Акопов Г.Л.

ХАКТИВИЗМ — ВЫЗОВ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННОМ ОБЩЕСТВЕ.

Аннотация. *В статье рассматриваются вопросы кибер угроз и кибер терроризма. Автор объясняет данный феномен динамичным информационно-коммуникационным развитием современного общества. В статье рассматриваются факторы породившие явление кибертерроризма. Особое внимание уделяется атак называемым хактивистам — безвозмездно совершающим кибер теракты в целях поддержки разделяемых ими политических идет. Приводиться ряд конкретных примеров хактивисткой деятельности. Как следствие, государствам сегодня все чаще приходиться задумываться о создании кибер-щита для обеспечения информационной безопасности. Теоретико-методологические основы заключаются в системном, сравнительном, проблемном и других общенаучных подходах и методах политической науки и смежных дисциплин. Основным выводом автора является необходимость противостояния информационным угрозам и противодействие кибе-террору. Обеспечение информационной и кибер безопасности должно стоять сегодня во главе угла каждого государства. Для обеспечения информационной и кибер безопасности и противодействию данным угрозам автор рекомендует формировать кибер войска на основе научных рот.*
Ключевые слова: *кибер-щит, кибертерроризм, киберугроза, кибервойска, хакерские атаки, хактивизм, информационный суверенитет, Информационная безопасность, кибер безопасность, информационное общество.*

Review. *This article examines the issues of cyber threats and cyberterrorism. The explanation for this phenomenon is the dynamic information-communication development of the modern society. The article examines the factors that gave rise to cyberterrorism. A special attention is given to the so-called hacktivists – those who commit acts of cyberterrorism without financial gain, but rather to support their political ideas; a number of specific examples of hacktivist activity are being presented. As a result, the governments today are forced to concentrate harder about creation of a cyber shield to ensure information safety. Among the main conclusions the author substantiates the need to place cyber security as the corner stone of every nation. To ensure information and cyber security and counteract these threads, the author recommends forming cyber forces based on scientific brigades.*
Keywords: *cyberterrorism, cyber threat, cyber forces, hacker attacks, hacktivism, information sovereignty, cyber shield, information security, cyber security, information society.*

Современное общество все более становиться информационно уязвимым и подвергается разнообразным информационным угрозам, необходимость в обеспечение информационной безопасности особенно актуально в эпоху тотальной информатизации общества[1]. Современные угрозы определяются не только развитием информации, но и повсеместным внедрение информационных технологий.

Как утверждает профессор Смирнов А. И.: «Планета охвачена беспрецедентной информационной революцией. Её феномен создал условия для формирования глобальной информационной инфраструктуры, которая предоставила принципиально новые возможности социализации людей, их общения и доступа к накопленным человечеством знаниям. Однако ИКТ, будучи технологиями двойного назначения, стали не только локомотивом, но и нервом глобализации, ибо несут в себе принципиально новые вызовы и стратегические риски» [2].

И подобных рисков и угроз возникает не мало[3], в данной статье мы считаем необходимым отдельно обозначить опасности превращения хакеров в политических террористов[4]

DOI: 10.7256/2073–8560.2015.4.15834

в современном информационном обществе. Особенно в контексте формирования в России и мире нового рода войск — кибервойск. Которые по своей сути, являются политическими хактивистами несущими воинскую обязанность.

«Хактивизм» как явление имеет ряд определений. Панарин И. Н. в книге «Информационная война и выборы» обозначил «Хактивизм», как «бескорыстное» хакерство в целях политического активизма[5]. Там же, автор справедливо утверждал, что современное хакерское движение оказалось, втянуто в игры политиков. На наш взгляд «Хактивизм» это не обязательно «бескорыстное» хакерство, мы скорее считаем, что «Хактивизм» это хакерство в политических и военных целях. Тем более, что политически ангажированные хакеры все чаще стоят на службе у властных и политических структур получая не только идеологическую поддержку, но и материальное стимулирование.

Хактивисты все чаще выступают в роли «кибертеррористов», нанося весьма ощутимые потери объектам хакерских атак.

Примечательно, что политика кибертеррора, как и многие современные политические технологии разработана в США. Как утверждается в докладе исследовательской службы Конгресса США № RL30735: «кибертерроризм — это один из многих видов киберугроз, которые вызывают всеобщую озабоченность … в число его целей могут входить политическая или экономическая дестабилизация, саботаж, кража военных или гражданских активов и ресурсов в политических целях» [6].

