную тайну[19].

Необходимо также отметить, что одним из важнейших международных актов, направленных на развитие норм по предотвращению кибератак, является Таллиннское руководство по ведению кибервойн.

Полное название данного международного акта – «Таллиннское руководство по международному праву, применимое к кибервойне»[20]. Этот документ носит академический, но не образовательный характер и включает в себя нормы международного права, нормы права вооруженных конфликтов и международного гуманитарного права касательно кибератак и кибервойн.

Таллиннское руководство по ведению кибервойн было подготовлено группой, состоящей из двадцати специалистов по международному праву на базе НАТО в Таллинне в Центре передового опыта по кибероборонe в период с 2009 по 2012 г. Данной группе было поручено разработать руководство по решению проблем, связанных с трактовкой норм международного права в контексте кибероперaций и кибервойн. Это руководство стало первой попыткой исчерпывающе проанализировать тему кибервойн, ссылаясь при этом на авторитетное мнение юристов-международников для того чтобы внести некоторую ясность по разрешению подобных конфликтов в соответствии с нормами международного права[21].

Авторами Таллиннского руководства являются весьма уважаемые ученые-юристы и юристы-практики с опытом работы, касающейся кибервойн, с которыми проводили консультации специалисты в области информационных технологий на протяжении всего проекта. Эту группу юристов-международников возглавлял профессор Майкл Н. Шмидт, заведующий кафедрой международного права Военно-морского колледжа в городе Ньюпорт, США, также являясь при этом руководителем данного проекта. Членами группы были профессор Вольф Хайнтшель фон Хайнегг из Европейского университета Виадрина, командор авиации (в отставке) Уильям Бутби из королевских ВВС Великобритании, профессор Томас С. Вингфилд из Европейского центра по изучению вопросов безопасности имени Джорджа С. Маршалла и другие юристы-международники. Также при составлении данного руководства роль наблюдателей выполняли представители Центра

передового опыта по кибероборонe, представители Международного комитета Красного Креста как организации, ответственной за выполнение норм международного гуманитарного права, а также представители командования США по кибербезопасности как сторонние специалисты в данной сфере[22].

Однако важно отметить тот факт, что данное руководство не следует характеризовать исключительно как руководство для стран НАТО. Таллиннское руководство является результатом работы независимой группы ученых-юристов и юристов-практиков. Оно представляет собой субъективное мнение его авторов относительно проблематики кибератак. В своей работе Гарольд Кох делает акцент на том, что руководство не отражает взгляды ни стран НАТО, ни любой другой организации или государства, несмотря на их представительство в качестве наблюдателей. Будучи первым авторитетным изложением применения и толкования норм международного права в контексте предотвращения кибератак, можно ожидать, что данное руководство будет оказывать влияние на то, как государства и организации будут разрабатывать свои подходы и позиции по разрешению данного вопроса[23].

В данном руководстве сказано: «Важно отметить, что данный документ не является руководством по вопросам “кибербезопасности”, исходя из общего понимания данного термина. Кибершпионаж, кража интеллектуальной собственности и другие виды киберпреступлений представляют собой серьезную угрозу для всех государств, в том числе и для корпораций, и для частных лиц. Адекватные меры по противодействию подобным видам преступлений должны быть предприняты и на национальном уровне, и на международном. Соответственно данное Руководство не содержит прямых указаний, которые должны быть выполнены в целях предотвращения киберпреступлений, лишь рекомендации по развитию норм международного права, поскольку существующие нормы по разрешению конфликтов в реальном мире не могут быть применимы для разрешения конфликтов в киберпространстве»[24].

Следует отметить, что Таллиннское руководство основывается на научной работе Международного института гуманитарного права, являющегося независимой, непрофильной гуманитарной организацией. Его основной целью является содействие в развитии норм международного гуманитарного права, норм прав человека, прав беженцев и смежных вопросов. Данной научной работой этого Института является руководство по международному праву, применимое к вооруженным конфликтам на море, разработанное в городе Сан-Ремо в 1994 году. Также Таллиннское руководство

опирается на положения, закрепленные исследовательской программой по международному праву университета Гарварда в сфере гуманитарной политики и конфликтов в результате воздушных и ракетных войн[25].

