

УДК 327.8

DOI: 10.31857/S268667300010630-3

## **Стратегия национальной кибербезопасности администрации Д. Трампа: содержание и экспертные оценки**

**Р.Р. Бакиров**

*Санкт-Петербургский государственный университет*

*Российская Федерация, 199034 Санкт-Петербург, Университетская набережная, д.7-9*

*ORCID: 0000-0001-7764-4048 e-mail: ramil.1905@mail.ru*

*Статья поступила в редакцию 31.05.2020.*

---

**Резюме:** В статье рассматривается Стратегия национальной кибербезопасности США, выпущенная администрацией Дональда Трампа. Автор выявляет новые подходы и методы политики информационной безопасности, рассматриваются взгляды администрации Дональда Трампа на такие вызовы и угрозы в киберпространстве, как информационная безопасность, политика сдерживания киберпреступников, всесторонняя защита национальных интересов, а также процедуры и правила, разработанные для решения национальных и международных проблем в киберпространстве.

**Ключевые слова:** США, Стратегия национальной кибербезопасности США, информационные технологии, кибербезопасность, кибератаки, киберпреступность, внешняя политика США

**Для цитирования:** Бакиров Р.Р. Стратегия национальной кибербезопасности администрации Д. Трампа: содержание и экспертные оценки. *США & Канада: экономика, политика, культура*, 2020; 50(8)87-96. DOI: 10.31857/S268667300010630-3

---

## **National Cybersecurity Strategy of D. J. Trump's Administration: Contents and Expert Assessments**

**Ramil R. Bakirov**

*Saint-Petersburg State University.*

*7 - 9, Universitetskaya Emb., Saint-Petersburg 199034, Russian Federation.*

*ORCID: 0000-0001-7764-4048 e-mail: ramil.1905@mail.ru*

*Received 31.05.2020.*

---

**Abstract:** The article discusses the recent U.S. National Cybersecurity Strategy issued by Donald Trump administration. The author reveals new approaches and methods of the U.S. information security policy. The paper considers Donald Trump administration's views on the following challenges and threats in the cyber sphere: the information security, the deterrence policy towards cyber adversaries, the comprehensive protection of the national interests, and the procedure and rules elaborated for dealing with national and international problems in cyberspace.

**Keywords:** USA, National cyber strategy, information technologies, cybersecurity, cyberattacks, cybercrime, U.S. foreign policy.

*For citation:* Bakirov R.R. National Cybersecurity Strategy of the D. J. Trump's Administration: Content and Expert Assessments. *USA & Canada: Economics, Politics, Culture*. 2020; 50(8):87-96. DOI: 10.31857/S268667300010630-3

## ВВЕДЕНИЕ

В сентябре 2018 г., администрация Дональда Трампа опубликовала новую стратегию национальной кибербезопасности впервые за 15 лет [14]. Это довольно долгий срок, поскольку новые технологии в этой сфере появляются практически каждый месяц. Но, стоит отметить, что Соединённые Штаты Америки, будучи лидерами в данной области, в последнее десятилетие активно совершенствуют нормативную и правовую базу. Происходит активный пересмотр методов и подходов ведения внешней политики в области кибербезопасности [18], которая определяет государственную политику государства в целом [16]. В новом документе отражены взгляды администрации Белого дома на различные вызовы и угрозы в информационной и цифровой сфере, определена политика сдерживания возможного противника в сетях и указан порядок решения национальных и межведомственных задач и целей в информационном пространстве (киберпространстве) [5].

Цель статьи – выявить основные черты новой политики кибербезопасности, которые отражены в стратегии 2018 г. Методологической основой для исследования является теория реализма и методы историко-сравнительного, системного и дискурс-анализа. Подходы реалистов позволяют рассматривать стратегию как документ, отражающий национальные интересы, а указанные методы – сравнить указанную стратегию с предшествующими документами, показать её место и роль в системе внешней политики США, а также выявить значения, смыслы и коннотации, отражающие политику кибербезопасности администрации Д. Трампа.

## СТРАТЕГИЯ НАЦИОНАЛЬНОЙ КИБЕРБЕЗОПАСНОСТИ 2018 г.: ОСНОВНЫЕ ПОЛОЖЕНИЯ И ОЦЕНКИ ЭКСПЕРТОВ США

Стратегия, по мнению президента США, впервые за 15 лет раскрывает реальные инструменты и подходы в политике кибербезопасности. В документе отмечается: «Администрация признаёт, что Соединённые Штаты ведут постоянную конкуренцию со стратегическими противниками, государствами-изгоями, террористическими и криминальными сетями. Россия, Китай, Иран и Северная Корея используют киберпространство как средство для борьбы с Соединёнными Штатами, их союзниками и партнёрами» [12]. По мнению США, «эти противники используют киберинструменты, чтобы подорвать нашу экономику и демократию, украсть нашу интеллектуальную собственность и посеять раздор в наших демократических процессах» [12]. Стоит отметить, что вопрос о краже интеллектуальной собственности в киберпространстве в новой стратегии стоит довольно остро, в

документе отмечается, что «кража в киберпространстве представляет собой серьёзную угрозу американскому экономическому благосостоянию, а также национальной безопасности Соединённых Штатов» [12]. Таким образом, Россия, Китай, Иран и Северная Корея, по сути, обвиняются в «кибератаках» на Соединённые Штаты Америки, нанося ущерб американским деловым кругам, а также их партнёрам и союзникам [13]. В данном случае стоит отметить кибератаку на Национальный демократический комитет в 2016 г., которая привела к утечке данных кандидата в президенты от Демократической партии Х. Клинтон. Соединённые Штаты Америки столкнулись в тот момент с новой формой киберугрозы, которая связана с проведением выборов. «В совместном заявлении директора Национальной разведки и Агентства внутренней безопасности США, утверждалось, что “Россия непосредственно причастна к краже информации и её публикации в целях вмешательства в американский избирательный процесс» [Илона Стадник, Наталья Цветкова. 2018:157-169]. Стало известно также, что Кибернетическое командование США (*United States Cyber Command*) уже подготавливает сценарии ответных кибердействий при попытке России вмешаться в избирательный процесс на выборах президента в 2020 г. Речь идёт об ответных мерах в виде киберопераций, направленных на ключевых лидеров служб безопасности, а также различные санкции [21].

Бывший помощник президента Соединённых Штатов по национальной безопасности Джон Болтон отмечал, что национальная киберстратегия является адекватным ответом угрозам со стороны киберпротивников США, а именно России, Китая, Ирана, Северной Кореи. Он утверждал, что «Америка и её союзники подвергаются атакам в киберпространстве каждый день. Злонамеренные государства, преступные и террористические организации стремятся похитить наши интеллектуальную собственность, персональные данные, нанести урон нашей инфраструктуре и даже подорвать нашу демократию с помощью киберинструментов» [9]. Сохранение преимущества и сдерживание, а также предотвращение дестабилизации международных интересов США в киберпространстве является, по мнению Джона Болтона, одной из основных целей стратегии [2].

Стоит отметить, что эксперт Фонда стратегической культуры Леонид Савин считает, что киберстратегия – это «преамбула агрессии» [1]. По мнению российского эксперта, «сторонники жёсткой линии в Америке довольны тем, что в новом документе нашёл отражение дух экспансионизма. А приверженцы «мягкой» линии удовлетворены возрождением интереса к теме киберпространства». В качестве основных противников, объектов сдерживания в киберпространстве называют Китай, Россию, Северную Корею, Иран. Согласно мнению эксперта, Соединённые Штаты приложат большие усилия для модернизации средств электронного наблюдения, передачи больших, чем сейчас, полномочий, силовым структурам [1].

С другой стороны, в документе содержится четыре основных «столпа» – цели и задачи, которые, по мнению экспертов [12], носят в основном оборонительный характер [11]:

- Защита американского народа, родины и образа жизни американцев, которая включает стратегию защиты государственных систем и критически важной инфраструктуры;
- Содействие американскому процветанию, которое поощряет инвестиции во внедрение технологий и инноваций в области кибербезопасности и развитие рабочей силы в области кибербезопасности;
- Сохранение мира с помощью силы, сдерживание «недопустимого поведения в киберпространстве», совместно со своими союзниками и партнёрами;
- Усиление и повышение американского влияния, включая «продвижение открытого, совместимого, надёжного и безопасного интернета» [12].

