Либерально-демократические ценности / Journal of liberal democratic values https://liberal-journal.ru

2020, №3-4, Том 4 / 2020, No 3-4, Vol 4 https://liberal-journal.ru/issue-3-4-2020.html

URL статьи: https://liberal-journal.ru/PDF/04KLGK320.pdf

Ссылка для цитирования этой статьи:
Бовтунова А.Я., Битиева З.Р. Киберугрозы КНР и Международное информационное пространство // Либерально-демократические ценности, 2020 №3-4, https://liberal-journal.ru/PDF/04KLGK320.pdf (доступ свободный). Загл. с экрана. Яз. рус., англ.

For citation:
Bovtunova A.Ya., Bitieva Z.R. (2020). China's cyber threats and International information space. *Journal of liberal democratic values*, [online] 3-4(4). Available at: https://liberal-journal.ru/PDF/04KLGK320.pdf (in Russian)

Бовтунова Анастасия Ярославовна
НАНО ВО «Институт мировых цивилизации», Москва, Россия
Факультет «Международных отношений и геополитики»
Студентка 2 курса, направление «Зарубежное регионоведение»
E-mail: n-bovtunova@inbox.ru

Битиева Зарина Руслановна
НАНО ВО «Институт мировых цивилизации», Москва, Россия
Факультет «Международных отношений и геополитики»
Заведующий кафедрой «Мировых цивилизаций и мировой политики»
Кандидат политических наук
E-mail: bitieva1987@gmail.com

Киберугрозы КНР и Международное информационное пространство

Аннотация. Статья посвящена исследованию действий государственных служб по обеспечению внутренней информационной безопасности и противодействию кибератакам, в связи с нарастающим присутствием Китайской Народной Республики в мировом информационном пространстве.

Ключевые слова: информационная безопасность; киберпространство; кибератаки; Китай

Обеспечение кибербезопасности – глобальная проблема, с которой сегодня сталкиваются все страны с прогрессивно-информационными технологиями. Поскольку Китайская Народная Республика является одним из ключевых игроков на международной арене, она подходит к этому вопросу со свойственной ей спецификой, которая значительно отличается от западной. Для недопущения утечки важной государственной информации или проникновения запрещенной информации, Китай предпочел выбрать политику блокирования поисковых систем и некоторых социальных сетей.

При этом число кибератак увеличивается, и мировая статистика[1] за 2019 год лишь подтверждает серьезность проблемы.

[1] Развитие информационных угроз во втором квартале 2019 года. Статистика https://securelist.ru/it-threat-evolution-q2-2019-statistics/94476/?utm_source=telegram&utm_medium=social&utm_campaign=ru_seclistpost_mk0131&utm_content=sm-post&utm_term=ru_telegram__mk0131_sm-post_social_seclistpost.

Тройка лидеров не изменилась по сравнению с 2016 г.[2]: США (23,72 %), Нидерланды (13,89 %), Германия (4,83 %). У США и Германии наблюдается снижение показателя, а у Нидерландов – прирост (+6,98 %).

Показатели Франция (5,95 %) уменьшились на 1,33 пункта, Россия (3,11 %) уменьшились на 7,11 пункта, что переместило страну с четвертого места на пятое.

Масштаб киберугроз невероятный и каждая страна определяет содержание проблемы по-своему.

Информационное противоборство в Китае рассматривается как совокупность действий, которые направлены на защиту собственных информационных систем, а также нейтрализацию систем противника.

Начнем с того, что Интернет в Китае появился в 1994 году. Первый коннект произошел в Институте физики высоких энергий и буквально через несколько лет он стал доступен для крупных компаний и богатейших китайцев.

Спустя четыре года правительство начало задумываться о защите масс от ненужной им информации. Решение этой проблемы заключалось в контроле за распространением ИКТ во все сферы общественной жизни.

Здесь возникла дилемма, ведь, с одной стороны власти не хотели терять контроль над ситуацией в стране, но с другой – перед ними остро стояли задачи экономической модернизации и внедрения передовых технологий.

И глобальная сеть – это как раз технология, которая могла бы максимально упростить работу государственных институтов и создать своего рода виртуальную систему управления китайским обществом [14].

В настоящее время Интернет в Китае очень популярен: в апреле 2020 года количество пользователей в стране впервые превысило 900 миллионов человек[3].

Но возможность свободного доступа породила большое количество дезинформации, что вынудило специальные органы КНР отсеивать информацию, содержащую потенциальную угрозу населению.

Как следствие в 2003 году была запущена система «Золотой Щит». Эта программа является эффективным инструментом борьбы с терроризмом и кибертерроризмом. Под кибертерроризмом следует понимать использование сети Интернет как способ и средство совершения теракта, а также вербовка новых членов в террористические организации, либо осуществление связи между существующими группами. Блокировка такого контента производится по ключевым словам и по черным спискам. В настоящий момент идет переход от черных списков к белым. Это означает, что сейчас китайцы могут зайти на любой незаблокированный сайт, а в будущем смогут посещать только разрешенные ресурсы.

На Wikipedia есть список популярных сайтов, заблокированных «Золотым Щитом». Среди них Google, Facebook, Instagram, Twitter и другие социальные ресурсы, без которых современная молодёжь трудно представляет свою жизнь.

[2] Развитие информационных угроз во втором квартале 2016 года. Статистика https://securelist.ru/it-threat-evolution-in-q2-2016-statistics/29062/.

[3] https://tass.ru/obschestvo/834967.

04KLGK320
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

На «Golden Shield» - это не только про блокировки. Это комплексная система безопасности с аутентификацией по паспорту, антивирусными системами, мониторингами «вторжений» и даже системами распознавания лиц и эмоций.

Все это интегрировано в единый центр на базе Министерства безопасности КНР, что позволяет в кратчайшие сроки находить людей, преступающих закон.

Суммы, потраченные на разработку, естественно хранятся в секрете, но по размаху заметно, что речь идет о сотнях миллионов.

Для управления населением используются следующие технические методики:

- устранения анонимности;
- персонификация граждан;
- оценка поведения граждан;
- фильтрация информационного потока;
- цензура.

Эти правила помогают властям без особой сложности определить авторов всех постов и публикаций, во всей сети Интернет в КНР, а также собирать информацию о всех действиях граждан.

Все это помогает усовершенствовать внутреннюю систему контроля населения.

Но все эти меры не могут защитить от внешних киберугроз, поэтому число хакерских атак постоянно увеличивается. Разработка системы реагирования на кибератаки была необходима благодаря отчетливому пониманию уровня мировой киберпреступности[4].

США и Китай – крупнейшие торговые партнеры, поэтому часто становятся объектами масштабных кибернетических нападений. Кибербезопасность долго оставалась за пределами официальных переговоров властей США и Китая, а шел только на уровне экспертов. И только в последнее время государства начали обсуждать взаимоотношения в киберпространстве на двусторонних и многосторонних переговорах.

Например, Белый дом считает, что именно Китай представляет наибольшую угрозу информационному пространству США, поскольку одним из направлений киберполитики Поднебесной может быть вмешательства в систему противоракетной обороны, управления спутниками и другие.

Но китайцы прекрасно понимают, что безопасность их информационных систем недостаточно уникальна и сильно уязвима для киберстратегий ведущих мировых держав и в случае конфронтации с США их армия и вооружения не смогут долго сопротивляться, несмотря на то, что в наши дни Китай считается экономическим монстром.

Помимо Штатов, в кибермахинациях Китай обвиняют и другие страны. Так Южная Корея до сих пор винит Поднебесную в выводе из-под контроля нескольких банков и телеканалов, а Евросоюз ввел санкции из-за якобы проведенных кибератак WannaCry, NotPetya Cloud Hopper.

В свою очередь, Китай либо никак не комментирует подобные заявления, либо все отрицает, но старается поддерживать равновесие с другими государствами. Власти разрабатывают инструменты, необходимые для выведения инструменты, необходимые для

[4] Facenews. Китай является жертвой американских атак – китайский доклад. URL: https://www.facenews.ua/articles/2013/104539/ (дата обращения: 31.10.2020).

04KLGK320
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

выведения из строя всей информации системы противника, в случае нападения на них. Также эти инструменты помогают решать внутренние конфликты.

Но главный недостаток КНР – неспособность самостоятельно новые технологии.

Это скорее умело скопированные и усовершенствованные разработки. Однако в последнее время данное направление стало приоритетным, благодаря Государственной стратегической программе инновационного развития Китая [13].

Здесь содержаться важные положения по развитию киберпространства и обеспечению безопасности его инноваций. Эта модель базируется на строгом соблюдении национальных интересов и расширении научно-технической базы страны.

Кроме того, Китай инвестирует в собственные веб-технологии, которые направлены на создание поисковых платформ и социальных сетей, а также создает определенный имидж страны в глазах иностранных наблюдателей.

На сегодняшний день Китай заключил договоры о кибербезопасности с рядом ведущих стран, как Россия, США, Великобритания, где обязуется сотрудничать и предотвращать любые киберугрозы и кибершпионаж.

Это означает, что Китай воспринимают как сильного противника на международной арене, который способен поднять мировую безопасность на новый уровень.

Одним словом, можно сказать, что на данный момент главным приоритетом национальной безопасности Китайской Народной Республики является решение проблем компьютерных угроз, поэтому особенностью китайского интернета является четкое регулирование не только технических и организационных практик, но и поведения пользователей в виртуальном пространстве. Такие меры должны позволить минимизировать утечку информации и обеспечить полный контроль за деятельностью пользователей в сети.

Кроме того, благодаря достижению лидерства на мировой арене, Китаю становится все сложнее скрывать свою непричастность к активной радиоэлектронной разведке и шпионажу в киберпространстве других государств.

В целях расширения возможностей киберпространства Китая, страны Азиатско-Тихоокеанского региона активно сотрудничают с коммерческими организациями и образовательными учреждениями, облегчая доступ к передовым исследованиям и технологиям, в том числе военным и телекоммуникационным системам двойного назначения.

Снижение зависимости от западных информационно-коммуникационных технологий и развитие собственного инновационного потенциала считаются важными средствами обеспечения кибербезопасности Китая.

ЛИТЕРАТУРА

1. Веб-монитор в реальном времени от Akamai. [Электронный ресурс] URL: https://www.akamai.com/us/en/solutions/intelligent-platform/visualizingakamai/real-time-web-monitor.jsp (дата посещения: 31.10.2020).
2. Rambler News Service. Китай представил стратегию по кибербезопасности. [Электронный ресурс] URL: https://rns.online/internet/Kitai-predstavil-strategiyu-po-kiberbezopasnosti-2016-12-27/ (дата посещения: 31.10.2020).

3. Либицки М. Информационная война XXI века и третье смещение стратегии Вашингтона, D.C. National Defense University Press, 1995. [Электронный ресурс] URL: http://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly82/Article/793229/twenty-first-century-information-warfare-and-the-third-offsetstrategy/ (дата посещения: 31.10.2020).
4. Интернет в Китае. [Электронный ресурс] URL: http://www.bizhit.ru/index/www_word_users_kitaj/0-175 (дата посещения: 31.10.2020).
5. Facenews. Китай является жертвой американских атак – китайский доклад. [Электронный ресурс] URL: https://www.facenews.ua/articles/2013/104539/ (дата посещения: 31.10.2020).
6. International organizations and conflict resolution: a Textbook / Editors T.A. Zakaurtseva, T.V. Kashirina, Moscow: ITK Dashkov and K, 2017. – 188 p. (accessed 31.10.2020).
7. Kaspersky Security Bulletin 2019 // Kaspersky Security Lab. URL: https://securelist.ru/files/2019/12/Kaspersky-Security-Bulletin2019_FINAL_RUS.pdf (accessed 31.10.2020).
8. Segal A. Is China a Paper Tiger in Cyberspace? Council on Foreign Relations. 2012, URL: http://blogs.cfr.org/asia/2012/02/08/is-china-a-paper-tiger-in-cyberspace/ (accessed 31.10.2020).
9. Ибрагимова Г. Стратегия КНР в киберпространстве: вопросы управления Интернетом и обеспечения информационной безопасности // С. 169–184.
10. Международные организации и урегулирование конфликтов: Учебное пособие / Отв. редакторы Т.А. Закаурцева, Т.В. Каширина. - М.: ИТК «Дашков и К», 2017. – 188 с.
11. Kaspersky Security Bulletin 2019 // Лаборатория Касперского. [Электронный ресурс] URL: https://securelist.ru/files/2019/12/Kaspersky-Security-Bulletin2019_FINAL_RUS.pdf (дата посещения: 31.10.2020).
12. Сигал А. Является ли Китай бумажным тигром в киберпространстве? Совет по международным отношениям. 2012, 8 февраля. [Электронный ресурс] URL: http://blogs.cfr.org/asia/2012/02/08/is-china-a-paper-tiger-in-cyberspace/ (дата посещения: 31.10.2020).
13. Афанасьева Е.В. Современная китайская цивилизация в условиях формирования новых трендов политических изменений в мире. В сборнике: Россия и мир: развитие цивилизаций. Трансформация политических ландшафтов за период 1999–2019 годы. Материалы IX международной научно-практической конференции: в 2-х частях. 2019. С. 15–20.
14. Афанасьева Е.В., Слоботчиков О.Н., Чернышов Б.А. Мирно-военные процессы в истории и действительности жизни цивилизаций. Вестник Института мировых цивилизаций. 2020. Т. 11. № 2 (27). С. 7–16.

