DOI: 10.7256/2073-8560.2014.3.11523
При цитировании этой статьи сноска на doi обязательна
Национальная безопасность — № 3(32) • 2014

Акопов Г.Л.

ХАКТИВИЗМ КАК НЕОТЪЕМЛЕМЫЙ ЭЛЕМЕНТ СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ ВОЙН

Аннотация: *Политически ориентированные компьютерные взломщики (хакеры) активизировались в связи с напряжением политической обстановки в Украине. Исследованы действия хактивистов (кибертеррористов) в процессе противостояние Россия — Запад. Анализируются противоправные действия компьютерных взломщиков (хакеров) и политические последствия результатов их деятельности. Обобщен новейший опыт применения кибероружия в политических целях и в контексте информационных войн в международном противостоянии. Обозначены методы противостояния кибертерроризму и политическому хактивизму, учтен зарубежный теоретический и практический опыт противостояния кибертерроризму и хактивизму. Методологические основы исследования предопределяются, с одной стороны, его характером, а с другой – концептуальным подходом и научной позицией автора. Особый акцент делается на контент-анализе СМИ. Определяющими исследовательскими принципами выступают: объективность, системность, всестороннее рассмотрение, историзм. В ходе исследования выявлено, что появились и применяются новые силы и средства информационного противоборства в политических конфликтах и локальных войнах. Назревают реальные угрозы возникновения «кибервойн», особенно, если за дело берутся организованные группы «кибертеррористов», руководимые спецслужбами, либо экстремистскими организациями различного рода.*
Ключевые слова: *Сетевые войны, Киберугроза, Киберактивизм, Политический интернет, Интернет и Политика, Кибербезопасность, Кибертерроризм, Хактивизм, Кибервойска, Информационная война.*

Современное общество все сильнее подвергается информационным угрозам, о потенциальных и реальных опасностях превращения хакеров в политических террористов мы уже писали[1], но развитие политических технологий в современном информационном социуме вынуждает нас вновь вернуться к обозначенной теме.

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»[2].

Совершенно не удивительно, что в период разногласий между Российской Федерацией и США по вопросам смены власти на Украине и референдума жителей Крымского полуострова, на официальные интернет-ресурсы органов государственной власти, СМИ, крупнейшие бизнес структуры обрушился шквал атак политически ангажированных хакеров — «хактивистов». «Хактивизм» как явление имеет ряд определений. Панарин И.Н. в книге «Информационная война и выборы» обозначил «Хактивизм», как «бескорыстное» хакерство в целях политического активизма[3]. Там же автор справедливо утверждал, что современное хакерское движение оказалось, втянуто в игры политиков.

Официальный сайт Президента Российской Федерации подвергается атакам хактивистов практически с момента его создания. «Нынешняя хакерская атака на Kremlin.ru стала самой мощной попыткой дестабилизировать работу ресурса за всю его историю»[4]. И это несмотря на то, что атаки на сайт Президента РФ регулярно происходят вот уже более десяти лет. Так еще, 19 декабря 2003 года, действо-

[1] Подр. см.: Акопов Г.Л. Политический хактивизм — угроза национальной безопасности // Национальная безопасность. — 2011. — № 2.

[2] 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

[3] Панарин И.Н. Информационная война и выборы. М.: ОАО «Издательский Дом «Городец»», 2003. — С. 345.

[4] Сайт президента России атаковали хакеры. [Электронный ресурс]. Доступ: http://www.rg.ru/2014/03/14/kremlin-ddos-site-anons.html. Дата публикации: 14.03.2014.

DOI: 10.7256/2073-8560.2014.3.11523
При цитировании этой статьи сноска на doi обязательна

вавший на тот момент руководитель ФСБ сообщил журналистам следующее: «В истекшем году только на сайт Президента Российской Федерации было осуществлено около 100 тысяч компьютерных атак. Всего же в 2003 году зарегистрированы свыше 730 тысяч атак на интернет-представительства органов государственной власти»[5].