Важно также отметить, что в 2016 г. было принято дополнение к Таллиннскому руководству «Таллинн 2.0». Оно расширило область применения оригинального руководства. Первое Таллиннское руководство сфокусировано на самых разрушительных и деструктивных последствиях кибератак. Подобные атаки необходимо квалифицировать как вооруженное нападение, и, следовательно, это позволит государствам предпринимать меры по самообороне, как при вооруженном конфликте. Поскольку угроза кибератак с такими последствиями вызывает особую тревогу государств, большинство научных исследований сосредоточено именно на этих проблемах[26].

Ввиду высокой степени угрозы для безопасности государств, которую представляет собой кибератака, сравнимой по уровню последствий с вооруженным нападением, в Таллиннском руководстве второй версии рассматриваются нормы международного права, применимые к подобным кибероперациям, а также условия, при которых будут применяться общие принципы международного права, такие как суверенитет, юрисдикция и запрет на вмешательство во внутренние дела государства в контексте кибербезопасности[27].

Таким образом, следует сделать вывод о том, что кибератака представляет собой явную угрозу не только для отдельных компьютерных сетей каких-либо корпораций или частных лиц, но и для компьютерных систем безопасности целого государства и ее необходимо квалифицировать как современную форму совершения акта агрессии, поскольку последствия подобных атак могут быть сравнимы с вооруженным нападением. На данный момент не существует единого международного договора, запрещающего кибератаку. Однако проводится постоянная работа специалистов, ученых-юристов, научная деятельность которых связана с киберпреступностью, разрабатывающих рекомендательные акты, направленные на развитие норм международного права в сфере предотвращения кибератак и установления ответственности за данное преступление. Следует также отметить важную роль РФ, международная деятельность которой направлена на сохранение международного мира и безопасности, в том числе и в киберпространстве.

Примечания

1 Уголовный кодекс Российской Федерации. М.: Омега-Л, 2014. Гл. 28.
2 *Ventre D.* Cyberespace et acteurs du cyber conflict. Hermes-Lavoisier, 2011.
3 *Brenner S.* Cyber Threats: The Emerging Fault Lines of the Nation State. Oxford University Press, 2009.
4 Ibid.
5 *Ventre D.* Op. cit.
6 *Janczewski L., Colarik A.* Cyber Warfare and Cyber Terrorism. Hershey, N.Y.: Information Science Reference, 2008.
7 Ibid.
8 *Рассолов И.М.* Правовые проблемы обеспечения кибербезопасности в России и зарубежных странах // Политика и общество. 2009. № 4 (58). С. 21.
9 *Rid Th.* Cyber War Will Not Take Place // Journal of Strategic Studies. 2011. Issue 6. P. 14.
10 *Owens L.L.* Justice and Warfare in Cyberspace // Boston Review. A Political and Literature Forum. [Электронный ресурс] URL: http://bostonreview.net/us/lisa-lucile-owens-cyber-warfare-national-security (дата обращения: 15.01.2017).
11 Ibid.
12 Ibid.
13 Ibid.
14 Ibid.
15 Ibid.
16 Ibid.
17 Ibid.
18 *Сычев В.* Россия подпишет пакт об электронном ненападении. [Электронный ресурс] URL: https://ria.ru/defense_safety (дата обращения: 12.02.2016).
19 Восьмое управление Генерального штаба Вооруженных сил Российской Федерации. [Электронный ресурс] URL:http://structure.mil.ru/structure/ministry_of_defence (дата обращения: 04.02.2016).
20 http://www.peacepalacelibrary.nl/ebooks
21 *Schmitt M.N.* Tallinn Manual on the International Law Applicable to Cyber Warfare. N.Y.: Cambridge University Press. 2013. [Электронный ресурс] URL: http://www.peacepalacelibrary.nl/ebooks (дата обращения: 23.04.2016).
22 Ibid.
23 *Koh H.H.* International Law in Cyberspace: Remarks of Harold Koh // Harvard International Law Journal, 2012.
24 *Schmitt M.N.* Op. cit.
25 Ibid.
26 *Koh H.H.* Op. cit.
27 Cyber Security Strategy Documents. [Электронный ресурс] URL: https://ccdcoe.org/research.html (дата обращения: 04.02.2016).