04KLGK320
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

Bovtunova Anastasiya Yaroslavovna
Institute of world civilizations, Moscow, Russia
E-mail: n-bovtunova@inbox.ru

Bitieva Zarina Ruslanovna
Institute of world civilizations, Moscow, Russia
E-mail: bitieva1987@gmail.com

China's cyber threats and International information space

Abstract. The article deals with the investigation of the actions of state services to ensure internal information security and counteract cyber attacks, in connection with the growing presence of the people's Republic of China in the global information space.

Keywords: information security; cyberspace; cyberattacks; China

REFERENCES

1. Beb-monitop v peal′nom vremeni ot Akamai. [Ehlektronnyy pesurs] URL: https://www.akamai.com/us/en/solutions/intelligent-platform/visualizingakamai/real-time-web-monitor.jsp (data poseshcheniya: 31.10.2020).
2. Rambler News Service. Kitay ppedstavil ctrategiyu po kiberbezopasnosti. [Ehlektponnyy pesurs] URL: https://rns.online/internet/Kitai-predstavil-strategiyu-po-kiberbezopasnosti-2016-12-27/ (data poseshcheniya: 31.10.2020).
3. Libitski M. Informatsionnaya voyna XXI veka i tret′e smeshchenie stpategii Vashingtona, D.C. National Defense University Press, 1995. [Ehlektronnyy resurs] URL: http://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly82/Article/793229/twenty-first-century-information-warfare-and-the-third-offsetstrategy/ (data poseshcheniya: 31.10.2020).
4. Internet v Kitae. [Ehlektponnyy pesurs] URL: http://www.bizhit.ru/index/www_word_users_kitaj/0-175 (data poseshcheniya: 31.10.2020).
5. Fasenews. Kitay yavlyaetsya zhertvoy amerikanskikh atak – kitayskiy doklad. [Ehlektronnyy resurs] URL: https://www.facenews.ua/articles/2013/104539/ (data poseshcheniya: 31.10.2020).
6. International organizations and conflict resolution: a Textbook / Editors T.A. Zakaurtseva, T.V. Kashirina, Moscow: ITK Dashkov and K, 2017. – 188 p. (accessed 31.10.2020).
7. Kaspersky Security Bulletin 2019 // Kaspersky Security Lab. URL: https://securelist.ru/files/2019/12/Kaspersky-Security-Bulletin2019_FINAL_RUS.pdf (accessed 31.10.2020).
8. Segal A. Is China a Paper Tiger in Cyberspace? Council on Foreign Relations. 2012, URL: http://blogs.cfr.org/asia/2012/02/08/is-china-a-paper-tiger-in-cyberspace/ (accessed 31.10.2020).
9. Ibragimova G. Strategiya KNR v kiberprostranstve: voprosy upravleniya Internetom i obespecheniya informatsionnoy bezopasnosti // S. 169–184.

10. Mezhdunarodnye organizatsii i uregulirovanie konfliktov: Uchebnoe posobie / Otv. redaktory T.A. Zakaurtseva, T.V. Kashirina. - M.: ITK «Dashkov i K», 2017. – 188 c.
11. Kaspersku Sesurity Vulletin 2019 // Laboratoriya Kasperskogo. [Ehlektronnyy resurs] URL: https://securelist.ru/files/2019/12/Kaspersky-Sesurity-Bulletin2019_FINAL_RUS.pdf (data poseshcheniya: 31.10.2020).
12. Cigal A. Yavlyaetsya li Kitay bumazhnym tigrom v kiberprostranstve? Sovet po mezhdunarodnym otnosheniyam. 2012, 8 fevralya. [Ehlektronnyy resurs] URL: http://blogs.cfr.org/asia/2012/02/08/is-china-a-paper-tiger-in-cyberspace/ (data poseshcheniya: 31.10.2020).
13. Afanas′eva E.V. Sovremennaya kitayskaya tsivilizatsiya v usloviyakh formirovaniya novykh trendov politicheskikh izmeneniy v mire. V sbornike: Rossiya i mir: razvitie tsivilizatsiy. Transformatsiya politicheskikh landshaftov za period 1999–2019 gody. Materialy IX mezhdunarodnoy nauchno-prakticheskoy konferentsii: v 2-kh chastyakh. 2019. S. 15–20.
14. Afanas′eva E.V., Slobotchikov O.N., Chernyshov B.A. Mirno-voennye protsessy v istorii i deystvitel′nosti zhizni tsivilizatsiy. Vestnik Instituta mirovykh tsivilizatsiy. 2020. T. 11. № 2 (27). S. 7–16.

04KLGK320
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com