SPIRITUAL LANDMARKS. THREATS AND PARTNERSHIPS IN THE PROVISION OF SPIRITUAL SECURITY OF MODERN YOUTH OF RUSSIA AND UKRAINE

Abstract

The article examines the issues of the state and dynamics of spiritual and cultural development of modern Russian society in the context of threats to national and spiritual safety of the state and the younger generation. We consider the strategy of countering threats to spiritual safety. Particular importance is given to the innovative nature of the Belgorod region as the border with Ukraine. The authors formulate an interesting approach to the national idea in the context of strengthening the spiritual security of modern Russian society.

Keywords: *spiritual security, danger, youth, the national idea.*

References

1. Tojnbi A.Dzh. Postizhenie istorii / Perevod s nemeckogo E.D. Zharkova. M.: Rol'f, 2001. 640 s.
2. Dal' V.I. Tolkovyj slovar' zhivogo velikorusskogo jazyka v 4 t. SPB, 1863-1866 // lingvo – 2004
3. Il'in I.A. Obshhee uchenie o prave i gosudarstve, glava 10, « O patriotizme»// jelektronnaja biblioteka Odincovskogo blagochinija. www. Odinblago.ru
4. Mangejm K. Ideologija i utopija. Diagnoz nashego vremeni. M.: Jurist, 1994. 693 s.
5. Novye religioznye organizacii Rossii destruktivnogo i okkul'tnogo haraktera: spravochnik // Missionerskij otdel Moskovskogo patriarhata russkoj pravoslavnoj cerkvi / Informacionno-analiticheskij vestnik №1. Izd. vtoroe, pererab. i dop. Belgorod, 1997.
6. Hlobustov O.M. Fal'shivka li plan Dallesa? // Obozrevatel'-Observer. 2006. № 1.
7. Lobazova O.F. Religiovedenie. Uchebnik. M.: Dashkov i Ko, 2004. 488 s.
8. Sv. Feofan zatvornik // Mysli na kazhdyj den' – 1887// Azbuka very pravoslavnoj// jelektronnaja biblioteka 2005.
9. Medvedev D.A. Vystuplenie na otkrytii 5-go Krasnojarskogo jekonomicheskogo foruma. 16.02.2008// www. Krasnoforum.ru

УДК 32

ХАКТИВИЗМ – УГРОЗА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННОМ СОЦИУМЕ

Акопов Григорий Леонидович доктор политических наук, профессор, директор, Ростовский филиал Московского государственного технического университета гражданской авиации (344029, Россия, г. Ростов-на-Дону, пр. Шолохова, 262). E-mail: akopovg@pochta.ru

Аннотация

Динамичное информационно-коммуникационное развитие современного общества обусловило столь же динамичное появление информационных угроз. Глобальное развитие интернет-технологий породило явление кибертерроризма. В качестве кибертеррористов могут выступать и так называемые хактивисты. В эпоху политических противостояний, одним из важнейших стратегических направлений государств является противостояние киберугрозам и кибертерроризму.

***Ключевые слова**: интернет, инфокоммуникации, хактивизм, политические коммуникации, кибертерроризм, киберузгроза, кибервойска, хакерские атаки.*

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. Ее 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, с. 73].

И подобных рисков и угроз возникает не мало [3], в данной статье мы считаем необходимым отдельно обозначить опасности превращения хакеров в политических террористов [4] 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, с. 345]. 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]. Примечательно, что еще 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 г. [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].

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 г. и референдума жителей Крымского полуострова, на официальные интернет-ресурсы органов государственной власти, СМИ, крупнейшие бизнес структуры обрушился шквал атак политически ангажированных хакеров – «хактивистов».

Очевидно, с целью дестабилизации экономической обстановки практически одновременно с атакой на сайт Президента РФ, хактивисты атаковали сайт Центрального Банка России [12]. В этот же день хакерам удалось парализовать работу сайта Министерства иностранных дел [13].

