УДК 343.9 DOI: 10.17748/2075-9908-2015-7-6/2-207-209

ЗВЕРЯНСКАЯ Лариса Павловна,
Эхирит-Булагатского филиала Иркутской областной коллегии адвокатов, Иркутск, Россия
ZveryanskayaL@mail.ru

ZVERIANSKAIA Larisa P.,
Ekhirit-Bulagat Irkutsk Regional branch of the Bar Association, Irkutsk, Russia
ZveryanskayaL@mail.ru

ПРОБЛЕМА КИБЕРТЕРРОРИЗМА С ТОЧКИ ЗРЕНИЯ РОССИЙСКОГО ОБЩЕСТВА

CYBERTERRORISM PROBLEM IN TERMS OF RUSSIAN SOCIETY

Проблема кибертерроризма в мировом сообществе считается первоочередной, годовой ущерб от такого вида преступной деятельности и киберпреступлений уже начитывает более 400 млрд долл. США. Зарубежные государства и частные компании тратят миллионы долларов на поиск идеальной защиты от террористов, кибергруппировок и простых хакеров. Что же касается нашего государства, то Российская Федерация столкнулась с этой проблемой сравнительно недавно, но уже сейчас можно увидеть примеры совершённых кибертеракт, направленных против нашего государства. Но в науке и в практике до сих пор идет дискуссия о существовании общественной опасности нового вида терроризма и его последствий. Одна из причин этого в том, что в современном законодательстве Российской Федерации не закреплено понятие кибертерроризма. Автором статьи проведено исследование проблемы с точки зрения российского общества. Приведены примеры недавних кибертеракт, совершенных на территории Российской Федерации и против нее. Проанализированы последствия, а также общественная опасность кибертеррора. Как итог исследования предложено принятие поправок в действующее законодательство, затрагивающее сферы информационного пространства, компьютерных преступлений и кибертерроризма.

The problem of cyber-terrorism in the international community is considered a priority, the annual losses from cyber terrorism and cybercrime have recites over 400 billion dollars. State and private companies spend millions of dollars on cyber defense against terrorists, and simple cyber group hackers. As for our country, the Russian Federation was faced with manifestations of cyber-terrorism are relatively not long ago, but now we can see examples of cyber-terrorism against our country. In science and practice is still going debate about the public danger of cyber terrorism and its consequences. One reason for this, is that in the current legislation of the Russian Federation there is no legal definition of the concept of terrorism and cyber-terrorism can not completely cover the entire spectrum of cyber-terrorism. The author of the article a study of cyber-terrorism from the perspective of Russian society. Examples of recent cyber act of terrorism committed in the territory of the Russian Federation and against it. Analyzed the effects of committed cyber act of terrorism and social danger of cyberterrorism. As a result of research suggested the adoption of amendments to the existing legislation that affects the scope of the information space, computer crimes and cyberterrorism.

Ключевые слова: **терроризм, кибертерроризм, Интернет, информационное пространство, кибертеррористы, киберпреступления.**

Keywords: **terrorism, cyber-terrorism, the Internet, information space, cyber terrorists, cyber-crime.**

Благодаря массовой компьютеризации основных инфраструктур жизнедеятельности человечества, сети Интернет, появлению электронных денег, социальных сетей, интернет-СМИ и интернет-магазинов, современный человек полностью стал зависим от бесперебойной работы сети Интернет. Все это сподвигло преступников использовать Интернет, как основное средство и место для совершения преступлений, большинство же традиционных правонарушений, таких как кража и мошенничество, трансформировалось в новые виды преступной деятельности, с новыми особенностями и следовой картиной. Ущерб от киберпреступлений в масштабе всей нашей страны только за 2014 г. составляет более 3,3 млрд долл. США, и это только обнародованные данные [3].

Современные террористы также решили не отставать от течения времени, и в следствие этого появился новый вид терроризма, а именно кибертерроризм. Новый вид характеризуется использованием новых информационных технологий, а также осуществлением своей деятельности посредством и внутри глобальной сети Интернет.

За последние пять лет выросло количество кибератак, проводимых на территории РФ. На 2015 г. было зафиксировано наибольшее количество, за этот год атакам подверглось более 600 сайтов российских компаний и государственных органов. В основном за это ответственны кибертеррористы «Исламского государства», а также кибергруппировки Team System Dz, FallaGa Team и Global Islamic Caliphate. Они блокировали работу сайтов, а затем размещали на них пропагандистские материалы. Главной же целью был вывод из строя общественно важных сайтов, сбой деятельности организаций, запугивание и распространение паники и хаоса среди населения Российской Федерации.

Установлено, что жертвами кибертеррористов стали: сайт девелопера элитного жилья «Анапа-Лазурное», крымского ЧОПа «Русичъ-Юг», портал администрации Борисоглебского района Ярославской области, НПП «Гидрокомплект», центр сердечной медицины «Черная речка», Управляющая компания «Нижнеисетская» из Екатеринбурга, сайт Североуральского краеведческого музея и др.