Распространение кибертеррора уже сегодня вызывает обеспокоенность у мировой политической элиты. Совершенно не случайно проблемы киберугроз все чаще становятся ключевыми аспектами переговорного процесса. Так, например, в мае 2015 представители БРИКС, курирующие вопросы безопасности, договорились выработать единые подходы в сфере обеспечения информационной безопасности [7]. В июне 2013 года лидеры США и Китая встречались с целью обсудить проблемы кибертерроризма[8]. А, за несколько месяцев до обозначенных событий Б. Обама выступив перед конгрессом отметив, что проблема борьбы с кибертерроризмом является приоритетной для США[9]. К тому же, в его выступлении была обозначена стратегия на формирования кибервойск, для защиты страны от киберугроз.

В течение 2013–2014 годов, Европа, Китай и Россия заявили о формирования кибервойск. Из уст Президента России подобное поручение прозвучало 21 января 2013 года [10].

Примечательно, что роль кибератак настолько велика, что возможности противодействия кибертеррору являются весомым аргументом в предвыборных баталиях. Так кандидат на пост Президента США, Хиллари Клинтон, в первой же официальной предвыборной речи, произнесенной в Нью-Йорке, отметила: «Ни одна страна лучше не подготовлена, чтобы ответить на растущие угрозы кибератак … » [11].

В июля месяце Х. Клинтон на встрече со своими сторонника заявила, что: «не только Китай представляет угрозу кибербезопасности США, но также Россия, КНДР и Иран» [12].

Как утверждают специалисты на сегодняшний день более сотни стран активно экспериментируют в области видения кибервойны. И угрозы проведения кибервойны становятся все более явными, подобная война может принимать самые разнообразные формы, от хакерских атак до «киберхиросимы».

И первые киберстолкновения показывают реальность обозначенной проблемы. Так, в контексте разногласий между Российской Федерацией и США по вопросам смены власти на Украине в 2014 году и референдума жителей Крымского полуострова, на официальные интернет-ресурсы органов государственной власти, СМИ, крупнейшие бизнес структуры обрушился шквал атак политически ангажированных хакеров — «хактивистов» [13].

Важно учесть, что все чаще действия хактивистов, отстаивающих определенные политические идеи, приводят к ответным действиям. Так после хакерских атак на Российские интернет-ресурсы, виртуальной атаке подверглись сайты НАТО [14]. Также хактивисты выложили в интернет-электронную переписку представителей руководства украинских партий «Удар» и «Батькивщина». Об этом хакеры сообщили на своих страницах «В Контакте» и Facebook [15].

Объединение хактивистов получившее название «КиберБеркут» взломало и уничтожило

DOI: 10.7256/2073–8560.2015.4.15834

систему ЦИК Украины [16]. После чего совершило еще не мало политических акций.

Трудно не согласиться с Фрэнком Барнаби, который в монографии «Будущее террора» утверждает, что кибертеррорист с ноутбуком способен нанести больше вреда, нежели террорист вооруженный бомбами и иными взрывчатыми веществами [17].

И если пару лет назад технологии кибервойн были орудием международного терроризма, то в настоящее время кибервойска официально создаются в информационно развитых государствах. А кибероружие активно применяется в военных конфликтах, например, в ходе интервенции США в Ливии, где они контролировали не только воздушное пространство, но и телекоммуникационные сети. Они входили в ливийские телесети и передавали передачи для местного населения [18].

Объективная оценка реальности угроз позволяет говорить о необходимости особого внимания процессу создания кибервойск, для обеспечения кибербезопасности государства.

Об этом, в частности, пишет Берг Гиацинт в работе «Кибервоины на войне», утверждая, что некоторые военные операции в рамках информационной войны, требуют новой правовой основы, и необходимы конкретные нормативно-правовые меры для противодействия вероятным информационным угрозам. По мнению доктора Гиацинта, успех в войнах будущего возможен при организации упреждающих ударов и решительных военных действий, осуществляемых по пятиугольной системе современной войны: «земля, море, воздуха, киберпространство, и космическое пространство» [19].

Вероятно, в ближайшие годы в России появятся кибервойска сформированные на основе научных рот, которые создаются в отечественных вооруженных силах. Именно научные роты смогут обеспечить армию высоко интеллектуальными специалистами способными сформировать кибер-щит и кибер-меч для обеспечения информационного суверенитета России.

А необходимость в формировании кибер-щита неоспорима. Так, согласно сведениям приведенным в выступлении специального представителя Президента РФ по вопросам международного сотрудничества в области информационной безопасности А. В. Крутских, только за 2014 год на Россию совершенно 74 миллиона электронных нападений [20]. Это ли не показатель, свидетельствующий о необходимости формирования кибервойск и обеспечения информационной безопасности.

БИБЛИОГРАФИЯ

1. Акопов Г. Л. Глобальные проблемы и опасности сетевой политики. Ростов-на-Дону: РостИздат, 2004;
2. Смирнов А. И. Глобальная безопасность в цифровую эпоху: стратагемы для России. М. 2014. с. 73.
3. Акопов Г. Л. Политико-правовые угрозы распространения социально ориентированных интернет-технологий//Национальная безопасность/nota bene. — 2012. — № 2.
4. Акопов Г. Л. Политический хактивизм — угроза национальной безопасности // Национальная безопасность. — 2011. — № 2.
5. Панарин И. Н. Информационная война и выборы. М.: ОАО «Издательский Дом «Городец»», 2003. — С. 345
6. Доклад Исследовательской службы Конгресса RL30735. Кибервойна. Стивен А. Хилдрет. Размещено на веб сайте Infousa.ru. 20 февраля 2003. {Электронный ресурс}. http://www.infousa.ru/information/bt-1028.htm
7. Страны БРИКС выработают единые подходы в информбезопасности. РИА Новости. 26 мая 2015. {Электронный ресурс}. Доступ: http://ria.ru/world/20150526/1066519380.html#ixzz3cxPWfJSe свободный.
8. Обама и лидер Китая Си Цзиньпин решили выстроить новую модель отношений. {Электронный ресурс}. Доступ http://www.newsru.com/world/08jun2013/obamaxi.html свободный. 08.06.2013.

DOI: 10.7256/2073–8560.2015.4.15834

9. Обама считает проблему борьбы с кибертерроризмом-приоритетной для США. {Электронный ресурс}. Доступ: http://internetua.com/obama-scsitaet-problemu-borbi-s-kiberterrorizmom—-prioritetnoi-dlya-ssha свободный. Дата публикации: 25.01.2012.
10. ФСБ поручено создать антихакерскую систему. Вести. 21 января 2013 года. [Электронный ресурс]. Доступ: http://www.vesti.ru/doc.html?id=1010793 свободный.
11. Хиллари Клинтон пообещала американцам защиту от России. LifeNews. Доступ: http://lifenews.ru/mobile/news/155587 свободный. Дата публикации 14 июня 2015 года.
12. Клинтон: Китай и Россия спонсировали хакеров. Доступ: http://vistanews.ru/politics/13018-klinton-kitay-i-rossiya-sponsirovali-hakerov.html свободный. Дата публикации: 8 июля 2015 года.
13. Акопов, Г. Л. Кибервойска как основа информационной безопасности современного государства //Реклама и связи с общественностью: традиции и инновации: материалы междунар. науч.— практ. конф. (18–19 сент. 2014 г.). РГУПС, 2014. С. 59–67.
14. DDoS-атаку на сайты НАТО устроил «КиберБеркут». НТВ. 16 марта 2014 года. [Электронный ресурс]. Доступ: http://www.ntv.ru/novosti/860377/свободный.
15. Украинские хакеры выложили в сеть переписку представителей партий «Удар» и «Батькивщина». ИТАР-ТАСС. 16 марта 2014 года. [Электронный ресурс]. Доступ: http://itar-tass.com/mezhdunarodnaya-panorama/1050998 свободный.
16. Киберберкут уничтожил систему ЦИК Украины. [Электронный ресурс]. Доступ: http://www.voicesevas.ru/news/yugo-vostok/958-kiberberkut-unichtozhil-sistemu-cik-ukra.html
17. Barnaby F. The Future of Terror. Granta Books. London. 2007.
18. Россия создает кибервойска («Stdaily.com», Китай). [Электронный ресурс]. Доступ: http://topwar.ru/31668-rossiya-sozdaet-kibervoyska-stdailycom-kitay.html свободный. Дата публикации: 8 августа 2013 года.
19. Berq P. Hyacinthe. Cyber Warriors at War. Xlibris Corporation. 2010.
20. Крутских А. В. Ключевые проблемы обеспечения международной информационной безопасности. Инфофорум. 7 июля 2015 года.
21. Коробейников А. Г., Гришенцев А. Ю., Святкина М. Н. Применение интеллектуальных агентов магнитных измерений для мониторинга объектов железнодорожной инфраструктуры // Кибернетика и программирование.— 2013.— 3.— С. 9–20. DOI: 10.7256/2306–4196.2013.3.8737. URL: http://www.e-notabene.ru/kp/article_8737.html
22. Яшина А. В. Информационные технологии и трансформация системы обеспечения безопасности. // Вопросы безопасности.— 2014.— 4.— С. 104–130. DOI: 10.7256/2409–7543.2014.4.13332. URL: http://www.e-notabene.ru/nb/article_13332.html
23. О. Н. Федорова Развитие правового регулирования информационной безопасности России // Политика и Общество.— 2012.— 4.— С. 64–67.
24. Попов В. В. Информация как фактор воздействия на политическую жизнь общества (социокультурный аспект) // Вопросы безопасности.— 2014.— 6.— С. 68–97. DOI: 10.7256/2409–7543.2014.6.13751. URL: http://www.e-notabene.ru/nb/article_13751.html
25. Заводцев И. В., Гайнов А. Е. Разработка механизмов сбора и преобразования формата представления исходной информации для систем мониторинга событий информационной безопасности // Программные системы и вычислительные методы.— 2015.— 1.— С. 21–31. DOI: 10.7256/2305–6061.2015.1.14010.
26. В. П. Хрыков Информационное общество в России: условия и проблемы формирования // Политика и Общество.— 2011.— 6.— С. 18–25.

REFERENCES (TRANSLITERATED)

1. Akopov G. L. Global'nye problemy i opasnosti setevoi politiki. Rostov-na-Donu: RostIzdat, 2004;
2. Cmirnov A. I. Global'naya bezopasnost' v tsifrovuyu epokhu: stratagemy dlya Rossii. M. 2014. s.73.
3. Akopov G. L. Politiko-pravovye ugrozy rasprostraneniya sotsial'no orientirovannykh internet-tekhnologii//Natsional'naya bezopasnost'/nota bene.—2012.—№ 2.

DOI: 10.7256/2073–8560.2015.4.15834

4. Akopov G. L. Politicheskii khaktivizm — ugroza natsional'noi bezopasnosti // Natsional'naya bezopasnost'.— 2011.— № 2.
5. Panarin I. N. Informatsionnaya voina i vybory. M.: OAO 'Izdatel'skii Dom 'Gorodets'', 2003.— S. 345
6. Doklad Issledovatel'skoi sluzhby Kongressa RL30735. Kibervoina. Stiven A. Khildret. Razmeshcheno na veb saite Infousa.ru. 20 fevralya 2003. {Elektronnyi resurs}. http://www.infousa.ru/information/bt-1028.htm
7. Strany BRIKS vyrabotayut edinye podkhody v informbezopasnosti. RIA Novosti. 26 maya 2015. {Elektronnyi resurs}. Dostup: http://ria.ru/world/20150526/1066519380.html#ixzz3cxPWfJSe svobodnyi.
8. Obama i lider Kitaya Si Tszin'pin reshili vystroit' novuyu model' otnoshenii. {Elektronnyi resurs}. Dostup http://www.newsru.com/world/08jun2013/obamaxi.html svobodnyi. 08.06.2013.
9. Obama schitaet problemu bor'by s kiberterrorizmom-prioritetnoi dlya SShA. {Elektronnyi resurs}. Dostup: http://internetua.com/obama-scsitaet-problemu-borbi-s-kiberterrorizmom—-prioritetnoi-dlya-ssha svobodnyi. Data publikatsii: 25.01.2012.
10. FSB porucheno sozdat' antikhakerskuyu sistemu. Vesti. 21 yanvarya 2013 goda. [Elektronnyi resurs]. Dostup: http://www.vesti.ru/doc.html?id=1010793 svobodnyi.
11. Khillari Klinton poobeshchala amerikantsam zashchitu ot Rossii. LifeNews. Dostup: http://lifenews.ru/mobile/news/155587 svobodnyi. Data publikatsii 14 iyunya 2015 goda.
12. Klinton: Kitai i Rossiya sponsirovali khakerov. Dostup: http://vistanews.ru/politics/13018-klinton-kitay-i-rossiya-sponsirovali-hakerov.html svobodnyi. Data publikatsii: 8 iyulya 2015 goda.
13. Akopov, G. L. Kibervoiska kak osnova informatsionnoi bezopasnosti sovremennogo gosudarstva //Reklama i svyazi s obshchestvennost'yu: traditsii i innovatsii: materialy mezhdunar. nauch.— prakt. konf. (18–19 sent. 2014 g.). RGUPS, 2014. S. 59–67.
14. DDoS-ataku na saity NATO ustroil 'KiberBerkut'. NTV. 16 marta 2014 goda. [Elektronnyi resurs]. Dostup: http://www.ntv.ru/novosti/860377/svobodnyi.
