***Международная научно-практическая конференция***
***«Экономика, политика, право: вчера, сегодня, завтра. Роль профсоюзов» 2017 год***

*Чернышев Игорь Александрович*
*магистрант юридического факультета*
*ФГБОУ ВО «БГУ»*
*Науменко Екатерина Николаевна*
*ст. преподаватель кафедры уголовного процесса*
*юридического факультета ФГБОУ ВО «БГУ»*

# НАИБОЛЕЕ АКТУАЛЬНЫЕ ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ КИБЕРТЕРРОРИЗМУ В РОССИИ НА ОСНОВЕ ОПЫТА ЗАРУБЕЖНЫХ СТРАН

*Аннотация: В работе рассмотрены актуальные проблемы кибертерроризма. Особое внимание уделено международному опыту борьбы с кибертеррористическими преступлениями. Также отмечены статистические данные о количестве пользователей сети Интернет. Сделан вывод о том, что изменения законодательства позволят сократить количество нарушений, что положительно скажется на качестве и безопасности киберпространства и защите лично информации.*
*Ключевые слова: терроризм, компьютерные преступления.*

**The most actual problems of countering cyber terrorism in Russia on the basis of the experience of foreign countries**

*The paper discusses topical issues of cyberterrorism. Particular attention is paid to the international experience of combating cyberterroristic crimes. Also noted statistics on the number of Internet users. It was concluded that changes in legislation will reduce the number of violations that have a positive impact on the quality and security of cyberspace and the protection of personal information.*
*Keywords: terrorism, computer*

Актуальность данной статьи обусловлена серьезной угрозой человечеству со стороны кибертерроризма. Имеющийся на данный момент у мирового сообщества опыт недостаточен для полноценного противодействия данной угрозе и говорит о наличии гарантированной уязвимости любого государства. Это напрямую связано с тем, что кибертерроризм является транснациональным явлением, а его участники имеют возможность угрожать информационным системам из любой точки мира. Ведь используя глобальную сеть Интернета террористам можно собрать подробную информацию об объектах атак, их

местонахождении. Так же осуществление сбора денег для поддержки террористических движений.

Кибертерроризм — это технический вид терроризма. По мнению А. Кассиса[3, ст. 2] (американский политолог), существует более сотни определений данного понятия. Предпосылкой возникновения такого феномена, как терроризм, в какой-то степени является проявление информационного терроризма в псевдонаучной среде. Т.е. понятие кибертерроризм эволюционировало от информационного терроризма.

Постоянно растет число пользователей сети Интернет. В США их уже 158 миллионов, в Европе - девяносто пять, в Азии - 90, в Латинской Америке - четырнадцать, а в Африке - три. В России, по разным оценкам, количество пользователей Интернет составляет от 3,5 до 8 миллионов человек.[2]

Сегодня можно говорить, что Интернет охватывает все страны мира, так как с применением новых технологий (использование мобильных спутниковых устройств связи) возможно подключение к сети Интернет с любой точки земного шара. Если же говорить о развернутой инфраструктуре, то в таком контексте Интернет охватывает сегодня более 150 стран мира.

В настоящее время более 100 стран, в том числе 60% членов Интерпола, не имеют законов, предназначенных для борьбы с киберпреступлениями». [2, ст 12]

Удачным примером профилактики информационных преступлений можно назвать Южную Корею. Ввиду развития информационных технологий, Южная Корея входит в число лидеров - стран, в которых были приняты законы об электронном обучении, индустрии электронного обучения и об индустрии знаний. Примером такой системы является «E-Learning». Существует определение, которое дали специалисты ЮНЕСКО: «e-Learning — обучение с помощью Интернет и мультимедиа». [5] Новые технологии дают возможность получать знания жителям самых удаленных регионов страны, в том числе детям-инвалидам. Об этом и многом другом рассказал профессор

южнокорейского Университета Сунгьюнкван Дэ Джун Хван. В стране поддерживают e-learning на государственном уровне. E-learning трансформировался в многообещающий бизнес, объемы которого ежегодно растут на 8,2%. Сегодня в Корее на основе закона о высшем образовании и закона о непрерывном образовании работают 18 виртуальных университетов. [6]

Министерство обороны Японии в свою очередь создаст комитет для защиты компьютерных сетей от растущего числа кибератак. Напомним, что в июле 2009г. правительственные сайты в Южной Корее и США были атакованы целой волной данных от зараженных вирусами компьютеров из нескольких десятков стран. Зараженная вирусами электронная почта была послана также в Министерство обороны и Силы самообороны Японии.

Помимо этого списка существует еще множество мер, которые принимаются правительствами данных стран. Проблема приобретает все больший масштаб, и отрицать ее актуальность и необходимость решения становится просто бессмысленным.

Китай, так же как и другие страны Восточной Азии, подвержен кибератакам. Но при этом мы можем говорить о том, что киберпреступления в основном процветают именно в этой стране. Как уже было сказано выше правительство КНР «закрывает глаза» на действия преступников. Или даже молчаливо «поощряют» их действия, ведь пиратство в Китае помогает в развитии информационных технологий.

Явным признаком такого «поощрения» является то, что Китай не принял участие в подписании как Европейской Конвенции по киберпреступлениям, так и Окинавской Хартии глобального информационного общества.

Предполагается, что мерами уголовно-правового противодействия кибертерроризму можно добиться существенного улучшения состояния защищённости критически важных объектов информационной инфраструктуры России.

Мнения исследователей по данному поводу разделились на два основных направления. Так, одна группа исследователей проблемы кибертерроризма полагает, что кибертерроризм подпадает по действие ст. 205 УК РФ и не требует включения в уголовный закон ещё одной нормы. Так, Д.Б. Фролов считает, что в ст. 205 УК РФ [1, ст. 2] налицо все признаки терроризма: и политическая окраска, и совершение деяний с целью создания атмосферы страха, напряженности, паники, и принцип публичности (четко выделяющий эту категорию преступлений из остальных разновидностей киберпреступности), и направленность не на конкретных лиц (в отличие от других видов преступлений), а на неопределенный круг граждан, становящихся жертвой кибертеррора. Только указанные деяния кибертеррориста носят характер не взрыва, поджога, а «иных действий». Данные поправки вступили в законную силу только 27 июля 2006 года, с чего можно сделать вывод, что доктринальное закрепление многих важных положений в нашей стране сильно отстает от авторов данных идей, которые были предложены еще в 2005 году. На сегодняшний день УК РФ к кибертерроризму относятся преступность террористической направленности – «Террористический акт» (ст. 205 УК РФ), «Содействие террористической деятельности» (ст. 205-1), «Публичные призывы к осуществлению террористической деятельности или публичное оправдание терроризма» (ст. 205-2), «Заведомо ложное сообщение об акте терроризма» (ст. 207).

Решения проблемы, кибертерроризма не просты и не однозначны. Кибертеррористы и их действия должны быть «привязаны» к закону. Это должно быть сделано в контексте как национальной, так и международной политики противодействия кибертерроризму. Серьезность террористической угрозы не может игнорироваться ни Россией, ни другими странами. Решимость принять необходимые меры может быть реализована в рамках новых эффективных международных законов и с новым воззрением на их действенность и применимость. Таким образом, решение проблемы борьбы с

этими опасными явлениями на сегодняшний день это задача, которая требует объединения усилий, интеллектуального потенциала и доброй политической воли всего мирового сообщества.

Комплексная реализация соответствующих мер в России будет способствовать обеспечению международной безопасности от кибертеррористических угроз, а также защите интересов государства, общества, личности.

В нынешнее время складывающаяся обстановка требует неотложного совершенствования и развития действующей системы борьбы с терроризмом как целостной, интегрированной структуры, объединяющей противодействие терроризму на всех направлениях, включая и новое его проявление. Одним из инструментов противодействия кибертерроризму является уголовно-правовой институт как в рамках национального законодательства, так и на уровне международном. В условиях борьбы с терроризмом особую значимость приобретает предупредительная функция уголовно-правовой системы.

*Список литературы:*

1. *Уголовный кодекс Российской Федерации от 13.06.1996 № 63 – ФЗ// Собрание законодательства РФ. 17.06.1996. № 25 (ред. от 30.12.2015).*
2. *Правовые аспекты борьбы с кибернетическими преступлениями в ЕС // Борьба с преступностью за рубежом. - 2003. -М: 48с.*
3. *Фролов Д.Б. Пути совершенствования законодательной системы в борьбе с кибертерроризмом в России и за рубежом // Законодательство и экономика. – 2005. – № 5.*
4. *В. Голубев. Кибертерроризм как новая форма терроризма. URL: http://www.crime-research.org/library/Gol_tem3.htm*
5. *Понятие E-Learning. 2009г. URL: http://elms.eoi.ru/Wiki/1.3.%20%D0%9F%D0%BE%D0%BD%D1%8F%D1%82%D0%B8%D0%B5%20e-Learning.aspx*
6. *Россия не торопится в электронное общество? 2009г. URL: http://old.poisknews.ru/articles/5835-otstavit-otstavanie.html*

*Bibliography:*

*1. The Criminal Code of the Russian Federation of 13.06.1996 number 63 - FZ // Meeting of the legislation of the Russian Federation. 17.06.1996. Number 25 (ed. By 12.30.2015).*
*2. Legal aspects of the fight against cybercrime in the EU // Crime abroad. - 2003-M: 48c.*
*3. D.B. Frolov Ways to improve the legislative framework in the fight against cyber-terrorism in Russia and abroad // the Legislation and economy. - 2005. - № 5.*

*4. V. Golubev. Cyber-terrorism as a new form of terrorism. URL: http://www.crime-research.org/library/Gol_tem3.htm*

*5. The concept of E-Learning. 2009. URL:*
*http://elms.eoi.ru/Wiki/1.3.%20%D0%9F%D0%BE%D0%BD%D1%8F%D1%82%D0%B8%D0%B5%20e-Learning.aspx*

*6. Russia is in no hurry to electronic society? 2009. URL: http://old.poisknews.ru/articles/5835-otstavit-otstavanie.html*