ГОСУДАРСТВЕННОЕ УПРАВЛЕНИЕ ЗА РУБЕЖОМ

Научная статья

DOI: 10.55959/MSU2073-2643-21-2023-3-59-78

«ЗАКУЛИСЬЕ» ПРЕЗИДЕНТСКИХ ВЫБОРОВ В США 2016 г. ПРОБЛЕМА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В.В. Бухарин

Московский государственный университет имени М.В. Ломоносова, Москва, Российская Федерация
Bukharin@spa.msu.ru

Аннотация. В статье рассматриваются обвинения России в несанкционированном вмешательстве в информационную систему Национального комитета Демократической партии США. Впервые в отечественной и зарубежной историографии основное внимание уделено анализу технических аспектов документов, опубликованных стороной обвинения. Исследование данной проблематики позволяет более детально раскрыть инструменты и механизмы информационной войны, которую США ведут против России, понять ее логику и основные направления. В этой связи анализируются инструменты и механизмы, технические возможности и приемы, применяемые различными американскими политическими и военными структурами, которые использовали СМИ. Автор приходит к выводу, что американская сторона с самого начала расследования была сосредоточена на решении двух основных проблем: во-первых, это внутренние политические вопросы, связанные с компанией против Д. Трампа; а во-вторых, геополитическое противостояние с Россией. Подобный подход США к решению возникшей проблемы не способствует развитию российско-американского диалога в области проблем кибербезопасности, а также ставит под сомнение перспективы сотрудничества в рамках Группы правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности.

Ключевые слова: президентские выборы в США, Д. Трамп, Национальный комитет Демократической партии США, информационная без-

опасность, хакеры, кибератака, информационная война, кибербезопасность, CrowdStrike, Fancy Bear, APT28, OverWatch, X-Agent, WikiLeaks.

Для цитирования: *Бухарин В.В.* «Закулисье» президентских выборов в США 2016 г.: проблема информационной безопасности // Вестник Московского университета. Серия 21. Управление (государство и общество). 2023. Т. 20. № 3. С. 59–78. DOI: 10.55959/MSU2073-2643-21-2023-3-59-78

Дата поступления в редакцию: 28.03.2023.

"BEHIND THE SCENES" OF THE 2016 US PRESIDENTIAL ELECTION: THE PROBLEM OF INFORMATION SECURITY

Bukharin V.V.

Lomonosov Moscow State University, Moscow, Russian Federation
Bukharin@spa.msu.ru

Abstract. The article deals with accusations against Russia of unauthorized interference in the information system of the National Committee of the Democratic Party of the USA. The main attention in the article, for the first time in domestic and foreign historiography, is paid to the analysis of technical aspects of documents published by the prosecution. Thanks to the study of this problem, it is possible to reveal in more detail the tools and mechanisms of the information war that the United States is trying to wage against Russia, as well as to understand its logic and main directions. In this regard, the tools and mechanisms, technical capabilities and techniques used by various American political and military structures, which were willingly used by the media as part of the information war, are analyzed. The author comes to the conclusion that from the very beginning of the investigation, the American side has been focused on solving two main problems: firstly, internal political issues related to the company against D. Trump; and secondly, the geopolitical confrontation with Russia. Such an approach by the United States to solving the problem does not contribute to the development of the Russian-American dialogue in the field of cybersecurity issues, and also casts doubt on the prospects for cooperation within the framework of the UN Group of Governmental Experts on Achievements in the Field of Information and Telecommunications in the Context of International Security.

Key words: US presidential election, Donald Trump, US Democratic National Committee, information security, hackers, cyberattack, information warfare, cybersecurity, CrowdStrike, Fancy Bear, APT28, OverWatch, X-Agent, WikiLeaks.

For citation: *Bukharin V.V.* "Behind the scenes" of the 2016 US presidential election: the problem of information security // Lomonosov Public Administration Journal. Series 21. 2023. Vol. 20. No. 3. P. 59–78. DOI: 10.55959/MSU2073-2643-21-2023-3-59-78

Received: 28.03.2023.

Введение

В настоящее время происходят тектонические изменения системы международных отношений. Завершается эпоха доминирования Запада, планы США, направленные на строительство однополярной системы международных отношений, «мира по "по-американски"»[1], потерпели крах, формируется новый мировой порядок, многополярная система международных отношений. Подобные изменения, как отмечают многие политологи, не могут происходить безболезненно. Обострилось глобальное геополитическое противостояние между отдельными центрами силы, наблюдаются признаки «холодной войны», все чаще в СМИ звучат опасения относительно начала так называемой Третьей мировой войны. В этих сложных условиях, как справедливо отметил В.В. Путин, против России была «развязана настоящая агрессия, война в информационном пространстве»[2], одним из проявлений которой стали обвинения России во вмешательстве в американские выборы 2016 г.

Изучение ее фактического материала, технических аспектов, опубликованных стороной обвинения, представляет научную значимость и практический интерес. Через призму изучения обвинений России в несанкционированном вмешательстве в информационную систему Национального комитета Демократической партии США возможно более детально раскрыть инструменты и механизмы информационной войны, которую США пытаются вести против России, а также понять ее логику и основные направления, что является основной целью данной статьи. В соответствии с поставленной целью исследования, автор попытался решить следующие задачи: на основе опубликованных документов проанализировать техническую составляющую американских обвинений, выявить причины обострения информационного противостояния между странами и перспективы развития российско-американского со-

[1] *Богатуров А.Д.* Попытка перестроить мир «по-американски». Вестн. МГИМО-Университета. М. 2021. № 14 (5). С. 49.

[2] Заседание Совета Безопасности РФ 20 мая 2022 г. // Президент России. URL: http://kremlin.ru/events/president/news/68451 (дата обращения: 15.10.2022).

трудничества по вопросам кибербезопасности. Данный ракурс статьи подчеркивает актуальность проблемы и одновременно свидетельствует о новизне представленного исследования.

В период президентских выборов в США в 2016 г. и 2021 г. основной пласт работ по наиболее близкой к данной проблеме был посвящен непосредственно обвинениям Трампа в связях с России[3]. Технический аспект обвинений России в несанкционированном вмешательстве в информационную систему Национального комитета Демократической партии США в период президентских выборов 2016 г. до настоящего времени остается вне поля зрения исследователей. В качестве методологической основы исследования использовались принципы историзма и объективности, которые были реализованы при анализе обвинений России в несанкционированном вмешательстве в информационную систему Национального комитета Демократической партии США в период президентских выборов 2016 г. В соответствии с принципом объективности был изучен широкий круг источников, среди которых наиболее значимыми являются официальные документы разведки США, Агентства по кибербезопасности и защите инфраструктуры США, Конгресса США, Постоянного специального комитет Сената США по разведке, IT-компаний, работающих в сфере информационной безопасности. Многие документы не получили освещения в отечественных и зарубежных исследованиях. Источником исследования стали публикации американской и российской прессы. В статье используется системный подход, который позволил проанализировать американские обвинения в рамках системы внешней политики США.

В контексте исследуемой проблемы «закулисье» рассматривается с точки зрения концепции «мировой закулисы»[4]. Под «закулисьем» понимается неявная или потаенная политическая борьба,

---

[3] *Miller G.* The Apprentice: Trump, Russia and the Subversion of American Democracy. United States: HarperCollins. 2020; *Pontell H.N., Tillman R., Ghazi-Tehrani A.K.* In-your-face Watergate: neutralizing government lawbreaking and the war against white-collar crime. Crime Law Soc Change. 2021. 75. P. 201–219; *Вольф М.* Огонь и ярость. В Белом Доме Трампа. М.: Издательство АСТ: COPRUS. 2018; *Кошкин П.Г.* «Российское досье» как внутриполитический фактор в США // Россия и Америка в XXI веке. Спецвыпуск. 2019. URL: https://rusus.jes.su/s207054760005318-6-1/ (дата обращения: 15.10.2022); *Самуилов С.М.* Внешняя политика Д. Трампа: предвыборные обещания, противоречивые шаги, угроза импичмента // США и Канада: экономика, политика, культура. 2017. № 8 (572). С. 27–44; *Самуйлов С.М.* Внутренние проблемы администрации Д. Трампа и российско-американские отношения // США и Канада: экономика, политика, культура. 2018. № 6 (582). С. 6–9.

[4] *Душенко К.В.* «Мировая закулиса»: истоки концепции // Россия в глобальной политике. 2022. Т. 20. № 4. С. 178.

происходившая в США в 2016 г. между кандидатами[5], а скрытые инструменты и механизмы, технические возможности и приемы, применяемые различными американскими политическими и военными структурами, которые в рамках информационной войны охотно использовали СМИ[6]. Так, 3 мая 2016 г. на страницах The Washington Post были опубликованы слова Хиллари Клинтон: «Я была на пути к победе, пока 28 октября не появилось это письмо Джима Коми, а русская WikiLeaks не посеяла сомнения в умах тех людей, которые были склонны голосовать за меня, но испугались. Мне кажется, доказательств такого вмешательства предостаточно, и они неопровержимы и убедительны»[7]. В июне 2016 г. в мировых СМИ появилась информация о несанкционированном вмешательстве в информационную систему Национального комитета Демократической партии США (DNC), которое произошло в конце апреля 2016 г. Данные с взломанных серверов были опубликованы на сайте WikiLeaks[8]. К расследованию инцидента (кроме Федерального бюро расследований) была привлечена частная компания CrowdStrike. В результате расследования опубликован отчет, согласно которому вина за взлом возлагалась на хакерские группы Cozy Bear и Fancy Bear[9]. Штаб Хиллари Клинтон (кандидат от Демократической партии) еще до завершения расследования обвинял Россию в причастности к взлому. Например, русская служба BBC сообщала: «Министерство внутренней безопасности США и управление национальной разведки страны выпустили совместное заявление, в котором официально обвинили российские власти в организации

---

[5] *Stone R.* The Myth of Russian Collusion: The Inside Story of How Donald Trump REALLY Won. United States: Skyhorse. 2019; *Самуилов С.М.* Внешняя политика Д. Трампа: предвыборные обещания, противоречивые шаги, угроза импичмента // США и Канада: экономика, политика, культура. 2017. № 8 (572). С. 43.

[6] *Шариков П.* Информационный суверенитет и вмешательство во внутренние дела в российско-американских отношениях // Международные процессы. 2018. Т. 16. № 3 (54). С. 170–188; *Бухарин В.В.* Компоненты цифрового суверенитета Российской Федерации как техническая основа информационной безопасности // Вестн. МГИМО-Университета. М. 2016. № 6 (51). С. 76–90.

[7] *Rucker P.* 'I would be your president': Clinton blames Russia, FBI chief for 2016 election loss // The Washington Post. 3 May 2017. URL: https://www.washingtonpost.com/politics/hillary-clinton-blames-russian-hackers-and-comey-for-2016-election-loss/2017/05/02/e62fef72-2f60-11e7-8674-437ddb6e813e_story.html (дата обращения: 15.10.2022).

[8] *Горбатюк Н.В.* WikiLeaks. Разоблачения, изменившие мир. Россия: Эксмо. 2022.

[9] CrowdStrike's work with the Democratic National Committee: Setting the record straight // CrowdStrike. URL: https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/ (дата обращения: 15.10.2022).

кибератак на американские политические структуры»[10]. Согласно их заявлению, опубликованному на официальном сайте, «данная деятельность не является новой для Москвы — россияне использовали подобную тактику и технику по всей Европе и Евразии, например, чтобы повлиять на общественное мнение»[11]. Однако обвинения так и остались без доказательств[12].

Вместе с тем компания CrowdStrike уже была замечена в антироссийской риторике. Так, еще в начале 2014 г. «CrowdStrike включила Россию в список стран, активно занимающихся шпионажем на глобальном рынке. По данным аналитиков, российская хакерская группировка Energetic Bear виновна в атаках на 23 страны мира, включая США и государства Европы. Используя уязвимости в Windows XP, хакеры крадут информацию, которая способствует укреплению России на международной арене»[13]. Стоит отметить, что Джулиан Ассандж неоднократно заявлял, что WikiLeaks не получал материалов от России или какого-либо другого государства.

В рамках данной темы представляется уместным упомянуть о расследовании убийства сотрудника Демократического национального комитета Сета Рича, которое произошло в июле 2016 г., за 12 дней до того, как на WikiLeaks опубликовали внутреннюю переписку Национального комитета демократов. Например, «один из федеральных следователей в своих выводах зашел еще дальше и на условиях анонимности сообщил Fox News, что убитый сотрудник комитета отправил WikiLeaks более 40 тысяч электронных писем и 17 тысяч прикрепленных документов; это позволяет предположить, что Рич, а не российская сторона, тайно передал WikiLeaks материалы»[14]. Более того, сайт WikiLeaks назначил награду в 20 тыс. долл. за поимку виновного в убийстве.

---

[10] США официально обвинили Россию в хакерских атаках на политиков // BBC русская служба. URL: https://www.bbc.com/russian/news-37592860 (дата обращения: 15.10.2022).

[11] Joint DHS and ODNI Election Security Statement // Office of the Director of National Intelligence. URL: https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2016/item/1635-joint-dhs-and-odni-election-security-statement (дата обращения: 15.10.2022).

[12] *Diesen G.* Russophobia: Propaganda in International Politics. Switzerland: Springer Nature Singapore. 2022. P. 189.

[13] *Попсулин С.* Россию обвинили в глобальном кибершпионаже // CNews. http://safe.cnews.ru/news/top/rossiyu_obvinili_v_globalnom_kibershpionazhe (дата обращения: 15.10.2022).

[14] *Lauria J.* Seth Rich Murder Case Stirs Russia Doubts // Consortium News. https://consortiumnews.com/2017/05/17/seth-rich-murder-case-stirs-russia-doubts/ (дата обращения: 15.10.2022).

Избранный президентом Дональд Трамп (кандидат от Республиканской партии) неоднократно выражал сомнения в причастности России к хакерским атакам. Через свой Twitter[15] он отмечал, что «грубая халатность Национального комитета Демократической партии позволила осуществить хакерские атаки. Национальный комитет республиканцев серьезно защищен!»[16]. Прямых обвинений России в хакерских атаках Трамп на тот момент избегал.

29 декабря 2016 г. Министерство внутренней безопасности США и Федеральное бюро расследований опубликовали совместный аналитический отчет под заголовком «Степной гризли — российская киберпреступность»[17]. В преамбуле документа сказано, что «приводятся технические подробности, касающиеся инструментов и инфраструктуры, используемых военной разведкой для компрометации и использования сетей и конечных точек, связанных с выборами в США, а также ряда правительственных, политических и частных организаций США»[18]. В документе подчеркивалось, что ранее подобные отчеты не были связаны с конкретными странами, однако обвинение государства стало возможным благодаря техническим данным, полученным от Разведывательного сообщества США, Министерства внутренней безопасности, Федеральное бюро расследований (ФБР), частных лиц и других организаций. В связи с приведенным обвинением следует более подробно остановиться на анализе документа. В докладе говорилось о двух хакерских атаках, зафиксированных в США летом 2015 г. и весной 2016 г. В документе они были обозначены как «продвинутые постоянные сетевые угрозы» (Advanced Persistent Threat, APT) APT28 и APT29. В документе утверждалось, что их якобы осуществили две группы российских разведывательных служб. Кроме того, утверждалось, что обе группы будто бы изначально были сформированы для атак на правительственные организации, аналитические центры, уни-

---

[15] Социальная сеть Twitter заблокирована на территории России на основании статьи 15.3 федерального закона «Об информации, информационных технологиях и о защите информации», которая регламентирует порядок ограничения доступа к сайтам, содержащим призывы к массовым беспорядкам, осуществлению экстремистской деятельности, участию в массовых (публичных) мероприятиях, проводимых с нарушением установленного порядка.

[16] Donald J. Trump. URL: https://twitter.com/realDonaldTrump/status/817579925771341825 (дата обращения: 09.02.2017).

[17] GRIZZLY STEPPE — Russian Malicious Cyber Activity // Cybersecurity and Infrastructure Security Agency. URL: https://www.cisa.gov/uscert/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf (дата обращения: 15.10.2022).

[18] Ibid.

верситеты и корпорации по всему миру. В отчете говорилось: «Эти субъекты создают оперативную инфраструктуру для запутывания своей исходной инфраструктуры, хост-доменов и вредоносных программ, предназначенных для организаций, устанавливают узлы управления, а также собирают учетные данные и другую ценную информацию от своих целевых объектов[19]». Если детально разобрать указанный выше документ, то мы увидим туманную картину. Во-первых, приведенная на с. 2–3 «схема», согласно которой «действовали» хакерские группы, относится к числу шаблонных и широко распространенных. Более того, она соответствует большинству алгоритмов атак хакеров в сети в мире. Во-вторых, размещенный на с. 4 список так называемых «альтернативных имен» хакеров, банальный и общераспространенный. Набор «прозвищ» можно встретить в сети почти на любом форуме. Нет оснований утверждать, что эти «прозвища», относятся именно к русским хакерам. В-третьих, приведен пример «PHP script», который возможно запустить на сервере для проверки инфицирования «корневым червем». Подобный способ борьбы с вирусами достаточно часто используется на практике. В-четвертых, представленные на с. 6–12 «общие рекомендации» по безопасности сервера, можно охарактеризовать как простейшие и тривиальные. Они известны каждому квалифицированному специалисту. Данные «рекомендации» вообще не имеют отношения к обозначенной выше проблеме. Отчет заканчивался публикацией контактов «Национального центра интеграции Кибербезопасности и коммуникаций и ФБР». Таким образом, тщательный анализ документа позволяет сделать вывод о том, что выдвигаемые серьезные обвинения в отношении России были лишены каких-либо доказательств.

Однако американские СМИ продолжали «раскручивать» тему, вбрасывать в информационное пространство новый «сенсационный материал», который расходился по сетям с огромной скоростью, насыщая информационное поле беспочвенными обвинениями России и ее руководства. Так, 13 апреля 2017 г. Алана Гудман в газете Daily Mail опубликовала статью, под заголовком «ЭКСКЛЮЗИВ: Эксперты по кибербезопасности, которые первыми пришли к выводу, что Путин взломал президентские выборы, ОТКАЗЫВАЮТСЯ от некоторых своих претензий к России — и отказываются сотрудничать с Конгрессом»[20]. В статье автор говорил

[19] Ibid.

[20] *Goodman A.* EXCLUSIVE: Cybersecurity experts who were first to conclude that Putin hacked presidential election ABANDON some of their claims against Russia — and refuse to co-operate with Congress // Daily Mail. 5 April 2017. URL: http://www.

об очередном отчете компании CrowdStrike, впервые опубликованном в декабре 2016 г. под заголовком «Опасность близка: Fancy Bear следит за украинскими подразделениями полевой артиллерии»[21]. В документе говорилось, что хакеры из группы Fancy Bear (якобы те же самые русские хакеры, которые, по ее версии, стояли за атаками на DNC) работали в интересах российского ГРУ. Примечательно, что аббревиатура ГРУ (Главное разведывательное управление) не используется в России, поскольку данное ведомство было переименовано в Главное управление Генерального штаба Вооруженных Сил Российской Федерации. В отчете утверждалось, что CrowdStrike будто бы нашла доказательства взлома Fancy Bear украинской военной техники. Для взлома использовалось то же самое программное обеспечение, что и для проникновения в серверы DNC.

Чтобы оценить «обоснованность» обвинений следует обратиться к обстоятельствам разработки и внедрения украинского программного обеспечения — баллистического калькулятора Ярослава Шерстюка. По информации, опубликованной на официальном сайте Минобороны Украины, «в 2009 году капитан запорожской 55-й артиллерийской бригады Ярослав Шерстюк впервые задумался над тем, как автоматизировать систему ведения боя. Спустя шесть лет его разработки стали комплексным решением — 'ArtOS'. В конце октября в зоне военных действий состоялась официальная презентация его системы для 55-й артиллерийской бригады»[22]. Позднее программа была перенесена на операционную систему Android. «К 2013-му году о программе Шерстюка уже знала вся артиллерия. Свой калькулятор Ярослав выложил в свободный доступ в интернете, но пользоваться им могли не все. Для установки нужна была активация»[23]. Разумеется, как сказано на официальном сайте Минобороны Украины, при активации проверялось, является ли пользователь программы военнослужащим Украины. С этой целью автор программы задавал вопросы пользователю, на которые мог ответить только украинский артиллерист. CrowdStrike в декабрьском отчете утверждала, что Fancy Bear склеило данную програм-

---

dailymail.co.uk/news/article-4376628/New-questions-claim-Russia-hacked-election.html#ixzz4dRgDW34o (дата обращения: 15.10.2022).

[21] *Meyers A.* Danger Close: Fancy Bear Tracking of Ukrainian Field Artillery Units // CrowdStrike. URL: https://www.crowdstrike.com/blog/danger-close-fancy-bear-tracking-ukrainian-field-artillery-units/ (дата обращения: 15.10.2022).

[22] Артиллерийская математика. История разработчика Ярослава Шерстюка // Министерство обороны Украины. URL: https://www.mil.gov.ua/ministry/zmi-pro-nas/2015/11/09/artillerijskaya-matematika-istoriya-razrabotchika-yaroslava-sherstyuka/ (дата обращения: 15.10.2022).

[23] Там же.