Эксперты объясняют выбор разных объектов для атак тем, что хакеры-исламисты, взламывая различные сайты, набираются опыта, чтобы затем атаковать сайты органов власти и государственных корпораций. По их мнению, самая большая опасность состоит в том, что кибертеррористы смогут добраться до системы автоматического управления объектов инфраструктуры – электростанций, водоканалов и т.п. [2].

Также очень опасны морально-психологические методы воздействия, давления и вербовки кибертеррористов, направленные на граждан нашего государства. Всемирная сеть – благодатная почва для распространения различных слухов, в том числе и тревожных, и эти возможности сети также используются террористическими организациями [1].

Как видно из примеров, уже сейчас проблема защиты от терроризма стоит как никогда остро, существует реальная опасность для Российской Федерации, но в масштабе всей страны, в науке и в практике нет единого мнения о кибертерроризме, этому свидетельствует отсутствие законодательного закрепления понятия и состава преступления. На сегодняшний день правовые основы противодействия киберпреступности и кибертерроризма все еще не отвечают реалиям дня, а уровень подготовки специалистов не достаточен и не адекватен угрозе. Сформировавшееся глобальное информационное пространство требует новых подходов в части борьбы с трансграничной организованной преступностью, имеющей на вооружении современнейшие знания и технологии, а также подготовки новых специалистов в сфере информационно-телекоммуникационных сетей.

Перед нашим государством стоит важная задача по обеспечению информационной безопасности как отдельной личности, так и всего российского общества в сети Интернет. В связи с этим обосновывается необходимость внесения ряда изменений в современное законодательство, затрагивающее сферы информационного пространства.

Целесообразно внесение законодательного определения кибертерроризма и ответственности за него, как сделано в зарубежных странах, либо внесение дополнительного квалификационного признака в ст. 205 УК РФ «Террористический акт»: *совершение террористического акта посредством использования сети Интернет* и дополнения в п. 2 ст. 205.2 УК РФ «Публичные призывы к осуществлению террористической деятельности или публичное оправдание терроризма»: *к средствам массовой информации добавить сеть Интернет.*

БИБЛИОГРАФИЧЕСКИЕ ССЫЛКИ

1. *Донская Д.* Кибертерроризм и свобода личности. Реалии и мифы кибертерроризма. Часть 2 [Электронный ресурс]. URL: http://www.honestnet.ru/terrorizm/kiberterrorizm-i-svoboda-lichnosti-realii-i-mify-kiberterrorizma-chast-2.html (дата обращения: 20.10.2015)
2. Кибертеррористы ИГ массово взламывают российские сайты. «Их цель – посеять панику» [Электронный ресурс]. URL: http://ura.ru/news/1052227021 (дата обращения: 20.10.2015)
3. Средний годовой ущерб от киберпреступлений в России достиг 3,3 млн долл. для организации [Электронный ресурс]. URL: http://pultnews.ru/srednij-godovoj-ushherb-ot-kiberprestuplenij-v-rossii-dostig-33-mln-doll-dlya-organizacii/ (дата обращения: 01.10.2015)

REFERENCES

1. *Donskaya D*. Cyberterrorism and freedom of the individual. Realities and myths of cyberterrorism [Kiberterrorizm i svoboda lichnosti. Realii i mify kiberterrorizma]. Part 2. Available at: http://www.honestnet.ru/terrorizm/kiberterrorizm-i-svoboda-lichnosti-realii-i-mify-kiberterrorizma-chast-2.html (accessed: 20.10.2015)
2. Cyberterrorists IG massively hack Russian sites. «Their goal is to sow panic». Available at: http://ura.ru/news/1052227021 (accessed: 20.10.2015)
3. Average annual damage from cyber crime in Russia has reached 3.3 million. for the organization. Available at: http://pultnews.ru/srednij-godovoj-ushherb-ot-kiberprestuplenij-v-rossii-dostig-33-mln-doll-dlya-organizacii/ (accessed: 01.10.2015 G.)

Информация об авторе

Зверянская Лариса Павловна, стажер адвоката Эхирит-Булагатского филиала Иркутской областной коллегии адвокатов, Иркутск, Россия
ZveryanskayaL@mail.ru

Получена: 03.11.2015

Information about the author

Zverianskaia Larisa P., Trainee Lawyer Ekhirit-Bulagat Irkutsk Regional branch of the Bar Association, Irkutsk, Russia
ZveryanskayaL@mail.ru

Received: 03.11.2015

Для цитирования статьи: Зверянская Л. П., Проблема кибертерроризма с точки зрения российского общества. Краснодар: Историческая и социально-образовательная мысль. 2015. Том 7. №6. Часть 2. с- doi-

For article citation: Zverianskaia L. P., Cyberterrorism problem in terms of russian society.[Problema kiberterrorizma s tochki zreniya rossiyskogo obshchestva]. Krasnodar. *Istoricheskaya i sotsial'no-obrazovatelnaya mys'l = Historical and Social Educational Ideas.* 2015. Tom 7. No. 6 vol-2. Pp. - . doi: