Yuridik fanlar axborotnomasi
Вестник юридических наук
Review of Law Sciences

COUNTERACTION TO CYBER TERRORISM: INTERNATIONAL LEGAL AND CRIMINAL LEGAL ASPECTS

A.RASULEV[a]
Academy of the Ministry of Internal Affairs of the Republic of Uzbekistan, Tashkent, 100029, Uzbekistan

ПРОТИВОДЕЙСТВИЕ КИБЕРТЕРРОРИЗМУ: МЕЖДУНАРОДНО-ПРАВОВЫЕ И УГОЛОВНО-ПРАВОВЫЕ АСПЕКТЫ

А.РАСУЛЕВ[a]
Академия Министерства внутренних дел Республики Узбекистан, Ташкент, 100029, Узбекистан

КИБЕРТЕРРОРИЗМГА ҚАРШИ КУРАШИШ: ХАЛҚАРО ҲУҚУҚИЙ ВА ЖИНОЯТ-ҲУҚУҚИЙ ЖИҲАТЛАРИ

А.РАСУЛЕВ[a]
[a]Ўзбекистон Республикаси ИИВ Академияси, Тошкент, 100029, Узбекистан

Аннотация*: в данной статье были проанализированы международные акты и нормы зарубежного уголовного законодательства, предусматривающие вопросы противодействия кибертерроризму.*

Ключевые слова*: кибертерроризм, международные акты, информационные технологии, преступление, ответственность.*

Аннотация*: мазкур мақолада кибертерроризмга қарши курашиш масалаларини назарда тутувчи халқаро ҳужжатлар ва хорижий мамлакатлар жиноят қонунчилиги нормалари таҳлил қилинган.*

Калит сўзлар*: кибертерроризм, халқаро ҳужжатлар, ахборот технологиялари, жиноят, жавобгарлик.*

Annotation*: this article analysis the international acts and standards of the foreign criminal legislation providing questions of counteraction to cyberterrorism.*

Key words*:cyberterrorism, international acts, information technologies, crime,liability.*

Данное направление представляется нам весьма перспективным в плане развития международно-правового регулирования, поскольку здесь степень общности интересов различных государств оценивается нами как достаточно высокая.

Как особая разновидность киберпреступленийкибертерроризм представляет собой комплексную акцию, выражающуюся в преднамеренной, политически мотивированной атаке на информацию, обрабатываемую компьютером и компьютерными системами, создающей опасность для жизни или здоровья людей либо наступления других тяжких последствий, если такие действия были содеяны с целью нарушения общественной безопасности, запугивания населения, провокации военного конфликта [10].

По мнению Е.В.Старостиной и Д.Б. Фролова, информационный терроризм отличается от этих форм воздействия на киберпространство, прежде всего своими целями, которые остаются свойственными политическому терроризму. Средства осуществления информационно-

террористических действий могут варьироваться и включать все виды современного информационного оружия. В то же время тактика и приемы его применения существенно отличаются от тактики информационной войны и приемов информационного криминала [6].

А.В. Соколов и О.М. Степанюк отмечают, что кибертерроризм предусматривает применение информационных технологий в целях террористического воздействия, ложную угрозу акта кибертерроризма, влекущую за собой серьезные экономические последствия, уничтожение или активное подавление линий связи, неправильную адресацию, искусственную перегрузку узлов коммутации [5].

Следовательно, самый опасный вид информационных преступлений на современном этапе развития общества – это кибертерроризм. Данный термин был предложен в 1980-х годах старшим научным сотрудником Института безопасности и разведки (*InstituteforSecurityandIntelligence*) Барри Коллином, который использовал его в контексте тенденции к переходу терроризма из физического в виртуальный мир, возрастающего пересечения и срастания этих миров [8; 25-с.].

Прежде всего, следует подчеркнуть, что УК многих стран пока не успевают за подобными новейшими рисками, вызовами и угрозами киберпреступности. Практически во всех странах преступления террористического характера, совершаемые в сетях (виртуальном мире) и информационном пространстве, остаются за пределами правового поля, а преступники привлекаются к ответственности по статьям за обычный терроризм.

В качестве одного из редких примеров можно назвать Закон **Великобритании** «О терроризме» 2000 года, который устанавливает, что *незаконное проникновение в компьютеры, их системы или сети, повлекшее за собой значительный ущерб или их использование полученной таким образом компьютерной информации для организации массовых насильственных действий,* может быть приравнено к актам террора и, соответственно, влечь за собой повышенную ответственность [9], а также статья 421^1 УК **Франции** – *«Террористические акты, связанные с деяниями в области информатики»*.

Примером кибертерроризма с использованием современных информационных технологий может служить убийство, совершенное в 1998 году в одной из клиник США, где в тяжелом состоянии и под охраной ФБР находился с тяжелым ранением особо важный свидетель. Получив через Интернет несанкционированный доступ к локальной сети клиники, и преодолев ряд шлюзов и защитных барьеров, хакер-убийца произвел перенастройку кардиостимулятора, в результате чего пациент скончался.

В настоящее время, исходя из диспозиции статей УК касательно терроризма, можно предположить, что под кибертерроризмом следует понимать преднамеренную, политически мотивированную атаку на информацию, обрабатываемую компьютером, компьютерную систему и сети, которая создает опасность для жизни или здоровья людей либо наступления других тяжких последствий, если такие действия были содеяны с целью нарушения общественной безопасности, запугивания населения, провокации военного конфликта [7]. **В УК Узбекистана ответственность за кибертерроризм не предусмотрена.**

Международные акты, в свою очередь, также не регламентируют вопросы противодействия кибертерроризму. В настоящее время наиболее авторитетным международно-правовым актом комплексного характера является **Конвенция Совета Европы о киберпреступности** от 23 ноября 2001 года, участниками которой по состоянию на 1 июня 2018 года выступают 56 государств [9]. 28 января 2003 года также был принят Дополнительный протокол к Конвенции о киберпреступности в отношении криминализации деяний расистского и ксенофобского характера, совершаемых при помощи компьютерных систем. Данные акты определяют составы киберпреступлений, процессуальные аспекты борьбы с ними, правила установления юрисдикции, а также регламентируют международное сотрудничество в борьбе с киберпреступностью.

Генеральной Ассамблеей и иными органами ООН в последние годы уделяется повышенное внимание данной проблематике. Однако пристальное внимание к указанной проблеме пока не повлекло принятия универсальных международных договоров, аналогичных названным документам Совета Европы. Между тем, наличие потребности в них безоговорочно признается международными экспертами. В частности, в рабочем документе, подготовленном Секретариатом Двенадцатого Конгресса ООН по предупреждению преступности и уголовному правосудию, прошедшего в Сальвадоре (Бразилия) 12-19 апреля 2010 года [1], содержалась рекомендация о разработке глобальной конвенции против киберпреступности.

Характеризуя региональный уровень международного сотрудничества в рассматриваемой сфере, следует отметить, что в рамках СНГ и ШОС действуют соответствующие соглашения.

Соглашение между правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной

безопасности определяет информационный терроризм как использование информационных ресурсов и (или) воздействие на них в информационном пространстве в террористических целях [2; 26]. Тем самым смысл данного определения указывает на то, что кибертерроризм является одним из видов терроризма, следовательно, квалификация указанного деяния должна осуществляться по аналогии с терроризмом. На первый взгляд, терроризм и кибертерроризм являются очень схожими понятиями. Однако, следует особо подчеркнуть, что кибертерроризм качественно отличается от общепринятого понятия терроризма, сохраняя лишь стержень этого явления и часть его уголовно-правовых элементов – субъективных и объективных признаков состава преступления. При этом, кибертерроризм как умышленное преступление, преследуя те же цели, что и терроризм, представляет собой наиболее важный вид информационных атак деструктивного характера на информационную инфраструктуру, являющихся дополнительным объектом. В свою очередь, основной объект терроризма и кибертерроризма сохраняются схожими.

Чаще всего кибертерроризм совершается в целях запугивания населения и оказания воздействия на органы государственной власти и международные организации. Отметим, что в информационной сфере границы между действиями криминальных элементов, террористов и государств чрезвычайно диффузны и подвижны. Учитывая стремление террористов к максимизации масштабов причиненного вреда и вызванного ими резонанса, полагаем, что ключевой целью атак террористов будет выступать критически значимая информационная инфраструктура.

Такие атаки террористов вполне подпадают под определения «бомбового терроризма» (статья 2 Международной конвенции о борьбе с бомбовым терроризмом от 15 декабря 1997 года [3; 5]) и «технологического терроризма» (статья 1 Договора о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с терроризмом от 4 июня 1999 года [4]), что позволяет использовать положения данных международно-правовых актов для борьбы с кибертерроризмом. Вместе с тем принятие специальных международных договоров универсального и регионального характера в области противодействия кибертерроризму также представляется необходимым, поскольку данная разновидность терроризма имеет тенденцию динамичного роста, свою специфику, тем самым представляет реальную угрозу глобальной безопасности.

Согласно УК Республики Узбекистан, общественно – опасные деяния, признаваемые экспертами и академическими кругами в качестве так называемого кибертерроризма, не предусмотрены в национальном уголовном законе. Указанные действия будут квалифицированы как терроризм (статья 155), использование информационных технологий рассматривается как орудие или способ совершения преступления. Представляется целесообразным разработать определение понятия «кибертерроризма» в законодательстве Республики Узбекистан и внести уголовную ответственность за подобные действия.

На наш взгляд, кибертерроризм должен включать следующие умышленные действия:

1. неправомерное завладение или уничтожение линий связи и телекоммуникаций, информационных ресурсов, программно-технических оборудований, имеющих стратегическую важность, путем преодоления систем защиты, внедрения вредоносных программ или вирусов, программных закладок и т.п.;

2. нанесение ущерба отдельным физическим элементам информационного пространства (разрушение сетей электропитания или электростанций, наведение помех, переадресация потока данных, искусственная перегрузка узлов коммутации, использование химических средств для разрушения элементной базы и др.);

3. воздействие на программное обеспечение или информацию в информационных системах и системах управления с целью их искажения или модификации;

4. раскрытие и угроза распространения или распространение конфиденциальной информации об информационной инфраструктуре государства, стратегически важных и информационных систем обороны, кодах шифрования, принципах работы систем шифрования;

5. захват технических каналов связи или сетей телекоммуникаций с целью распространения дезинформации, слухов, демонстрации мощи террористических организаций и антиконституционных структур;

6. проведение информационно-психологических операций, воздействие на операторов и разработчиков информационных и телекоммуникационных сетей и систем путем насилия или угрозы насилия, шантажа, подкупа, использования нейролингвистического программирования,

гипноза, средств создания иллюзий, мультимедийных средств для ввода информации в подсознание или ухудшения здоровья человека и т.д.

Таким образом, использование как обязательных, так и необязательных международных или региональных документов может обеспечить значительный положительный результат с точки зрения усиления эффективности и согласованности национального законодательства, а в долгосрочной перспективе может содействовать укреплению международного сотрудничества в борьбе с глобальными вызовами, в том числе с кибертерроризмом. В связи с этим, считаем целесообразным включить в Закон Республики Узбекистан «О борьбе с терроризмом» понятие кибертерроризма. Также считаем необходимым, включить в Уголовный кодекс Республики Узбекистан статью следующего содержания:

«Статья ___. Кибертерроризм

Кибертерроризм, а именно неправомерное завладение, воздействие и иные действия в отношении информационно-коммуникационного пространства, сетей телекоммуникации и сети Интернет с целью дестабилизации деятельности государственных органов или общественно-политической обстановки либо подрыва экономики Республики Узбекистан, -

наказывается лишением свободы от пяти до восьми лет.

Те же действия, повлекшие смерть человека или иные тяжкие последствия, -

наказывается лишением свободы от восьми до двенадцати лет».

Установление уголовной ответственности за кибертерроризм позволит обеспечить надежную защиту мира и безопасности в информационно-коммуникационном пространстве.

References:

1. Salvadorskaya deklaratsiya o kompleksnix strategiyax dlya otveta na globalniye vizovi: sistemi preduprejdeniya prestupnosti i ugolovnogo pravosudiya i ix razvitiye v izmenyayushemsya mire, prinyataya rezolyutsiyey 65/230 Generalnoy Assamblei ot 21 dekabrya 2010 goda (http://www.un.org).
2. Soglasheniye mejdu pravitelstvami gosudarstv-chlenov SHOS o sotrudnichestve v oblasti obespecheniya mejdunarodnoy informatsionnoy bezopasnosti // Byulleten mejdunarodnix dogovorov. - №1. - 2012. - S.24-27.
3. Byulleten mejdunarodnix dogovorov. - 2001. - № 11. - 256 s.
4. Byulleten mejdunarodnix dogovorov. - 2006. - № 9. - 324 s.
5. Sokolov A. V. Informatsionnoye obshestvo v virtualnoy i sotsialnoy realnosti. - SPb.: Aleteyya, 2012. - 178 s.
6. Starostina Ye.V., Frolov D.B. Zashita ot kompyuternix prestupleniy i kiberterrorizma. Voprosi i otveti (Istochnik: http://kursak.net/kiberterrorizm-i-osobennosti-ego-proyavleniya/)
7. Golubev V.A., Golovin A.Yu. Problemi rassledovaniya prestupleniy v sfere ispolzovaniya kompyuternix texnologiy. http://www.crime-research.org/library/New_g.htm
8. Collin B. The Future of Cyberterrorism // Crime & Justice International Journal. 1997. Vol. 13. - R. 23-26.
9. www.coe.int
10. www.kursak.net