му с вредоносным шпионским программным обеспечением Sofacy (X-Agent) и с конца 2014 г. до 2016 г. скрытно распространило ее на украинских военных форумах. Примечательно, что на данные интернет-ресурсы в отчете ссылки отсутствовали. В отчете утверждалось, что из-за зараженной программы Вооруженные силы Украины (ВСУ) потеряли 80% своих 122-мм гаубиц Д-30. Возникает вопрос: «Почему артиллеристы пользовались именно зараженной версией с форумов, а не официальной с сайта Ярослава? Данный вопрос остался без ответа. Важно отметить, что украинская армия публично опровергла факт хакерской атаки и потерю такого количества гаубиц. Международный институт стратегических исследований, штаб-квартира которого расположена в Лондоне (на данные которого сослалась CrowdStrike), заявил, что реальные потери гаубиц составили около 15–20%[24]. В марте CrowdStrike без лишнего шума отредактировала отчет и убрала из своего доклада утверждения о потере 80% гаубиц. Издание также сообщало: «В марте сооснователь CrowdStrike Дмитрий Альперович и ее президент Шон Генри отклонили приглашение дать показания о российском вмешательстве в выборы в США в комитете по делам разведки Палаты представителей США»[25].

Следует отметить, что группа кибершпионов Sofacy (также известная как APT28, Pawn Storm, Fancy Bear и Sednit), упомянутая выше, существовала задолго до американских выборов. По некоторым данным она действует с 2007 г.[26] В 2015 г. румынская IT-компания Bitdefender, разрабатывающая и выпускающая антивирусы, файрволы и спам-фильтры, в отчете, посвященном деятельности группы APT28, отмечала ее высокую активность на территории таких стран, как Украина, Испания, Россия, Румыния, США и Канада. В документе говорилось, что 14 февраля 2015 г. команда APT28 просканировала 8 536 272 IP-адреса на предмет возможных уязвимостей. Авторам доклада не известно, какие критерии использовали APT28 для выбора целей, но согласно проведенному исследованию сотрудниками румынской компании, хакеров интересовала политика, «услуги электронной преступности», телекоммуникационное обеспечение и аэрокосмическая промышлен-

[24] *Goodman A.* EXCLUSIVE: Cybersecurity experts who were first to conclude that Putin hacked presidential election ABANDON some of their claims against Russia — and refuse to co-operate with Congress // Daily Mail. 5 April 2017. URL: http://www.dailymail.co.uk/news/article-4376628/New-questions-claim-Russia-hacked-election.html#ixzz4dRgDW34o (дата обращения: 15.10.2022).

[25] Ibid.

[26] Sofacy // Malpedia. URL: https://malpedia.caad.fkie.fraunhofer.de/actor/sofacy (дата обращения: 09.02.2017).

ность[27]. В отчете также утверждалось, что за APT28 стояли либо граждане России, либо русскоговорящие граждане соседней страны. В качестве доказательства данной версии, кроме названий на кириллице, авторы доклада приводили время компиляции файлов — с 08:00 до 18:00 (рабочие дни, с понедельника по пятницу) для каждого часового пояса. Подавляющее большинство файлов компилировалось во временном интервале, который соответствовал часовому поясу UTC + 4. Авторы утверждали, что из стран, расположенных в данном часовом поясе якобы только Россия имела достаточный технический уровень для совершения подобных атак. Изложенные выше выводы отчета представляются весьма сомнительными. Использование неизвестными хакерами русского языка не только не доказывает их связь с российским правительством, но даже не свидетельствует об их гражданстве. Часовой пояс выглядит еще более спорным доказательством, поскольку таким образом предполагалось, что хакеры действовали строго в рабочее время. Остается также неизвестным, учли ли авторы документа изменения часовых поясов в Российской Федерации.

В качестве примера действия американских спецслужб, следует также обратиться к событиям, произошедшим в Чехии, где 18 октября 2016 г. полиция, действуя совместно с ФБР США, заявила о задержании российского хакера Евгения Никулина, обвиняемого в причастности к кибератакам на объекты в США. На официальном сайте полиции Чехии сообщалось об успешной операции, проведенной совместно с Федеральным бюро расследований США: «Целью полицейских на сей раз был российский гражданин, подозреваемый в хакерских атаках на объекты США. Интерпол выдал так называемый 'красный ордер' на данное лицо. Благодаря быстрому обмену информацией, мужчина был задержан уже через 12 часов после получения первых сведений»[28]. Арест произошел всего за два дня до того, как администрация Б. Обамы официально обвинила российское правительство в краже и раскрытии электронных писем от демократического Национального комитета, других учреждений и известных лиц. По утверждению газеты The New York Times, «сотрудники правоохранительных органов в Вашингтоне, выступая на условиях анонимности (поскольку они не были уполномочены

[27] APT28 Under the Scope A Journey into Exfiltrating Intelligence and Government Information // Bitdefender. URL: https://download.bitdefender.com/resources/media/materials/white-papers/en/Bitdefender_In-depth_analysis_of_APT28%E2%80%93The_Political_Cyber-Espionage.pdf (дата обращения: 15.10.2022).