Очевидно, с целью дестабилизации экономической обстановки практически одновременно с атакой на сайт Президента РФ, хактивисты атаковали сайт Центрального Банка России[6]. В этот же день хакерам удалось парализовать работу сайта Министерства иностранных дел[7].

Особо рьяно хактивисты взялись за ведущие Российские СМИ; продолжительное время были заблокированы сайты: «Российской газеты», РИА Новости, "ИТАР-ТАСС", «Лента.ру»[8], "Эксперта", "Русского репортера"[9], Вестей.Ru[10], а сайт «Первого канала» атаковали дважды за один день. Как сказано на официальной странице "Первого канала" в соцсети "ВКонтакте" причины неполадок объяснили DDoS-атакой из Киева[11].

Атаки на телевизионные каналы не ограничивались воздействием на интернет-порталы телеканалов, телевизионные спутники России также подверглись атаке хакеров с территории Западной Украины. В министерстве связи и массовых коммуникаций России заявили, что имеются сведения, что все атаки совершаются с территории Западной Украины[12].

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[13].

Непосредственно в ночь на 16 марта 2014 года, хактивистами был атакован сайт крымского референдума Referendum2014.ru. По словам пресс-службы ресурса, речь идет о "DDoS-атаке последнего поколения"[14].

Ряд взломов, осуществленных 12-14 марта 2014 года, сопровождались разглашением, добытой в результате несанкционированного проникновения, информации. Так, например: «Хакерская группировка «Русское киберкомандование» (Russian Cyber Command) объявила о взломе ИБ-компании SearchInfrom и опубликовала большое количество приписываемых ей документов"[15]. Хакеры намекают "на связь SearchInform с ФСБ и полагают, что продукты этой компании работают «в основных российских инфраструктурных компаниях»: в частности, в «Велес Капитал», «Русал», «Газпром», «Сухой», «Объединенной авиастроительной компании», в корпорации «Иркут» и других"[16].

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

За большинство хакерских атак ответственность на себя взяла Международная хакерская группа Anonymous, которая и раньше нередко брала на

---

[5] Чекисты отразили около 100 тысяч атак на сайт Президента. {Электронный ресурс}. Размещено на: www.strana.ru. 19.12.2003.

[6] Сайт Центробанка подвергся хакерской атаке. [Электронный ресурс]. Доступ: http://www.rg.ru/2014/03/14/centrobank-site-anons.html. Дата публикации: 14.03.2014.

[7] Сайт МИД РФ не работает, возможно, его атаковали хакеры. [Электронный ресурс]. Доступ: http://www.interfax.ru/russia/364738. Дата публикации: 14.03.2014.

[8] Сайт «Ленты.ру» могли атаковать хакеры из Anonymous. [Электронный ресурс]. Доступ: http://rbcdaily.ru/media/562949990837912 свободный. Дата публикации: 14.03.2014.

[9] 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.

[10] Хакеры атаковали сервер ВГТРК. [Электронный ресурс]. Доступ: http://www.tltnews.ru/rus_news/32/480939/ свободный. Дата публикации: 13.03.2014.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] Подр. см.: 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.

[16] Там же.

DOI: 10.7256/2073-8560.2014.3.11523
При цитировании этой статьи сноска на doi обязательна

себя ответственность за интернет-атаки. Anonymous —движение хакеров, выступающее «за свободу Интернета». Хакеры приобрели известность благодаря целому ряду крупных атак. Так, в мае 2012 года организация взяла на себя ответственность за атаку на сайты президента и правительства России. Летом 2011 года хакеры Anonymous распространили в Сети видеообращение, в котором призывали своих сторонников объединиться по всему миру и уничтожить социальную сеть Facebook[17].

Наибольшую известность Anonymous приобрели после ряда хакерских атак в защиту основателя портала «WikiLeaks» Джулиана Ассанжа. В 2010 году по данным NewsInfo[18], портал известной платежной системы MasterCard приостановил свою работу из-за хакерской атаки. Нападение на сайт было совершено в отместку за арест Ассанжа. Кроме того, хакеры обрушились на сайт платежной системы PayPal, отказавшейся принимать пожертвования для WikiLeaks, и на сайт швейцарского банка Swiss Post Office, где были заморожены счета австралийца.

Следует заметить, что первыми от виртуальных мстителей пострадал сайт шведской прокуратуры, которая инициировала преследование основателя WikiLeaks Джулиана Ассанжа по обвинению в изнасиловании, и финансовый сервис Postfinance швейцарской почтовой службы, заморозившей счета Ассанжа[19].

На наш взгляд, атаки на противников Д. Ассанжа, действия против интернет-ресурсов Российской Федерации и ряд иных организованных хакерских атак с политической целью демонстрируют объективную угрозу объединения хакерских групп. Виртуальный социум готов к организованным акциям, и назревает реальная угроза возникновения кибервойны.

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[20]. 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[21].

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[22].

Именно международный терроризм активно использует компьютерные сети в своей деятельности. Об этом, в частности, пишет М. Кастельс во втором томе «Сила идентичности»[23] трилогии «Информационный век — экономика, общество и культура»[24]. Совладать с массовым распространением киберпреступлений сложно, но можно путем принятия всесторонних мер. Прежде всего, необходима четкая и последовательная международная политика по противостоянию кибертеррору. Нужна высококвалифицированная разведка. Особо важна работа правоохранительных органов и вооруженных сил, нацеленная на предотвращение техногенного и кибернетического террора.

Поскольку компьютерный терроризм — уже реальность сегодняшнего дня, необходимо закрепить на законодательном уровне обязанность государственных и частных структур по принятию технических мер, обеспечивающих защиту компьютерных сетей, как одного из наиболее уязвимых элементов современного общества.

Об этом говорят иные специалисты, так в публикации доктора наук Берг Гиацинт «Кибервоины на

---

[17] Сайт «Ленты.ру» могли атаковать хакеры из Anonymous. [Электронный ресурс]. Доступ: http://rbcdaily.ru/media/562949990837912 свободный. Дата публикации: 14.03.2014.

[18] Владельцу WikiLeaks и арест не помеха. {Электронный ресурс}. http://www.newsinfo.ru/articles/2010-12-08/wikileaks/744696/

[19] Хакеры пошли кибер-войной на обидчиков Ассанжа. Правда.Ру. {Электронный ресурс}. Доступно: http://www.pravda.ru/news/world/09-12-2010/1060291-hakeri-0/

[20] Подр. см.: DDoS-атаку на сайты НАТО устроил «КиберБеркут». НТВ. 16 марта 2014 года. [Электронный ресурс]. Доступ: http://www.ntv.ru/novosti/860377/ свободный.

[21] 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.

[22] Barnaby F. The Future of Terror. Granta Books. London. 2007.

[23] Manuel Castells. The Power of Identity: The Information Age — Economy, Society, and Culture: 2. Wiley-Blackwell. U.K. 2010.

[24] Manuel Castells. The Rise of the Network Society: Information Age: Economy, Society, and Culture v. 1. Wiley-Blackwell. U.K. 2010; Manuel Castells. The Power of Identity: The Information Age — Economy, Society, and Culture: 2. Wiley-Blackwell. U.K. 2010; Manuel Castells. End of Millennium: v. 3: The Information Age: Economy, Society, and Culture. Wiley-Blackwell. U.K. 2010.

DOI: 10.7256/2073-8560.2014.3.11523
При цитировании этой статьи сноска на doi обязательна

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»[25].

