

Национальная киберстратегия США: новый подход администрации Дональда Трампа

Научный руководитель – Капицын Владимир Михайлович

Ходыкин Максим Игоревич

Аспирант

Московский государственный университет имени М.В.Ломоносова, Факультет политологии, Кафедра сравнительной политологии, Москва, Россия

E-mail: masterkin94@mail.ru

Актуальность данной темы объясняется той ролью, которую сфера кибербезопасности играет во внутривнутриполитической жизни США в настоящее время. Обвинения, подчас бездоказательные, иностранных акторов (стран, компаний) в атаках на кибер инфраструктуру США ставит необходимость перед американскими властями выработать новый подход деятельности в данной сфере. Инициативы Д. Трампа по формированию нового подхода к киберсфере в США представляют значительный интерес, поскольку отражают новый вектор политики США, на основании которого свои доктрины и концепции будут ориентировать как союзники, так и противники Соединенных Штатов. В частности, Россия начала выработать ответные действия, создавая собственный «суверенный интернет» [1,4], реагируя на агрессивную риторику новой американской киберстратегии. Китай, например, названный в Стратегии одной из угроз давно создал собственную систему, независимую от атак извне[2].

В сентябре 2018 года на сайте Белого Дома была опубликована новая киберстратегия Соединенных Штатов [8], пришедшая на смену Национальной стратегии защиты киберпространства 2003 года[9], опубликованной еще в период первого президентского срока Д.Буша-младшего. Изданный администрацией Трампа документ предусматривает усиление национальной безопасности, цифровизацию, укрепление международного партнерства. Данные меры мало отличают доктрину Трампа от документов предыдущих администраций по кибербезопасности. Однако существует масса нововведений, позволяющих судить о новом подходе истеблишмента Соединенных Штатов к киберсфере. Составляющие активный глоссарий термины свидетельствуют о характере документа: «государства-противники», «заставить заплатить», «налагать последствия» и т.д.

Речь идет о противодействии информационным угрозам. Прежде всего, здесь подразумеваются бездоказательные обвинения истеблишмента США в адрес России по поводу вмешательства в президентские выборы 2016 года. Важна и декларация стремления распространить интернет по всему миру, что позволит еще больше усилить влияние американских IT-компаний. Сегодня, по данным Internet World Stats на июнь 2018 года, доступ к Интернету имеет лишь 55% населения Земли (4,208 млрд человек) [6] и эта цифра будет только увеличиваться по мере активизации усилий американских IT-компаний.

Наиболее важным, однако, представляется регламентация наступательного подхода в киберпространстве. Как сообщил советник Д.Трампа по национальной безопасности Джон Болтон: «наши руки больше не связаны, как это было в период деятельности администрации Обамы» [7], объясняя выгоды нового документа в сравнении с политикой предыдущего президента. При этом политик отметил стремление Соединенных Штатов к сохранению и достижению лидерства в международной киберсреде. Это объясняет восприятие ее важности на самом высоком уровне.

Глядя на «Международную стратегию для киберпространства» [5] в период президентства Б.Обамы можно наблюдать существенное ужесточение риторики новой администра-

ции. «Соединенные Штаты будут работать над созданием стимулов и достижением консенсуса в международном сообществе, где государства, признавая внутреннюю ценность открытого, интероперабельного, безопасного и надежного киберпространства, работают вместе и выступают в качестве ответственных заинтересованных сторон» - гласила доктрина Обамы.

Выработка нового подхода администрации Трампа к киберпространству ведет к усилению зависимости международного сообщества от киберугроз, ставя их на равных с традиционными угрозами на земле, воде и воздухе. Растущая зависимость порождает и рост уязвимости человечества, порождая новые проблемы и формы обеспечения национальной и международной безопасности [3].

Источники и литература

- 1) 1. Мамедьяров З., Ходыкин М. Суверенный, защищенный, свой // Эксперт. 2019. №8. С.12-17.
- 2) 2. Ходыкин М. Призрак русского файрвола / Эксперт. 2019. №8. С. 44.
- 3) 3. Шариков П.А. Подходы РФ и США к проблеме международно-правового обеспечения информационной безопасности / Проблемы национальной стратегии. 2013.№5(20).
- 4) 4. О внесении изменений в некоторые законодательные акты Российской Федерации (в части обеспечения безопасного и устойчивого функционирования сети «Интернет» на территории Российской Федерации) [Электронный ресурс] / URL: <http://sozd.duma.gov.ru/bill/608767-7> (дата обращения: 23.02.2019)
- 5) 5. International strategy for cyberspace, 2011 [Электронный ресурс] / URL: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (дата обращения: 24.02.2019)
- 6) 6. INTERNET USAGE STATISTICS [Электронный ресурс] / URL: <https://www.internetworldstats.com/stats.htm> (дата обращения: 24.02.2019)
- 7) 7. Nakashima E. White House authorizes 'offensive cyber operations' to deter foreign adversaries [Электронный ресурс] / URL: https://www.washingtonpost.com/world/national-security/trump-authorizes-offensive-cyber-operations-to-deter-foreign-adversaries-bolton-says/2018/09/20/b5880578-bd0b-11e8-b7d2-0773aa1e33da_story.html?noredirect=on&utm_term=.b78f26003859 (дата обращения: 23.02.2019)
- 8) 8. National cyber strategy of the United States of America, 2018 [Электронный ресурс] / URL: <https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf> (дата обращения: 24.02.2019)
- 9) 9. The National Strategy to secure cyberspace, 2003 [Электронный ресурс] / URL: https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf 2003 (дата обращения: 24.02.2019)