[28] *Schön D.* Hacker je ve vazbě // Policie České republiky. URL: http://www.policie.cz/clanek/hacker-je-ve-vazbe.aspx (дата обращения: 15.10.2022).

комментировать ситуацию во время расследования), заявили в среду, что подозреваемый, скорее всего, не связан с взломом электронных писем демократов или таких организаций, как DCLeaks или WikiLeaks»[29]. По словам бывшего адвоката хакера Ильи Макеева, от Никулина настоятельно требовали признания в атаке на Национальный комитет Демократической партии. Позднее Никулин рассказал, как агент ФБР требовал признаться, что он лично взломал почтовый ящик Хиллари Клинтон для Дональда Трампа по приказу В. Путина, а также дать согласие на экстрадицию в США, где ему было обещано снятие обвинения, предоставление жилья, денег и американского гражданства[30]. Никулин отказался признаваться в том, что он не совершал. Несмотря на протест со стороны Российской Федерации в марте 2018 г. Никулин был экстрадирован в США. Его дело рассматривалось в Калифорнии, он обвинялся во взломе баз данных LinkedIn, Dropbox и Formspring в 2012 г. По информации, опубликованной на портале CyberScoop 29 сентября 2020 г. Никулин был приговорен к 88 месяцам лишения свободы[31].

Примечательно, что в 2016 г. Центральное разведывательное управление (ЦРУ) не проводило брифингов и фактически отказывалось публиковать какую-либо информацию, подтверждающую обвинения в адрес России. Подобные действия выглядели, как попытка скрыть отсутствие доказательств[32].

Представляется уместным исследовать также доклад компании CrowdStrike, озаглавленный «Взлом Национального комитета Демократической партии США показал одну из трех тенденций, на которые следует обратить внимание в 2017»[33]. Казалось, что

---

[29] *Lyman R., De Goeij H.* Russian Hacker, Wanted by F.B.I., Is Arrested in Prague, Czechs Say // The New York Times. Oct. 19, 2016. URL: https://www.nytimes.com/2016/10/20/world/europe/prague-russian-hacker.html (дата обращения: 15.10.2022).

[30] *Обухов А.* Арестованный «русский хакер» рассказал о требовании признать взлом Демпартии США // Электронное периодическое издание «MK.ru». URL: https://www.mk.ru/politics/2017/05/11/arestovannyy-russkiy-khaker-rasskazal-o-trebovanii-priznat-vzlom-dempartii-ssha.html (дата обращения: 15.10.2022).

[31] *Stone J.* LinkedIn hacker Nikulin sentenced to 7 years in prison after years of legal battles // CyberScoop. URL: https://www.cyberscoop.com/nikulin-sentence-russian-cybercrime-linkedin-hacker/ (дата обращения: 15.10.2022).

[32] *Harris S., Barrett D., Barnes J.* Republican National Committee Security foiled Russian hackers // The Wall Street Journal. Dec. 16, 2016. URL: http://www.wsj.com/articles/republican-national-committee-security-foiled-russian-hackers-1481850043 (дата обращения: 15.10.2022).

[33] DNC Hack Exhibits One of 3 Attack Trends To Watch for in 2017 // CrowdStrike. URL: https://www.crowdstrike.com/blog/dnc-hack-exhibits-one-of-3-attack-trends-to-watch-for-in-2017/ (дата обращения: 09.02.2017).

кричащее название свидетельствует о наличии вопиющих фактов, неопровержимых сведений и доказательств. Однако именно факты и доказательства не присутствовали в докладе, который сводился к трем выводам: 1. Использование хакерами антикриминальных средств для сокрытия следов нападения. 2. Доверие по отношению к сторонним организациям создает значительные риски. 3. Внедрение вредоносных программ стало нормой[34].

Хакеры используют доверенные процессы Windows для выполнения эксплойтов, поскольку они почти наверняка позволят обойти традиционные алгоритмы безопасности. Речь идет как о PowerShell, так и об инструментарии управления Windows (WMI). Команда Falcon OverWatch из CrowdStrike, анализируя текущие угрозы безопасности, отмечала, что в своих атаках хакеры все меньше прибегают к использованию вредоносных программ, предпочитая взламывать и получать контроль над исполняемыми файлами Windows.