Вероятно, в ближайшие годы в России придется применить экстренные меры для обеспечения кибербезопасности. И подобные поручения уже прозвучали из уст Президента России 21 января 2013 года, когда В.В. Путин дал поручение ФСБ создать антихакерскую систему[26]. Напомним, что большинство развитых стран уже формируют кибервойска и ведут работу по формированию кибербезопасности. Так в 2011 году, Президент США определил десять экстренных мер необходимых для реализации стратегии кибербезопасности:

1. Учредить подразделения кибер-полиции, отвечающие за обеспечение кибербезопасности.
2. Подготовка для утверждения Президента обновленной национальной стратегии по обеспечению информационной и коммуникационной инфраструктуры.
3. Контроль за кибербезопасностью передать в прямое управление Президента США и установить показатели ее эффективности.
4. Обеспечить конфиденциальность и гражданские свободы в рамках работы национальной секретной службы кибербезопасности.
5. Провести межведомственной нормативно-правовой анализ приоритетных вопросов кибербезопасности.
6. Инициировать национальную информационно-просветительскую кампанию содействия кибербезопасности.
7. Разработка единого международного плана действий по обеспечению кибербезопасности и укрепления наших международных партнеров.
8. Подготовка ответа кибератакам: инициировать план действий и начать диалог для укрепления государственно-частного партнерства.
9. Разработать основу для исследований, направленных на применение новейших технологий, которые способны обеспечить повышение безопасности, надежности и устойчивости работы цифровой инфраструктуры.
10. Принять протокол кибербезопасности на основе стратегии управления и обеспечения конфиденциальности технологий повышения национальной безопасности[27].

На наш взгляд, названные меры необходимо внедрить во всех цивилизованных государствах, т.к. Интернет предоставляет уникальные возможности применения инновационных технологий в «подрывной» деятельности в целях политического воздействия.

Библиография:

1. Подр. см.: Акопов Г.Л. Политический хактивизм — угроза национальной безопасности // Национальная безопасность / nota bene. — 2011. — № 2.
2. 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
3. Панарин И.Н. Информационная война и выборы. М.: ОАО «Издательский Дом «Городец»», 2003. — С. 345.
4. Сайт президента России атаковали хакеры. [Электронный ресурс]. Доступ: http://www.rg.ru/2014/03/14/kremlin-ddos-site-anons.html. Дата публикации: 14.03.2014.
5. Чекисты отразили около 100 тысяч атак на сайт Президента. {Электронный ресурс}. Размещено на: www.strana.ru. 19.12.2003.

[25] См. подр.: Berq P. Hyacinthe. Cyber Warriors at War. Xlibris Corporation. 2010.

[26] ФСБ поручено создать антихакерскую систему. Вести. 21 января 2013 года. [Электронный ресурс]. Доступ: http://www.vesti.ru/doc.html?id=1010793 свободный.

[27] Официальный сайт Президента США. Cybersecurity. 3 апреля 2011. {Электронный ресурс}. Доступ: http://www.whitehouse.gov/administration/eop/nsc/cybersecurity свободный.