Особо рьяно хактивисты взялись за ведущие Российские СМИ; продолжительное время были заблокированы сайты: "Российской газеты", РИА Новости, “ИТАР-ТАСС”, «Лента.ру» [14], "Эксперта", "Русского репортера" [15], Вестей.Ru [16], а сайт «Первого канала» атаковали дважды за один день. Как было сказано на официальной странице "Первого канала" в соцсети "ВКонтакте" причины неполадок объяснили DDoS-атакой из Киева [17].

Атаки на телевизионные каналы не ограничивались воздействием на интернет-порталы телеканалов, телевизионные спутники России также подверглись атаке хакеров. В министерстве связи и массовых коммуникаций России заявили, что имеются сведения, что все атаки совершаются с территории Западной Украины [18]. За несколько дней до обозначенных событий, жертвой хакеров стал сайт телеканала Russia Today. Киберхулиганы взломали портал и добавили слово Nazi (нацист, нацистский) к заголовкам всех статей на английском языке [17].

Непосредственно в ночь на 16 марта 2014 г. хактивистами был атакован сайт крымского референдума Referendum2014.ru. По словам пресс-службы ресурса, речь идет о "DDoS-атаке последнего поколения" [19]. Ряд взломов, осуществленных 12–14 марта 2014 г., сопровождались разглашением, добытой в результате несанкционированного проникновения, информации. Так, например: «Хакерская группировка «Русское киберкомандование» объявила о взломе ИБ-компании SearchInfrom и опубликовала большое количество приписываемых ей документов" [20].

В СМИ прошла информация о хакерских атаках и на иные сайты стратегически значимых предприятий и организаций Российской Федерации.

Важно учесть, что все чаще действия хактивистов, отстаивающих определенные политические идеи, приводят к ответным действия. Так после обозначенных ранее атак на российские интернет-ресурсы, хакерской атаке подверглись сайты НАТО [21]. В тот же день хактивисты выложили в интернет-электронную переписку представителей руководства украинских партий "Удар" и "Батькивщина". Об этом хакеры сообщили на своих страницах "В Контакте" и Facebook [22].

Объединение хактивистов получившее название «КиберБеркут» взломало и уничтожило систему ЦИК Украины [23]. 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 [24].

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 [25].

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» [26].

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.

Литература

1. *Акопов Г.Л.* Глобальные проблемы и опасности сетевой политики. Ростов н/Д.: РостИздат, 2004.
2. *Смирнов А.И.* Глобальная безопасность в цифровую эпоху: стратагемы для России. М., 2014.
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.

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.
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. Сайт Центробанка подвергся хакерской атаке. [Электронный ресурс]. Доступ: http://www.rg.ru/2014/03/14/centrobank-site-anons.html. Дата публикации: 14.03.2014.
13. Сайт МИД РФ не работает, возможно, его атаковали хакеры. [Электронный ресурс]. Доступ: http://www.interfax.ru/russia/364738. Дата публикации: 14.03.2014.
14. Сайт «Ленты.ру» могли атаковать хакеры из Anonymous. [Электронный ресурс]. Доступ:http://rbcdaily.ru/media/562949990837912 свободный. Дата публикации: 14.03.2014.
15. Сайты "Эксперта" и "Русского репортера" стали объектами хакерской атаки. [Электронный ресурс]. Доступ:http://eliberator.ru/news/detail.php?ID=904 свободный. Дата публикации: 11.03.2014.
16. Хакеры атаковали сервер ВГТРК. [Электронный ресурс]. Доступ: http://www.tltnews.ru/rus_news/32/480939/ свободный. Дата публикации: 13.03.2014.
17. Хакеры второй раз за день обрушили сайт "Первого канала". [Электронный ресурс]. Доступ: http://top.rbc.ru/society/13/03/2014/910974.shtml свободный. Дата публикации: 13.03.2014.
18. Спутники России подверглись атаке хакеров из Украины. [Электронный ресурс]. Доступ: http://www.vladtime.ru/internet/362086-sputniki-rossii-podverglis-atake-hakerov-iz-ukrainy.html свободный. Дата публикации: 14.03.2014.
19. Сайт крымского референдума атаковали из США. Российская газета. [Электронный ресурс]. Доступ: http://www.rg.ru/2014/03/16/ref2014-site.html свободный. Дата публикации: 16.03.2014.
20. Поставщик ИБ-решений для «Газпрома», «Русала» и «Сколково» взломан хакерами. Cnews.ru[Электронный ресурс]. Доступ: http://www.cnews.ru/top/2014/03/12/postavshhik_ibresheniy_dlya_gazproma_rusala_i_skolkovo_vzloman_hakerami_564100 свободный. Дата публикации: 12.03.2014.
21. DDoS-атаку на сайты НАТО устроил «КиберБеркут». НТВ. 16 марта 2014 года. [Электронный ресурс]. Доступ: http://www.ntv.ru/novosti/860377/свободный.
22. 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.
23. Киберберкут уничтожил систему ЦИК Украины. [Электронный ресурс]. Доступ: http://www.voicesevas.ru/news/yugo-vostok/958-kiberberkut-unichtozhil-sistemu-cik-ukra.html
24. Barnaby F. The Future of Terror. Granta Books. London. 2007.
25. 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.
26. *Berq P.* Hyacinthe. Cyber Warriors at War. Xlibris Corporation. 2010.