Для того чтобы эти цели были достигнуты, администрация Д. Трампа намерена провести комплекс мероприятий: организацию эффективной и чёткой борьбы с киберуязвимостями и совершенствование защиты сетей, данных и систем, а также своевременное обнаружение кибератак, укрепление устойчивости по отношению к ним и оперативное восстановление работоспособности критической инфраструктуры. Стоит отметить и такие мероприятия, как сдерживание активности других государств, (что противоречит свободе поведения в киберпространстве), посредством создания таких условий, при которых ответные меры или действия (в том числе с использованием кибернетических и других средств) будут неприемлемы для «злоумышленников» [12]. Но, с другой стороны, по мнению Тома Келлермана, главы компании «Карбон блэк» (*Carbon Black*), киберстратегия – правильный шаг, но в ней недостаточно внимания уделяется, в частности, теневой интернет-экономике, а также выстроенным сетям для нанесения хакерских атак [11].

Одно из приоритетных направлений в стратегии связано с «немедленными и решительными мерами», необходимостью тщательного анализа существующих и перспективных рисков, а также с определением приоритетных мер по их минимизации в таких областях, как энергетика, национальная безопасность, информационные технологии, связь, банковская сфера. Следуя принципу поддержания американских интересов и безопасности, администрация Д. Трампа придаёт ключевое значение выработке методов реагирования на действия в информационных сетях, которые наносят ущерб Соединённым Штатам и их союзникам [8]. В данном случае утверждается, что для предотвращения, сдерживания и реагирования на преступную киберактивность «злоумышленника», будут использованы все инструменты национальной мощи: военные, финансовые, дипломатические, информационные, а также разведывательные [12]. В том числе предусматривается организовать работу разведывательных органов таким образом, чтобы федеральные ведомства и их зарубежные партнёры обменивались информацией и сведениями для своевременного раскрытия планов и действий в киберпространстве,

проводимых враждебными по отношению к США и их союзникам государствами. Г. Тохил, президент «Цикстера федерал групп» (*Cyxtera Federal Group*), утверждает, что киберстратегия является большим шагом вперед в обеспечении кибербезопасности Соединённых Штатов Америки и всего мира [11].

Но, с другой стороны, по мнению Ж. Вольф, исследователя из Рочестерского технологического института (*Rochester Institute of Technology*), новая политика нанесения превентивных ударов по интернет-злоумышленникам может только спровоцировать новые кибератаки, а не сдерживать их [20]. Эксперт отмечает, что, на первый взгляд, новую стратегию национальной кибербезопасности США 2018 г. легко спутать с предшествующими стратегиями, а именно с Обзором политики киберпространства администрации Барака Обамы 2009 г. [4;6] и Национальной стратегией по обеспечению безопасности киберпространства Дж. Буша-младшего 2003 г. [17]. Действительно, все три документа подчёркивают поразительно сходные задачи: важность укрепления инфраструктуры, работу с частным сектором, защиту правительственных сетей и установление более прочных партнёрских отношений для обмена информацией об интернет-угрозах. К слову, А. Шварц, управляющий директор службы кибербезопасности юридической фирмы «Венейбл» (*Venable*), отмечает, что стратегия не содержит в себе ничего принципиально нового и в общих чертах повторяет Национальный план действий 2016 г., созданный при Б. Обаме. По мнению Шварца, данная киберстратегия является по большей части риторикой, нежели руководством к политическим действиям [11].

Несмотря на сходство трёх стратегий и планов реализации политики кибербезопасности предыдущих администраций, по мнению Ж. Вольф, новая национальная киберстратегия США представляет собой резкий сдвиг политики правительства по взаимодействию с потенциальными противниками в информационной сфере и киберпространстве [20]. Таким образом, вместо того, чтобы сосредоточиться на укреплении защитных технологий, администрация Дональда Трампа наоборот – планирует наращивать наступательные кибероперации. Стратегия 2018 г. обозначает новую цель – сдерживать противников с помощью упреждающих кибератак и заставить другие государства опасаться ответных ударов.