15. Ukrainskie khakery vylozhili v set' perepisku predstavitelei partii 'Udar' i 'Bat'kivshchina'. ITAR-TASS. 16 marta 2014 goda. [Elektronnyi resurs]. Dostup: http://itar-tass.com/mezhdunarodnaya-panorama/1050998 svobodnyi.
16. Kiberberkut unichtozhil sistemu TsIK Ukrainy. [Elektronnyi resurs]. Dostup: http://www.voicesevas.ru/news/yugo-vostok/958-kiberberkut-unichtozhil-sistemu-cik-ukra.html
17. Barnaby F. The Future of Terror. Granta Books. London. 2007.
18. Rossiya sozdaet kibervoiska ('Stdaily.com', Kitai). [Elektronnyi resurs]. Dostup: http://topwar.ru/31668-rossiya-sozdaet-kibervoyska-stdailycom-kitay.html svobodnyi. Data publikatsii: 8 avgusta 2013 goda.
19. Berq P. Hyacinthe. Cyber Warriors at War. Xlibris Corporation. 2010.
20. Krutskikh A. V. Klyuchevye problemy obespecheniya mezhdunarodnoi informatsionnoi bezopasnosti. Infoforum. 7 iyulya 2015 goda.
21. Korobeinikov A. G., Grishentsev A. Yu., Svyatkina M. N. Primenenie intellektual'nykh agentov magnitnykh izmerenii dlya monitoringa ob'>ektov zheleznodorozhnoi infrastruktury // Kibernetika i programmirovanie.— 2013.— 3.— C. 9–20. DOI: 10.7256/2306–4196.2013.3.8737. URL: http://www.e-notabene.ru/kp/article_8737.html
22. Yashina A. V. Informatsionnye tekhnologii i transformatsiya sistemy obespecheniya bezopasnosti. // Voprosy bezopasnosti.— 2014.— 4.— C. 104–130. DOI: 10.7256/2409–7543.2014.4.13332. URL: http://www.e-notabene.ru/nb/article_13332.html
23. O. N. Fedorova Razvitie pravovogo regulirovaniya informatsionnoi bezopasnosti Rossii // Politika i Obshchestvo.— 2012.— 4.— C. 64–67.
24. Popov V. V. Informatsiya kak faktor vozdeistviya na politicheskuyu zhizn' obshchestva (sotsiokul'turnyi aspekt) // Voprosy bezopasnosti.— 2014.— 6.— C. 68–97. DOI: 10.7256/2409–7543.2014.6.13751. URL: http://www.e-notabene.ru/nb/article_13751.html

DOI: 10.7256/2073–8560.2015.4.15834

25. Zavodtsev I. V., Gainov A. E. Razrabotka mekhanizmov sbora i preobrazovaniya formata predstavleniya iskhodnoi informatsii dlya sistem monitoringa sobytii informatsionnoi bezopasnosti // Programmnye sistemy i vychislitel'nye metody. — 2015. — 1. — C. 21–31. DOI: 10.7256/2305–6061.2015.1.14010.
26. V. P. Khrykov Informatsionnoe obshchestvo v Rossii: usloviya i problemy formirovaniya // Politika i Obshchestvo. — 2011. — 6. — C. 18–25.

DOI: 10.7256/2073–8560.2015.4.15834