Akopov Grigory Leonidovich, doctor of political sciences, professor, director; Rostov branch of the Moscow state technical university of civil aviation (262, Sholokhov Ave, Rostov-on-Don, 344029, Russian Federation). E-mail: akopovg@pochta.ru

CYBER TROOPS AS THE BASIS OF INFORMATION SECURITY

Abstract

Dynamic info-communicative development of modern society is the cause of different information threats. There is such phenomenon as cyberterrorism in modern information area due to global development of Internet technologies. So-called hactivists are considered to be cyberterrorists. One of the most important strategic directions is confrontation with cyber threats and cyberterrorism in epoch of political oppositions.

Keywords: *hactivism, cyberterrorism, cyber threat, cyber troops, hacker attacks.*

References

1. Akopov G.L. Global'nye problemy i opasnosti setevoj politiki. Rostov n/D.: RostIzdat, 2004.
2. Cmirnov A.I. Global'naja bezopasnost' v cifrovuju jepohu: stratagemy dlja Rossii. M., 2014.
3. Akopov G.L. Politiko-pravovye ugrozy rasprostranenija social'no orientirovannyh internet-tehnologij // Nacional'naja bezopasnost'/nota bene. 2012. № 2.
4. Akopov G.L. Politicheskij haktivizm – ugroza nacional'noj bezopasnosti // Nacional'naja bezopasnost'. 2011. № 2.
5. Panarin I.N. Informacionnaja vojna i vybory. M.: OAO «Izdatel'skij Dom «Gorodec»», 2003.
6. Doklad Issledovatel'skoj sluzhby Kongressa RL30735. Kibervojna. Stiven A. Hildret. Razmeshheno na veb sajte Infousa.ru. 20 fevralja 2003. {Jelektronnyj resurs}. http://www.infousa.ru/information/bt-1028.htm
7. Strany BRIKS vyrabotajut edinye podhody v informbezopasnosti. RIA Novosti. 26 maja 2015. {Jelektronnyj resurs}. Dostup: http://ria.ru/world/20150526/1066519380.html#ixzz3cxPWfJSe svobodnyj.
8. Obama i lider Kitaja Si Czin'pin reshili vystroit' novuju model' otnoshenij. {Jelektronnyj resurs}. Dostup http://www.newsru.com/world/08jun2013/obamaxi.html svobodnyj. 08.06.2013.
9. Obama schitaet problemu bor'by s kiberterrorizmom - prioritetnoj dlja SShA. {Jelektronnyj resurs}. Dostup: http://internetua.com/obama-scsitaet-problemu-borbi-s-kiberterrorizmom---prioritetnoi-dlya-ssha svobodnyj. Data publikacii: 25.01.2012.
10. FSB porucheno sozdat' antihakerskuju sistemu. Vesti. 21 janvarja 2013 goda. [Jelektronnyj resurs]. Dostup: http://www.vesti.ru/doc.html?id=1010793 svobodnyj.
11. Hillari Klinton poobeshhala amerikancam zashhitu ot Rossii. LifeNews. Dostup: http://lifenews.ru/mobile/news/155587 svobodnyj. Data publikacii 14 ijunja 2015 goda.
