УДК 94
ББК 63.3(7)

РАЗВИТИЕ ПОНЯТИЯ «КИБЕРВОЙНА» В СТРАТЕГИЯХ БЕЗОПАСНОСТИ США ПОСЛЕ 11 СЕНТЯБРЯ (2001–2018)

Сейед Асгар Кейван Хоссейни, Мохаммад Юсоф-ванд

Аннотация. *Появление новых проблем в киберзоне ставит под угрозу безопасность многих правительственных и неправительственных субъектов. Кибертерроризм, кибервойна, кибершпионаж и т.п. — новые темы на арене национальной безопасности, которые приводят к ограничению и угрозе национальному суверенитету и разрушению жизненно важных инфраструктур. Соединенные Штаты Америки являются одной из основных стран, фундаментальная инфраструктура которых полностью встроена в киберпространство, и в этом отношении они больше всех влияют и при этом подвергаются наиболее серьезному влиянию на мировой арене. Настоящее исследование направлено на изучение статуса кибервойн и связанных с ними механизмов безопасности в стратегии безопасности трех правительств США — Джорджа Буша-младшего, Барака Обамы и Дональда Трампа. Ключевой вопрос статьи заключается в том, как в рамках американской стратегии безопасности после 11 сентября изменилось понятие кибервойны и соответствующих инициатив по безопасности? Авторы приходят к выводу, что в процессе ведения политики кибервойны США предприняли три шага: в эпоху Буша заметна попытка «первых шагов по формированию политики кибербезопасности», в руководстве Обамы была сформулирована политика «киберсдерживания», в правление Трампа в центре внимания находится «отход от прошлого на основе всестороннего превосходства».*

Ключевые слова: *кибервойна / кибербезопасность, стратегии безопасности США, политика кибербезопасности, киберсдерживания.*

DEVELOPMENT OF THE CONCEPT "CYBER WAR" IN US SECURITY STRATEGIES AFTER SEPTEMBER 11 (2001–2018)

Seyed Asgar Keivan Hosseini, Mohammad Yusof-vand

Abstract. *The emergence of new problems in the cyber zone threatens the security of many governmental and non-governmental actors. Cyber terrorism, cyber warfare, cyber espionage, all these are new topics in the national security arena that lead to the restriction and threat to the national sovereignty and the destruction of the vital infrastructures of different countries. The United States of America is one of the main countries whose fundamental infrastructure is fully integrated into cyberspace, and in this respect, it is most influential and at the same time, most seriously affected on the world stage. This study aims to examine the status of cyber warfare and related security mechanisms in the security strategy of the three US governments, George W. Bush, Barack Obama, and Donald Trump. The key question of the article is how, in the framework of the American security strategy, the category of cyber warfare and related security initiatives changed after September 11th. The authors conclude that in the process of conducting a cyber war policy, the United States took three steps: in the Bush era, an attempt was made to "the first steps to formulate a cybersecurity policy", the policy of "cyber containment" was formulated in the Obama leadership, in Trump's rule, the focus is on "moving away from past based on overall superiority.*

Keywords: *cyber warfare/cybersecurity, US security strategies, cybersecurity policy, cyber containment.*

Введение

В XXI веке, который также назвали веком информационной (коммуникационной) революции, киберпространство занимает особое место. В этой ситуации некоторые страны используют концепцию «цифровых обществ» для описания последствий такого рода технологических изменений. Эффективность в сфере безопасности в данном случае имеет высокую важность, так как может привести к изменению позиции негосударственных субъектов и размыванию границ суверенных государств [1]. В американской системе принятия решений по вопросам безопасности особое развитие получило включение кибернетических возможностей в Стратегию безопасности, особенно после инцидентов 11 сентября. Ключевой вопрос статьи заключается в осмыслении того, как в рамках американской стратегии безопасности после 11 сентября изменилась отношение к кибервойне и соответствующим инициативам по безопасности.

1. Концептуальная модель: кибервойна

Существуют различные определения понятия «кибервойна». Некоторые считают, что это война, которую ведут правительства, как клю-

чевые игроки, чтобы уничтожить объекты, возможности и сильные стороны врага. Важно то, что в этом типе конфликта конечная цель состоит в том, чтобы враг сдался посредством мобилизации кибер-армии, неправительственных субъектов или даже хакеров и отдельных лиц. Но все же главным и ведущим игроками остаются правительства [2, p. 99–113]. Корпорация Рэнд определяет кибервойну как «борьбу правительств и международных организаций против других правительств, направленную на уничтожение информационной и компьютерной сети». Эти атаки включают вирусы, трояны и другие вредоносные программы [3]. Нужно отметить, что ни одно из приведенных определений не согласовано экспертами разных стран и четкое определение «кибервойны» отсутствует до сих пор. Оно должно быть описано как сложное и неясное понятие, не имеющее необходимого всеобъемлющего содержания относительно его аспектов и функций [4]. Одна из причин возникновения «естественной неясности» связана с его новизной, другая — с «неизменностью традиционного восприятия» вопроса войны, которое по-прежнему уделяет особое внимание военным вопросам и насильственному использованию военного потенциала. Одна из отличительных черт традиционной концепции войны и кибератаки может рассматриваться в таких терминах и понятиях, как враг, друг, союз, коалиция, фронт, начало и конец войны и т.д., в то время как все они в области кибервойн носят, скорее, метафорический, чем реальный характер [5, p. 170–182). Экспертами отмечается также неопределенность, связанная с идентификацией силы вторжения [6, p. 1].

2. Джордж Буш-младший; первые шаги по определению инициативы «политики кибербезопасности»

Чувствительность Буша к безопасности и кибервойне заметна уже во время его избирательных кампаний [7, p. 22–25]. Но самым ярким событием, повлиявшим на актуализацию данного понятия, можно считать события 11 сентября 2001 г. Несомненно, этот инцидент следует рассматривать как поворотный момент во внешней политике и соображениях безопасности США в условиях, значительно отличающихся на макрополитическом уровне от последнего десятилетия XX века. В результате был сформулирован подход, который предписывал «транснациональные реакции на транснациональный характер угроз» [8, p. 134–136], а киберпространство стало рассматриваться как нервная система США и центр ее управления [9, p. vii–ix]. Буш также подписал Национальную директиву, в которой указал время и способы проведения кибератак против компьютерных сетей противника [10]. Другом шагом американского президента стало «создание управления кибербезопасностью» в Белом доме [11, p. 3]. Третьим — возложение различных обязанностей в области кибербезопасности на Министерство внутренней безопасности [9, p. x]. Указ Буша о разработке «Национальной стратегии безопасности киберпространства» стал еще одним актом, принятым в феврале 2003 г. [12, p. 50]. Некоторые исследователи утверждают,

что этот акт был показателем того, насколько важным стало управление киберпространством в литературе по безопасности США [13, p. 13].

Наряду с приведенным выше особо следует отметить еще три документа, которые были опубликованы соответствующими органами в период с 2006 по 2008 год. Во-первых, речь идет о «Национальной военной стратегии операций в киберпространстве», представленной Минобороны США в декабре 2006 г. Данный документ подчеркивает роль Минобороны в «интеграции оборонительных и наступательных кибернетических операций» [14, p. vii]. Во-вторых, о «Национальной стратегия внутренней безопасности», предъявленной в 2007 г. В документе отмечается «Угроза окружающей среды» для Соединенных Штатов из-за асимметричного характера террористических нападений [15, p. 21]. В-третьих, о представленном в январе 2008 г. документе под названием «Комплексная национальная инициатива по кибербезопасности», включающем 12 целей, в том числе «Определение и разработку стратегий и программ устойчивого предупреждения» [16, p. 6].

В целом можно сказать, что во время руководства Буша возникали инновационные инициативы по работе с киберпространством. Укрепляя альянсы и международные союзы для борьбы с терроризмом, президент готовил НАТО к противодействию новым угрозам XXI века. В этом отношении он указал на необходимость укрепления кибер-инфраструктуры НАТО. Следует отметить и приоритетность «Комплексной политики кибербезопасности» в качестве нового подхода к борьбе с террористическими атаками [17, p. 2].

3. Барак Обама: эпоха реализации «киберсдерживания»

Масштабныя переориентация Обамы под названием «перемены» стала поводом для пересмотра американской политики безопасности. На самом деле, хотя стратегия «борьбы с терроризмом» по-прежнему занимала центральное место в повестке дня военной безопасности его правительства, по разным причинам (энтузиазм местной элиты в отношении изменения внешнего направления; трансформации международной обстановки, особенно с появлением новых очагов угроз; и, наконец, отношение Обамы к международным явлениям и его восприятие их модели взаимосвязанности) постепенно начали материализовывать изменения в его понимании политики безопасности, особенно в области кибербезопасности. Действия этого президента, направленные на решение проблем в области кибербезопасности в период руководства Обамы, могут быть определены по следующим осям.

А. Модернизация политики безопасности в связи с киберугрозами

Первая позиция Обамы относительно связи киберпространства и национальной безопасности в мае 2009 года подчеркивала, что цифровая инфраструктура США является своего рода стратегическим национальным достоянием, и на этой основе «киберсдерживание» в военной политике нового правительства стало более эффективным в борьбе за кибербезопасность [18]. Концепция была включена в документ «Международная стратегия кибербезопасности 2011». Впоследствии Обама под-

черкнул концепцию «коллективного сдерживания», в которой подчеркивалась необходимость реализации международного сотрудничества в борьбе для устранения указанных угроз [19, p. 12].

Б. Работа по нормализации международных отношений

Первые признаки ориентации на международную нормализацию как подход к борьбе с киберугрозами обнаруживаются во введении к документу «Комплексной национальной инициативы по кибербезопасности», который был опубликован в 2010 году [20]. Этот тренд можно проследить в «Международной стратегии для киберпространства», где она относится к «Нормализации в рамках Устава ООН», так что действия правительства в этом отношении регулируются и поддерживаются верховенством права [19, p. 8]. Необходимо также упомянуть о таком документе, как «Киберстратегии министерства обороны США» (2015), в котором, помимо проблемы нормализации и укрепления доверия, четко прописано возможность применения карательных и наступательных мер [21, p. 2].

В. Угроза применения «взаимных действий» против угрожающих лиц

Глава американского разведывательного сообщества в рамках доклада Сенату заявил, что киберпространство из экономической возможности превратилась в «угрозу безопасности» интересам правительства в период с 2010 по 2016 год, в то время как до этого главной угрозой считался терроризм. Документ «Стратегии безопасности киберпространства» (2015) впервые признал использование агрессивных действий и контрмер в киберпространстве относительно враждебных государственных и негосударственных субъектов [21, p. 12]. В этом отношении привлекает внимание желание США наладить сотрудничество с такими потенциальными соперниками, как Китай и Россия, с целью взаимного сдерживания угроз, связанных с нарушением кибербезопасности.

Что касается Китая, то следует отметить, что, хотя для руководств безопасности и обороны США это правительство считалось одной из основных баз нападения на США в киберпространстве, напряженность между ними постепенно ослабла до такой степени, что в ходе поездки в Соединенные Штаты китайского президента Си Цзиньпина в сентябре 2015 года была достигнута договоренность, что оба правительства будут избегать преднамеренной поддержки кибератаки в интеллектуальную собственность [22]. Аналогично развивались в этом вопросе и отношения с Россией. В американской оценке глобальных угроз 2012 года она (наряду с Китаем) была названа главной заботой США в киберпространстве, тем не менее, после встречи 5 сентября 2016 года с Владимиром Путиным Обама заявил о нежелании предпринимать меры против этой страны [23]. Однако ослабление дружеских отношений и некоторые события тех лет побудили Обаму принять санкции против России по обвинению в кибератаках на Центральный комитет Демократической партии и преследовании американских дипломатов. Вслед за этим последовало увольнение 35 российских дипломатов из США [24].

4. Дональд Трамп: радикальный разрыв с прошлым и широкомасштабное продвижение кибербезопасности

После прихода Дональда Трампа американская внешняя политика приняла инновационную ориентацию. Ключевым ее моментом стал принцип «Америка превыше всего», который означал перенесение внимания от сотрудничества с внешним миром на сами Соединенные Штаты. Присущие ему атрибуты лидерства, сильно связанные с его индивидуальными особенностями (странная экстраверсия) и восприятием окружающей среды, способствовали появлению новой модели принятия решений, направленной для обеспечения превосходства США. Одним из ее проявлений можно считать его отношение к вопросам кибервойны. В этой связи можно ссылаться на позиции Трампа в избирательной кампании 2016 года, в частности, на его обещания сформировать «группу киберобзора» [25]. В своем первом публичном выступлении Трамп подчеркнул, что у него на повестке дня есть комплексный проект по защите жизненно важной инфраструктуры США против кибератак [26]. Данный подход показал, что этот тип безопасности (кибербезопасность) имеет онтологическое или экзистенциальное значение для США и поэтому его можно охарактеризовать как «радикальный разрыв» от кибернетического подхода Обамы [27]. В документе «Стратегия национальной безопасности» (декабрь 2017 г.) также подчеркивается связь между кибербезопасностью и экономическим процветанием и настаивается на необходимости инвестировать в потенциал быстрого реагирования против кибератак. Однако, не было предъявлено никаких предложений, как выиграть такого рода войну [28, p. 21]. Также можно увидеть настойчивое требование в отношении кибербезопасности в стратегическом документе «Стратегия национальной кибербезопасности США». Важным является следующие вопросы повестки дня для достижения превосходства Америки в киберпространстве:

- защита граждан, родины и американского образа жизни;
- повышение экономического процветания;
- достижение мира вместе с силой и сдерживанием;
- усиление проникновения и влияния США на международной арене.

В документе «Кибер-стратегия Министерства обороны» от 18 сентября 2018 года подчеркивается, что цифровая эра создала проблемы для Министерства обороны США и американского народа, в частности, усугубила угрозу, создаваемую соперниками, воздерживающимися от вооруженного конфликта с Соединенными Штатами и их союзниками. Этот вопрос до сих пор остается открытым. Важный момент заключается в том, что в основе документа лежат «стратегическое соперничество великих держав» и «готовность к войне» [29, p. 1]. Некоторые эксперты считают этот документ более рискованным и агрессивным, чем предыдущий, так как он обеспечивает больше пространства для маневров армии и ответных реакций [30].

Заключение

Одной из определяющих особенностей стратегии безопасности является выявление новых угроз и разра-

ботка подходящих и эффективных ответных действий. Это правило всегда имело первостепенное значение в американской среде при принятии решений по вопросам безопасности. После инцидентов 11 сентября прогнозирование изменение состояния мира, в том числе с связи с переходом от традиционных военных угроз к другим типам угроз, а также возможность невоенного характера будущих войн стали предлогом для разработки системных мер по противодействию киберугрозам. Эта разработка привела, как минимум, к трем шагам по «ведению политики кибербезопасности», предпринятым на протяжении последних пятнадцати лет. Между тем, огромный объем соответствующих документов и включенных в них новшеств поставили новые задачи. Похоже, что в поисках согласования между «растущим темпом кибертехнологий», «динамичным потоком киберугроз» и «восприятием лидерами США кибербезопасности и соответствующей ему политики» правительства этой страны все более четко и строго воспринимают вопросы кибервойны / кибербезопасности, а также пространство мышления в сфере безопасности, что требует внимательного исследования.

СПИСОК ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

1. Drezner, McQuade, Singh, Ford, McLeary, Zenko, Walt and Boot. I'm cyber-confused // Foreign Policy. 2017. URL: http://foreignpolicy.com/2013/02/04/im-cyber-confused/ (accessed: 27.10.2017).
2. *Lee, D.* China dismisses U.S. accusations of cyber-spying // Los Angeles Times. 2013. URL: http://articles.latimes.com/2013/may/07/world/la-fg-wn-china-us-cyber-spying-20130507 (accessed: 19.11.2017).
3. Rand.org. Cyber Warfare. 2019. URL: https://www.rand.org/topics/cyber-warfare.html (accessed: 10.05.2019).
4. *Clarke, R.* War From Cyberspace. 2009. URL: http://users.clas.ufl.edu/zselden/courseread ing2011/Clarkecyber.pdf (accessed: 10.05.2019).
5. *Libicki, M.* Cyberdeterrence and Cyberwar. 2009. URL: https://www.rand.org/content/dam/rand/ pubs/monographs/2009/RAND_MG877.pdf (accessed: 10.05.2019).
6. *Sanger, D.* Document Reveals Growth of Cyberwarfare between the U.S. and Iran. 2015. URL: https://www.nytimes.com/2015/02/23/us/document-reveals-growth-of-cyberwarfare-between-the-us-and-iran.html (accessed: 10.05.2019).
7. *Dietrich, J.* The George W. Bush foreign policy reader. London: Routledge, 2015.
8. *Rice, S.* U.S. National Security Policy Post-9/11: Perils and Prospects. 2004. URL: https://www. brookings.edu/wp-content/uploads/2016/06/20040122.pdf (accessed: 10.05.2019).
9. *Bush, W.G.* National Strategy to Secure Cyberspace. Washington DC: The White House, 2003.
10. *Graham, B.* Bush Orders Guidelines for Cyber-Warfare. 2003. URL: https://www.washingtonpost. com/archive/politics/2003/02/07/bush-orders-guidelines-for-cyber-warfare/dd8b4a18-140c-4690-88a5-0041d4ce1b1c/?noredirect=on&utm_term=.aef70711cce7 (accessed: 10.05.2019).
11. *Weimann, G.* Cyberterrorism How Real Is the Threat? Washington, DC: United States Institute of Peace, 2004. URL: https://www.usip.org/sites/default/files/sr119.pdf (accessed: 10.05.2019).
12. White House. The National Strategy to Secure Cyberspace. Washington, D.C., 2003. URL: https:// www.uscert.gov/sites/default/files/publications/cyberspace_strategy.pdf (accessed: 10.05.2019).

13. *Hare, F.* "The Cyber Threat to National Security: Why Can't We Agree?", in: Conference on Cyber Conflict Proceedings 2010. Tallinn, Estonia, CCD COE Publications, 2010, pp. 211–226.
14. National Military Strategy for Cyberspace Operations. Washington, D.C: U.S. Department of Defense, 2006. URL: https://www.hsdl.org/?view&did=35693 (accessed: 01.01.2019).
15. Department of Homeland Security. National Strategy For Homeland Security. 2007. URL: https://www.dhs.gov/national-strategy-homeland-security-october-2007 (accessed: 30.05.2019).
16. *Henning, A.* Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations. Washington, D.C.: Congressional Research Service Reports, 2009. URL: https://fas.org/sgp/crs/natsec/R40427.pdf (accessed: 02.05.2019).
17. Whitehouse Archives. Policies of the Bush Administration: 2001–2009. 2008. URL: https://georgewbush-whitehouse.archives.gov/infocus/bushrecord/documents/Policies_of_the_Bush_Administration.pdf (accessed: 02.05.2019).
18. *Trujillo, C.* The Limits of Cyberspace Deterrence. Washington, D.C: The National Defense University Press, 2014.
19. International Strategy for Cyberspace. Washington, D.C.: The White House, 2011. URL: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (accessed: 07.05.2019).
20. The Comprehensive National Cybersecurity Initiative. 2010. URL: www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative (accessed: 07.05.2019).
21. DoD Cyber Strategy. Washington, D.C.: United States Department of Defense. 2015. URL: http://archive.defense.gov/home/features/2015/0415_cyber-strategy/final_2015_dod_cyber_strategy_for_web.pdf (accessed: 07.05.2019).
22. White House. FACT SHEET: President Xi Jinping's State Visit to the United States. 2015. URL: https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states (accessed: 19.11.2018).
23. Chicagotribune.com. Chicago Tribune – We are currently unavailable in your region. 2016. URL: https://www.chicagotribune.com/news/90728462-132.html (accessed: 19.05.2019).
24. BBC News. 2016 .اوباما روسیه را به اتهام حمله سایبری انتخاباتی تحریم کرد. URL: http://www.bbc.com/persian/world-38459984 (accessed: 19.05.2019).
25. *Shabad, R.* Donald Trump vows to strengthen cybersecurity capabilities. 2016. URL: https://www.cbsnews.com/news/donald-trump-vows-to-strengthen-cybersecurity-capabilities/
26. Billington CyberSecurity. On Day 1, Pres. Trump to Direct Pentagon to Develop Plan to Protect Cybersecurity of Infrastructure – Billington CyberSecurity. 2017. URL: https://www.billingtoncybersecurity.com/day-1-pres-trump-direct-pentagon-develop-plan-protect-cybersecurity-infrastructure/ (accessed: 03.06.2019).
27. Council on Foreign Relations. The White House National Cyber Strategy: Continuity with a Hint of Hyperbole. 2018. URL: https://www.cfr.org/blog/white-house-national-cyber-strategy-continuity-hint-hyperbole (accessed: 10.05.2019).
28. *Encina, C.* The Trump Administration's National Security Strategy. 2018. URL: http://www.realinstitutoelcano.org (accessed: 09.05.2019).
29. DoD Cyber Strategy. Washington, D.C.: United States Department of Defense, 2018. URL: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF (accessed: 09.05.2019).
30. Realcleardefense.com. 2018. URL: https://www.realcleardefense.com/articles/2018/12/03/an_assessment_of_the_2018_us_department_of_defense_cyber_strategy_summary_113997.html (accessed: 12.04.2019).

REFERENCES

1. BBC News. اوباما روسیه را به اتهام حمله سایبری انتخاباتی تحریم کرد. 2016, available at: http://www.bbc.com/persian/world-38459984 (accessed: 19.05.2019).
2. Billington CyberSecurity. On Day 1, Pres. *Trump to Direct Pentagon to Develop Plan to Protect Cybersecurity of Infrastructure — Billington CyberSecurity*. 2017, available at: https://www.billingtoncybersecurity.com/day-1-pres-trump-direct-pentagon-develop-plan-protect-cybersecurity-infrastructure/ (accessed: 03.03.2019).
3. Bush W.G. *National Strategy to Secure Cyberspace*. Washington DC: The White House, 2003.
4. Chicagotribune.com. *Chicago Tribune — We are currently unavailable in your region*. 2016, available at: https://www.chicagotribune.com/news/90728462-132.html (accessed: 19.05.2019).
5. Clarke R. *War from Cyberspace*. 2009, available at: http://users.clas.ufl.edu/zselden/coursereading2011/Clarkecyber.pdf (accessed: 10.05.2019).
6. Council on Foreign Relations. *The White House National Cyber Strategy: Continuity with a Hint of Hyperbole*. 2018, available at: https://www.cfr.org/blog/white-house-national-cyber-strategy-continuity-hint-hyperbole (accessed: 10.05.2019).
7. *Department of Homeland Security. National Strategy For Homeland Security*. 2007, available at: https://www.dhs.gov/national-strategy-homeland-security-october-2007 (accessed: 30.05.2019).
8. Dietrich J. *The George W. Bush foreign policy reader*. London: Routledge, 2015.
9. *DoD Cyber Strategy*. (online) Washington, D.C.: United States Department of Defense, 2018, available at: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF (accessed: 09.05.2019).
10. *DoD Cyber Strategy*. Washington, D.C.: United States Department of Defense. 2015, available at: http://archive.defense.gov/home/features/2015/0415_cyber-strategy/final_2015_dod_cyber_strategy_for_web.pdf (accessed: 07.05.2019).
11. Drezner McQuade, Singh, Ford, McLeary, Zenko, Walt and Boot. *I'm cyber-confused.* Foreign Policy. 2017, available at: http://foreignpolicy.com/2013/02/04/im-cyber-confused/ (accessed: 27.11.2017).
12. Encina C. *The Trump Administration's National Security Strategy*. 2018, available at: http://www.realinstitutoelcano.org (accessed: 10.05.2019).
13. Graham B. *Bush Orders Guidelines for Cyber-Warfare*. 2003, available at: https://www.washingtonpost.com/archive/politics/2003/02/07/bush-orders-guidelines-for-cyber-warfare/dd-8b4a18-140c-4690-88a5-0041d4ce1b1c/?noredirect=on&utm_term=.aef70711cce7 (accessed: 10.05.2019).
14. Hare F. "The Cyber Threat to National Security: Why Can't We Agree?" In: *Conference on Cyber Confl ict Proceedings 2010*. Tallinn, Estonia: CCD COE Publications, 2010, pp. 211–226.
15. Henning A. *Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations*. (online) Washington, D.C.: Congressional Research Service Reports, 2009, available at: https://fas.org/sgp/crs/natsec/R40427.pdf (accessed: 02.05.2019).
16. *International Strategy for Cyberspace*. Washington, D.C.: The White House, 2011, available at: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (accessed: 07.05.2019).
17. Lee D. *China dismisses U.S. accusations of cyber-spying //* Los Angeles Times. 2013, available at: http://articles.latimes.com/2013/may/07/world/la-fg-wn-china-us-cyber-spying-20130507 (accessed: 19.11.2017).
18. Libicki M. *Cyberdeterrence and Cyberwar*. 2009, available at: https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf (accessed: 10.05.2019).

19. *National Military Strategy for Cyberspace Operations*. (online) Washington, D.C., U.S. Department of Defense, 2006, available at: https://www.hsdl.org/?view&did=35693 (accessed: 01.01.2019).
20. Rand.org. *Cyber Warfare.* 2019, available at: https://www.rand.org/topics/cyber-warfare.html (accessed: 10.05.2019).
21. *Realcleardefense.com. 2018,* available at: https://www.realcleardefense.com/articles/2018/12/03/an_assessment_of_the_2018_us_department_of_defense_cyber_strategy_summary_113997.html (accessed: 12.04.2019).
22. Rice S. *U.S. National Security Policy Post-9/11: Perils and Prospects*. 2004, available at: https://www.brookings.edu/wp-content/uploads/2016/06/20040122.pdf (accessed: 10.05.2019).
23. Sanger D. *Document Reveals Growth of Cyberwarfare between the U.S. and Iran*. 2015, available at: https://www.nytimes.com/2015/02/23/us/document-reveals-growth-of-cyberwarfare-between-the-us-and-iran.html (accessed: 10.05.2019).
24. Shabad R. *Donald Trump vows to strengthen cybersecurity capabilities*. 2016, available at: https://www.cbsnews.com/news/donald-trump-vows-to-strengthen-cybersecurity-capabilities/
25. *The Comprehensive National Cybersecurity Initiative*. 2010, available at: www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative (accessed: 07.05.2019).
26. Trujillo *C. The Limits of Cyberspace Deterrence*. Washington, D.C., The National Defense University Press, 2014.
27. Weimann G. *Cyberterrorism How Real Is the Threat?* Washington, D.C., United States Institute of Peace, 2004, available at: https://www.usip.org/sites/default/files/sr119.pdf (accessed: 10.05.2019).
28. White House. *FACT SHEET: President Xi Jinping's State Visit to the United States*. 2015 (online), available at: https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states (accessed: 19.11.2018).
29. White House. *The National Strategy to Secure Cyberspace*. Washington, D.C., 2003, available at: https://www.uscert.gov/sites/default/files/publications/cyberspace_strategy.pdf (accessed: 10.05.2019).
30. Whitehouse Archives. *Policies of the Bush Administration: 2001–2009*, available at: https://georgewbush-whitehouse.archives.gov/infocus/bushrecord/documents/Policies_of_the_Bush_Administration.pdf (accessed: 02.05.2019).

Сейед Асгар Кейван Хоссейни (Иран), доцент, кафедра международных отношений, Университет им. Алламе Табатабаи, Тегеран, a.keivan.ir@gmail.com

Seyed Asgar Keivan Hosseini, Associate Professor, International Relations Department, Allameh Tabataba'i University, Tehran, a.keivan.ir@gmail.com

Мохаммад Юсоф-ванд (Иран), магистрант, Университета им. Алламе Табатабаи, Тегеран, Yusefvand@gmail.com

Mohammad Yusof-vand, Post-Graduate Student, Allameh Tabataba'i University, Tehran, Yusefvand@gmail.com