6. Сайт Центробанка подвергся хакерской атаке. [Электронный ресурс]. Доступ: http://www.rg.ru/2014/03/14/centrobank-site-anons.html. Дата публикации: 14.03.2014.
7. Сайт МИД РФ не работает, возможно, его атаковали хакеры. [Электронный ресурс]. Доступ: http://www.interfax.ru/russia/364738. Дата публикации: 14.03.2014.
8. Сайт «Ленты.ру» могли атаковать хакеры из Anonymous. [Электронный ресурс]. Доступ: http://rbcdaily.ru/media/562949990837912 свободный. Дата публикации: 14.03.2014.
9. 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.
10. Хакеры атаковали сервер ВГТРК. [Электронный ресурс]. Доступ: http://www.tltnews.ru/rus_news/32/480939/ свободный. Дата публикации: 13.03.2014.
11. 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.
12. 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.
13. 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.
14. Подр. см.: 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.
15. Владельцу WikiLeaks и арест не помеха. {Электронный ресурс}. http://www.newsinfo.ru/articles/2010-12-08/wikileaks/744696/
16. Хакеры пошли кибер-войной на обидчиков Ассанжа. Правда.Ру. {Электронный ресурс}. Доступно: http://www.pravda.ru/news/world/09-12-2010/1060291-hakeri-0/
17. Подр. см.: DDoS-атаку на сайты НАТО устроил «КиберБеркут». НТВ. 16 марта 2014 года. [Электронный ресурс]. Доступ: http://www.ntv.ru/novosti/860377/ свободный.
18. 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.
19. Barnaby F. The Future of Terror. Granta Books. London. 2007.
20. Manuel Castells. The Power of Identity: The Information Age-Economy, Society, and Culture: 2. Wiley-Blackwell. U.K. 2010.
21. Manuel Castells. The Rise of the Network Society: Information Age: Economy, Society, and Culture v. 1. Wiley-Blackwell. U.K. 2010; Manuel Castells. The Power of Identity: The Information Age-Economy, Society, and Culture: 2. Wiley-Blackwell. U.K. 2010; Manuel Castells. End of Millennium: v. 3: The Information Age: Economy, Society, and Culture. Wiley-Blackwell. U.K. 2010.
22. См. подр.: Berq P. Hyacinthe. Cyber Warriors at War. Xlibris Corporation. 2010.
23. ФСБ поручено создать антихакерскую систему. Вести. 21 января 2013 года. [Электронный ресурс]. Доступ: http://www.vesti.ru/doc.html?id=1010793 свободный.
24. Официальный сайт Президента США. Cybersecurity. 3 апреля 2011. {Электронный ресурс}. Доступ: http://www.whitehouse.gov/administration/eop/nsc/cybersecurity свободный.
25. Акопов Г.Л. Хактивизм в процессе информационно-политических конфликтов // NB: Национальная безопасность. — 2014. — 1. — С. 24–32. DOI: 10.7256/2306-0417.2014.1.11609. URL: http://www.e-notabene.ru/nb/article_11609.html
26. Карпович О.Г. Современные концепции и модели управления международными конфликтами (сравнительный политологический анализ) // Национальная безопасность / nota bene. — 2013. — 4. — С. 605–612. DOI: 10.7256/2073-8560.2013.4.6434.
27. Манойло А.В. Управление психологической войной // Международные отношения. — 2013. — 3. — С. 377–389. DOI: 10.7256/2305-560X.2013.3.6221.

28. Валиуллин И.И. Эволюция понятия «информационная война» в политической науке // Международные отношения. — 2014. — 1. — С. 68–74. DOI: 10.7256/2305-560X.2014.1.10064.
29. Курилкин А.В. Современные подходы к ведению информационных войн // Международные отношения. — 2014. — 1. — С. 75–80. DOI: 10.7256/2305-560X.2014.1.10063.
30. М.И. Бения. Восстание машин, или Человек и ковш. // Психология и Психотехника. — 2012. — № 12. — С. 8–22.
31. М. В. Шугуров. «Группа восьми» (G8) и дилеммы глобального управления Интернетом: международно-правовой аспект. // Право и политика. — 2012. — № 6. — С. 1098–1127.
32. Г. Ю. Филимонов, С. А. Цатурян. Социальные сети как инновационный механизм «мягкого» воздействия и управления массовым сознанием. // Политика и Общество. — 2012. — № 1. — С. 65–75.
33. М. В. Шугуров. Совет Европы и информационно-коммуникационные технологии (ICT): реализация прав человека в информационном обществе.. // Международное право и международные организации / International Law and International Organizations. — 2010. — № 4.
34. Горохов В.Г., Сюнтюренко О.В.. Технологические риски: информационные аспекты безопасности общества. // Программные системы и вычислительные методы. — 2013. — № 4. — С. 344–353. DOI: .10.7256/2305-6061.2013.4.970

References:

1. Podr. sm.: Akopov G.L. Politicheskii khaktivizm — ugroza natsional'noi bezopasnosti // Natsional'naya bezopasnost' / nota bene. — 2011. — № 2.
2. 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
3. Panarin I.N. Informatsionnaya voina i vybory. M.: OAO «Izdatel'skii Dom «Gorodets»», 2003. — S. 345.
4. Sait prezidenta Rossii atakovali khakery. [Elektronnyi resurs]. Dostup: http://www.rg.ru/2014/03/14/kremlin-ddos-site-anons.html. Data publikatsii: 14.03.2014.
5. Chekisty otrazili okolo 100 tysyach atak na sait Prezidenta. {Elektronnyi resurs}. Razmeshcheno na: www.strana.ru. 19.12.2003.
6. Sait Tsentrobanka podvergsya khakerskoi atake. [Elektronnyi resurs]. Dostup: http://www.rg.ru/2014/03/14/centrobank-site-anons.html. Data publikatsii: 14.03.2014.
7. Sait MID RF ne rabotaet, vozmozhno, ego atakovali khakery. [Elektronnyi resurs]. Dostup: http://www.interfax.ru/russia/364738. Data publikatsii: 14.03.2014.
8. Sait «Lenty.ru» mogli atakovat' khakery iz Anonymous. [Elektronnyi resurs]. Dostup: http://rbcdaily.ru/media/562949990837912 svobodnyi. Data publikatsii: 14.03.2014.
9. Saity «Eksperta» i «Russkogo reportera» stali ob''ektami khakerskoi ataki. [Elektronnyi resurs]. Dostup: http://eliberator.ru/news/detail.php?ID=904 svobodnyi. Data publikatsii: 11.03.2014.
10. Khakery atakovali server VGTRK. [Elektronnyi resurs]. Dostup: http://www.tltnews.ru/rus_news/32/480939/ svobodnyi. Data publikatsii: 13.03.2014.
11. Khakery vtoroi raz za den' obrushili sait «Pervogo kanala». [Elektronnyi resurs]. Dostup: http://top.rbc.ru/society/13/03/2014/910974.shtml svobodnyi. Data publikatsii: 13.03.2014.
12. Sputniki Rossii podverglis' atake khakerov iz Ukrainy. [Elektronnyi resurs]. Dostup: http://www.vladtime.ru/internet/362086-sputniki-rossii-podverglis-atake-hakerov-iz-ukrainy.html svobodnyi. Data publikatsii: 14.03.2014.
13. Sait krymskogo referenduma atakovali iz SShA. Rossiiskaya gazeta. [Elektronnyi resurs]. Dostup: http://www.rg.ru/2014/03/16/ref2014-site.html svobodnyi. Data publikatsii: 16.03.2014.
14. Podr. sm.: Postavshchik IB-reshenii dlya «Gazproma», «Rusala» i «Skolkovo» vzloman khakerami. Cnews.ru [Elektronnyi resurs]. Dostup: http://www.cnews.ru/top/2014/03/12/postavshhik_ibresheniy_dlya_gazproma_rusala_i_skolkovo_vzloman_hakerami_564100 svobodnyi. Data publikatsii: 12.03.2014.
15. Vladel'tsu WikiLeaks i arest ne pomekha. {Elektronnyi resurs}. http://www.newsinfo.ru/articles/2010-12-08/wikileaks/744696/