12. Sajt Centrobanka podvergsja hakerskoj atake. [Jelektronnyj resurs]. Dostup: http://www.rg.ru/2014/03/14/centrobank-site-anons.html. Data publikacii: 14.03.2014.
13. Sajt MID RF ne rabotaet, vozmozhno, ego atakovali hakery. [Jelektronnyj resurs]. Dostup: http://www.interfax.ru/russia/364738. Data publikacii: 14.03.2014.
14. Sajt «Lenty.ru» mogli atakovat' hakery iz Anonymous. [Jelektronnyj resurs]. Dostup:http://rbcdaily.ru/media/562949990837912 svobodnyj. Data publikacii: 14.03.2014.
15. Sajty "Jeksperta" i "Russkogo reportera" stali ob#ektami hakerskoj ataki. [Jelektronnyj resurs]. Dostup:http://eliberator.ru/news/detail.php?ID=904 svobodnyj. Data publikacii: 11.03.2014.
16. Hakery atakovali server VGTRK. [Jelektronnyj resurs]. Dostup: http://www.tltnews.ru/rus_news/32/480939/ svobodnyj. Data publikacii: 13.03.2014.
17. Hakery vtoroj raz za den' obrushili sajt "Pervogo kanala". [Jelektronnyj resurs]. Dostup: http://top.rbc.ru/society/13/03/2014/910974.shtml svobodnyj. Data publikacii: 13.03.2014.
18. Sputniki Rossii podverglis' atake hakerov iz Ukrainy. [Jelektronnyj resurs]. Dostup: http://www.vladtime.ru/internet/362086-sputniki-rossii-podverglis-atake-hakerov-iz-ukrainy.html svobodnyj. Data publikacii: 14.03.2014.
19. Sajt krymskogo referenduma atakovali iz SShA. Rossijskaja gazeta. [Jelektronnyj resurs]. Dostup: http://www.rg.ru/2014/03/16/ref2014-site.html svobodnyj. Data publikacii: 16.03.2014.
20. Postavshhik IB-reshenij dlja «Gazproma», «Rusala» i «Skolkovo» vzloman hakerami. Cnews.ru[Jelektronnyj resurs]. Dostup: http://www.cnews.ru/top/2014/03/12/postavshhik_ibresheniy_dlya_gazproma_rusala_i_skolkovo_vzloman_hakerami_564100 svobodnyj. Data publikacii: 12.03.2014.
21. DDoS-ataku na sajty NATO ustroil «KiberBerkut». NTV. 16 marta 2014 goda. [Jelektronnyj resurs]. Dostup: http://www.ntv.ru/novosti/860377/svobodnyj.
22. Ukrainskie hakery vylozhili v set' perepisku predstavitelej partij "Udar" i "Bat'kivshhina". ITAR-TASS. 16 marta 2014 goda. [Jelektronnyj resurs]. Dostup: http://itar-tass.com/mezhdunarodnaya-panorama/1050998 svobodnyj.
23. Kiberberkut unichtozhil sistemu CIK Ukrainy. [Jelektronnyj resurs]. Dostup: http://www.voicesevas.ru/news/yugo-vostok/958-kiberberkut-unichtozhil-sistemu-cik-ukra.html
24. Barnaby F. The Future of Terror. Granta Books. London. 2007.
25. Rossija sozdaet kibervojska ("Stdaily.com", Kitaj). [Jelektronnyj resurs]. Dostup: http://topwar.ru/31668-rossiya-sozdaet-kibervoyska-stdailycom-kitay.html svobodnyj. Data publikacii: 8 avgusta 2013 goda.
26. Berq P. Hyacinthe. Cyber Warriors at War. Xlibris Corporation. 2010.