В итоге, основа новой политики кибербезопасности заключена в нескольких документах, а именно – в недавней Стратегии национальной кибербезопасности Соединённых Штатов Америки [12], где представлено общее видение того, как администрация Дональда Трампа будет подходить к онлайн-проблемам, особенно связанным с важностью навязывать быстрые, дорогостоящие, явные и прозрачные последствия для злоумышленников в киберсфере. Во-вторых, в новой стратегии Министерства обороны США [7], где описывается развёрнутый план того, как военные будут подходить к вопросу кибербезопасности. В частности, там изложен план «превентивной защиты» [10], в соответствии с которым угрозы преследуются до того, как они достигнут своих целей, а злонамеренная активность подрывается у его источника [15]. И в-третьих, секретный меморандум №13 президента США [19], который облегчает военным начинать упрежда-

ющие кибероперации, значительно упрощает долгий процесс межведомственного утверждения и одобрения киберопераций [3].

Стоит отметить, что активная реализация политики кибербезопасности США стартовала уже в начале 2019 г. В феврале – марте в Конгрессе США прошли слушания по делу китайских компаний «Хуавэй» (*Huawei*) и ЗТЕ (*ZTE*). В них указывалось, что эти компании являются серьёзной и непосредственной угрозой национальной безопасности США, так как активно наращивают свою инвестиционную политику и вкладывают значительные средства в развитие беспроводной технологии следующего поколения 5G. В том числе увеличивают долю своих компаний на мировом рынке телекоммуникационных технологий. Особую озабоченность властей США вызывает также тот факт, что китайские службы разведки и безопасности могут использовать китайские фирмы, занимающиеся информационными технологиями в качестве рутинных и системных шпионских платформ против США и их союзников [22]. Отмечается, что Китайская Народная Республика продолжает способствовать росту киберпреступности, используя слабые места в международной системе для подрыва честной конкуренции в технологиях и киберпространстве, в том числе путём кражи интеллектуальной собственности и спонсируемых государством злонамеренных действий для подрыва и ослабления конкуренции [23]. Отметим, что вопросы в отношении китайских производителей информационных технологий обсуждались и ранее. Ещё в августе 2018 г. был принят закон «О полномочиях в области национальной обороны», который запрещал всем американским государственным ведомствам не только покупать оборудование и сервисы «Хуавэй», но также и заключать контракты и предоставлять гранты и займы третьим лицам, приобретающим оборудование и сервисы компании в обход исполнительных и судебных процедур [24].

Уже 15 мая 2019 г. Д. Трамп, подписал указ, который запрещает компаниям в США пользоваться оборудованием «Хуавэй» из-за высокого риска для национальной безопасности США, включающего кибершпионаж и кражу данных [25]. В результате многие американские фирмы и корпорации, такие как «Майкрософт», «Гугл» и т.д. стали отказываться от сотрудничества с «Хуавэй», и им требуется специальная лицензия властей США. Такой шаг помешает компаниям, принадлежащим иностранцам, использовать американские технологии для подрыва национальной безопасности США [26]. Таким образом, упомянутые выше действия политического истеблишмента Соединённых Штатов указывают на верность своей политике, и их действия наглядным образом демонстрируют превентивную риторику политики кибербезопасности США по обеспечению национальной безопасности государства.

## ЗАКЛЮЧЕНИЕ

Новый подход администрации Дональда Трампа к ведению киберопераций отличается резкостью и наступательностью, по сравнению с более осторожными

и сдержанными подходами администрации Барака Обамы. Осторожное принятие решений в отношении кибератак на США соответствуют киберстратегии Министерства обороны от 2015 г., в которой контроль за эскалацией киберконфликтов определён в качестве ключевой стратегической цели. В новой стратегии Министерства обороны данная цель отсутствует.

Переход администрации Дональда Трампа к наступательному подходу явно обострит киберконфликты, и такая эскалация может быть достаточно опасной. Многие эксперты отмечают, что «это не только отвлечёт ресурсы и внимание от более насущных вопросов защиты и управления рисками в киберпространстве, но и побудит правительство действовать безрассудно, направляя кибератаки на цели, прежде чем они смогут быть уверены, что это за цели» [20].

Таким образом, используя данную превентивную риторику, Соединённые Штаты Америки могут столкнуться с ответными атаками России, Северной Кореи или Китая, которые имеют значительный потенциал в кибератаках и, несомненно, используют его [16]. Более того, упреждающие кибератаки на своих противников приведут к росту конфликтов в международной среде, так как, несомненно, при превентивной агрессии со стороны Соединённых Штатов Россия, Северная Корея или Китай ответят аналогичным образом, если их критическим инфраструктурам будет угрожать опасность. Поэтому данный подход является достаточно рискованным и уязвимым для Соединённых Штатов Америки.

## ИСТОЧНИКИ

1. Савин Л. Национальная киберстратегия США – преамбула агрессии. Фонд Стратегической Культуры. 28.09.2018. Available at: <https://www.fondsk.ru/news/2018/09/28/nacionalnaja-kiberstrategia-us-preambula-agressii-46860.html> (accessed 22.02.2020).

2. Трамп утвердил новую стратегию кибербезопасности США. ТАСС. 20.09.2018. Available at: <https://tass.ru/mezhdunarodnaya-panorama/5588614> (accessed 01.03.2020).

3. A Bill H.R. 3359. 115th Congress 1st Session. July 2017. Available at: <https://www.congress.gov/115/bills/hr3359/BILLS-115hr3359rh.pdf> (accessed 25.02.2020).

4. Adelman K. A war we can fight to win. *Foreign Policy*. 29.05.2009. Available at: <https://foreignpolicy.com/2009/05/29/a-war-we-can-fight-to-win/> (accessed 21.02.2020).

5. Carter W.A. Extending Federal Cybersecurity to the Endpoint. Center for Strategic and International Studies (CSIS). 09.10.2018. Available at: <https://www.csis.org/analysis/extending-federal-cybersecurity-endpoint> (accessed 20.03.2020).

6. Cyberspace Policy Review 2009. The White House. Available at: <https://fas.org/irp/eprint/cyber-review.pdf> (accessed 13.02.2020).

7. Department of Defense Cyber Strategy 2018. US Department of Defense. Available at: [https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER\\_STRATEGY\\_SUMMARY\\_FINAL.PDF](https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF) (accessed 12.03.2020).
8. Kirk J. Trump Pulls Gloves Off on Offensive Cyber Actions. Info Security. 17.08.2018. Available at: <https://www.govinfosecurity.com/trump-pulls-gloves-off-on-offensive-cyber-actions-a-11374> (accessed 20.02.2020).
9. Kirk J. US, UK: Russian Hackers Deeply Embedded in Routers, Switches. Info Security. 17.04.2018. Available at: <https://www.bankinfosecurity.com/us-uk-russia-deeply-embedded-in-routers-switches-a-10806> (accessed 20.02.2020).
10. Lange K. 5 Keys To Success Here's The DoD Cybersecurity Strategy. The Department of the Navy's Information Technology. 16.05.2015. Available At: <https://www.doncio.navy.mil/CHIPS/ArticleDetails.aspx?ID=10846> (accessed 24.02.2020).
11. McGee M. K. White House National Cyber Strategy: An Analysis. Info Security. 26.09.2018. Available at: <https://www.bankinfosecurity.com/white-house-national-cyber-strategy-analysis-a-11558> (accessed 26.02.2020).
12. National Cyber Strategy of the United States of America 2018. The White House. September, 2018. Available at: <https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf> (accessed 10.03.2020).
13. Perlroth N. Chinese and Iranian Hackers Renew Their Attacks on U.S. Companies. *The New York Times*. 18.02.2019. Available at: <https://www.nytimes.com/2019/02/18/technology/hackers-chinese-iran-usa.html?searchResultPosition=8> (accessed 26.02.2020).
14. Release of the 2018 National Cyber Strategy. U.S. Department of State. September, 2018. Available at: <https://www.state.gov/r/pa/prs/ps/2018/09/286093.htm> (accessed 20.03.2020).
15. Tadjeh Y. Analysts Laud New Federal Cyber Strategies. *National Defense*. 01.11.2018. Available at: <https://www.nationaldefensemagazine.org/articles/2018/11/1/analysts-laud-new-federal-cyber-strategies> (accessed 24.03.2020).
16. Crandall M., Thayer B. The Balance of Cyber power. *The National Interest*. 25.11.2018. Available at: <https://nationalinterest.org/feature/balance-cyberpower-36637> (accessed 25.03.2020).
17. The National Strategy to Secure Cyberspace 2003. The White House. Available at: [https://www.us-cert.gov/sites/default/files/publications/cyberspace\\_strategy.pdf](https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf) (accessed 12.03.2020).
18. Volz D. Trump, Seeking to Relax Rules on U.S. Cyberattacks, Reverses Obama Directive. *The Wall Street Journal*. 15.08.2018. Available at: <https://www.wsj.com/articles/trump-seeking-to-relax-rules-on-u-s-cyberattacks-reverses-obama-directive-1534378721> (accessed 23.03.2020).