16. Khakery poshli kiber-voinoi na obidchikov Assanzha. Pravda.Ru. {Elektronnyi resurs}. Dostupno: http://www.pravda.ru/news/world/09-12-2010/1060291-hakeri-0/
17. Podr. sm.: DDoS-ataku na saity NATO ustroil «KiberBerkut». NTV. 16 marta 2014 goda. [Elektronnyi resurs]. Dostup: http://www.ntv.ru/novosti/860377/ svobodnyi.
18. 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.
19. Barnaby F. The Future of Terror. Granta Books. London. 2007.
20. Manuel Castells. The Power of Identity: The Information Age-Economy, Society, and Culture: 2. Wiley-Blackwell. U.K. 2010.
21. Manuel Castells. The Rise of the Network Society: Information Age: Economy, Society, and Culture v. 1. Wiley-Blackwell. U.K. 2010; Manuel Castells. The Power of Identity: The Information Age-Economy, Society, and Culture: 2. Wiley-Blackwell. U.K. 2010; Manuel Castells. End of Millennium: v. 3: The Information Age: Economy, Society, and Culture. Wiley-Blackwell. U.K. 2010.
22. Sm. podr.: Berq P. Hyacinthe. Cyber Warriors at War. Xlibris Corporation. 2010.
23. FSB porucheno sozdat' antikhakerskuyu sistemu. Vesti. 21 yanvarya 2013 goda. [Elektronnyi resurs]. Dostup: http://www.vesti.ru/doc.html?id=1010793 svobodnyi.
24. Ofitsial'nyi sait Prezidenta SShA. Cybersecurity. 3 aprelya 2011. {Elektronnyi resurs}. Dostup: http://www.whitehouse.gov/administration/eop/nsc/cybersecurity svobodnyi.
25. Akopov G.L. Khaktivizm v protsesse informatsionno-politicheskikh konfliktov // NB: Natsional'naya bezopasnost'. — 2014. — 1. — C. 24–32. DOI: 10.7256/2306-0417.2014.1.11609. URL: http://www.e-notabene.ru/nb/article_11609.html
26. Karpovich O.G. Sovremennye kontseptsii i modeli upravleniya mezhdunarodnymi konfliktami (sravnitel'nyi politologicheskii analiz) // Natsional'naya bezopasnost' / nota bene. — 2013. — 4. — C. 605–612. DOI: 10.7256/2073-8560.2013.4.6434.
27. Manoilo A.V. Upravlenie psikhologicheskoi voinoi // Mezhdunarodnye otnosheniya. — 2013. — 3. — C. 377–389. DOI: 10.7256/2305-560X.2013.3.6221.
28. Valiullin I.I. Evolyutsiya ponyatiya «informatsionnaya voina» v politicheskoi nauke // Mezhdunarodnye otnosheniya. — 2014. — 1. — C. 68–74. DOI: 10.7256/2305-560X.2014.1.10064.
29. Kurilkin A.V. Sovremennye podkhody k vedeniyu informatsionnykh voin // Mezhdunarodnye otnosheniya. — 2014. — 1. — C. 75–80. DOI: 10.7256/2305-560X.2014.1.10063.
30. M.I. Beniya. Vosstanie mashin, ili Chelovek i kovsh. // Psikhologiya i Psikhotekhnika. — 2012. — № 12. — C. 8–22.
31. M. V. Shugurov. «Gruppa vos'mi» (G8) i dilemmy global'nogo upravleniya Internetom: mezhdunarodno-pravovoi aspekt. // Pravo i politika. — 2012. — № 6. — C. 1098–1127.
32. G. Yu. Filimonov, S. A. Tsaturyan. Sotsial'nye seti kak innovatsionnyi mekhanizm «myagkogo» vozdeistviya i upravleniya massovym soznaniem. // Politika i Obshchestvo. — 2012. — № 1. — C. 65–75.
33. M. V. Shugurov. Sovet Evropy i informatsionno-kommunikatsionnye tekhnologii (ICT): realizatsiya prav cheloveka v informatsionnom obshchestve.. // Mezhdunarodnoe pravo i mezhdunarodnye organizatsii / International Law and International Organizations. — 2010. — № 4.
34. Gorokhov V.G., Syuntyurenko O.V.. Tekhnologicheskie riski: informatsionnye aspekty bezopasnosti obshchestva. // Programmnye sistemy i vychislitel'nye metody. — 2013. — № 4. — C. 344–353. DOI: .10.7256/2305-6061.2013.4.970