19. Volz D. White House Confirms It Has Relaxed Rules on U.S. Use of Cyberweapons. *The Wall Street Journal*. 20.09.2018. Available at: <https://www.wsj.com/articles/white-house-confirms-it-has-relaxed-rules-on-u-s-use-of-cyber-weapons-1537476729> (accessed 24.03.2020).

20. Wolff J. Trump's Reckless Cybersecurity Strategy. *The New York Times*. 02.10.2018. Available at: <https://www.nytimes.com/2018/10/02/opinion/trumps-reckless-cybersecurity-strategy.html?searchResultPosition=2> (accessed 18.03.2020).

21. Nakashima E. U.S. Cybercom contemplates information warfare to counter Russian interference in 2020 election. *The Washington Post*. 26.12.2019. Available at: [https://www.washingtonpost.com/national-security/us-cybercom-contemplates-information-warfare-to-counter-russian-interference-in-the-2020-election/2019/12/25/21bb246e-20e8-11ea-bed5-880264cc91a9\\_story.html](https://www.washingtonpost.com/national-security/us-cybercom-contemplates-information-warfare-to-counter-russian-interference-in-the-2020-election/2019/12/25/21bb246e-20e8-11ea-bed5-880264cc91a9_story.html) (accessed 27.03.2020).

22. S.Con.Res.10 - A concurrent resolution recognizing that Chinese telecommunications companies such as Huawei and ZTE pose serious threats to the national security of the United States and its allies. US Congress. 28.03.2019. Available at: <https://www.congress.gov/bill/116th-congress/senate-concurrent-resolution/10/text?q=%7B%22search%22%3A%5B%22cyber+N+136%22%5D%7D&r=10&s=3> (accessed 24.03.2020).

23. Res.140 - A resolution urging the establishment of a Cyber League of Indo-Pacific States to address cyber threats. US Congress. 04.03.2019. Available at: <https://www.congress.gov/bill/116th-congress/senate-resolution/140/text?q=%7B%22search%22%3A%5B%22cybersecurity%22%5D%7D&r=7&s=1> (accessed 18.03.2020).

24. H.R.5515 - John S. McCain National Defense Authorization Act for Fiscal Year 2019. US Congress. 18.04.2018. Available at: <https://www.congress.gov/115/bills/hr5515/BILLS-115hr5515enr.pdf> (accessed 20.03.2020).

25. Executive Order on Securing the Information and Communications Technology and Services Supply Chain. The White House. 15.05.2019. Available at: <https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/> (accessed 17.03.2020).

26. Kuo L., Siddiqui S. Huawei hits back over Trump's national emergency on telcoms 'threat'. *The Guardian*. 15.05.2019. Available at: <https://www.theguardian.com/us-news/2019/may/15/donald-trump-national-emergency-telecoms-threats-huawei> (accessed 20.03.2020).

## **СПИСОК ЛИТЕРАТУРЫ**

Цветкова Н.А, Стадник И. Политика кибербезопасности США: эволюция восприятия угроз. *Международные процессы*. 2018. №3. С. 157-169. DOI 10.17994/IT.2018.16.3.54.9

## **REFERENCES**

Tsvetkova N.A, Stadnik I. US Cybersecurity policy: threat perception evolution. *International processes*. 2018. №3. P. 157-169. DOI 10.17994/IT.2018.16.3.54.9

## **ИНФОРМАЦИЯ ОБ АВТОРЕ / INFORMATION ABOUT THE AUTHOR**

**БАКИРОВ Рамиль Раилевич**, аспирант,  
кафедры американских исследований  
Санкт-Петербургского государственного  
университета.  
Российская Федерация, Санкт-Петербург  
199034, Университетская наб., 7-9.

**Ramil R. BAKIROV**, Post-Graduate at  
the Department of American Studies,  
Saint-Petersburg State University.  
7-9 Universitetskaya Emb., 199034  
Saint-Petersburg, Russia.