Команда OverWatch предоставила указанные выше выводы консультантам CrowdStrike Services. В документе указывалось, что в процессе расследования было выявлено множество потенциальных угроз безопасности, в том числе: 1) использование PowerShell в качестве промежуточного инструмента для выполнения скриптов для компрометации системы; 2) использование WMI для установки бэкдоров[35], которые позволяют противнику автоматически запускать вредоносный код после определенного периода безотказной работы системы или в соответствии с «определенным графиком»; 3) распространение сложных вредоносных программ с товарами через сетевые ресурсы с помощью полиморфизма[36] или путем изменения хэшей[37].

Приведенные выше выводы доклада лишь отражают некоторую тенденцию в сфере защиты информации. Данный текст был удален с сайта компании. Безусловно, последнее время хакеры чаще используют инструменты администрирования, находящиеся на целевом сайте, вместо вредоносных программ. Данная тенденция была широко известна еще в 2015 г. Стоит отметить, что эксперты по безопасности были обеспокоены проблемой защиты встроенных

---

[34] Ibid.

[35] От анг. back door — «черный ход» или «тайный ход», позволяющий получить несанкционированный доступ к данным.

[36] Специальная техника, позволяющая скрыть вредоносный код от обнаружения антивирусным программным обеспечением.

[37] Функция свертки, применяемая в данном контексте для определения аутентичности файлов.

инструментов Windows, например проблемой обхода PowerShell Execution Policy[38]. Скотт Сазерленд[39] — сотрудник компании NetSPI, специализирующийся на разработке технических услуг и методов кибербезопасности, тестировании приложений, сетей и облачной инфраструктуры на предмет проникновения хакеров — утверждал, что командный интерпретатор PowerShell представляет интерес для хакеров, поскольку он «встроен в Windows», позволяет обращаться к Windows API[40], «может запускать команды без записи на диск», а также дает возможность «избегать обнаружения антивирусами», поскольку «помечен» как «достоверный» и находится в большинстве «белых списков», что часто используется при написании многих «утилит безопасности с открытым исходным кодом» [41].

5 января 2017 г. вопросы кибербезопасности обсуждались на открытых заседаниях в Комитете по вооруженным силам[42] и по разведке[43] США. Важно отметить, что проблема «причастности» российского руководства к хакерским атакам на них фактические не затрагивалась.

6 января 2017 г. Центральное разведывательное управление, Федеральное бюро расследований и Агентство национальной безопасности опубликовали рассекреченную часть доклада под названием «Оценки деятельности и намерений России на американских выборах»[44]. В документе полностью отсутствовали сколько-нибудь

---

[38] *Perez C.* Shell is only the beginning // Carlos Perez. URL: https://www.darkoperator.com/blog/2013/3/5/powershell-basics-execution-policy-part-1.html (дата обращения: 15.10.2022).

[39] Подробнее об авторе: Sutherland Scott // NetSPI. URL: https://blog.netspi.com/author/scott-sutherland/ (дата обращения: 15.10.2022).

[40] От англ. application programming interfaces — общее наименование набора базовых функций интерфейсов программирования приложений операционных систем семейств Microsoft Windows корпорации «Майкрософт».

[41] Подробнее см.: *Sutherland S.* 15 способов обхода PowerShell Execution Policy // SecurityLab.ru. URL: https://www.securitylab.ru/analytics/461333.php (дата обращения: 15.10.2022).

[42] Foreign Cyber Threats to the United States // Official site of the United States Senate Committee on Armed Services. URL: https://www.armed-services.senate.gov/imo/media/doc/17-01_01-05-17.pdf (дата обращения: 15.10.2022).

[43] ODNI Statement on Declassified Intelligence Community Assessment of Russian Activities and Intentions in Recent U.S. Elections // U.S. Senate Select Committee on Intelligence. URL: https://www.intelligence.senate.gov/hearings/open-hearing-intelligence-communitys-assessment-russian-activities-and-intentions-2016-us# (дата обращения: 15.10.2022).

[44] Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution // Office of the Director of National Intelligence. URL: https://www.dni.gov/files/documents/ICA_2017_01.pdf (дата обращения: 15.10.2022).

убедительные доказательства связи правительства РФ и исполнителей киберпреступлений. Основная часть публикации была посвящена анализу передач телеканала RT America TV, который «значительно расширил репертуар передач, посвященных критике предполагаемых дефектов американской демократии и гражданских свобод» и, по мнению авторов доклада, так же как и хакеры, связан с Кремлем. После публикации доклада помощник Д. Трампа в интервью телеканалу Fox News заявил: «Трамп не отрицает, что организации из России стояли за этой хакерской кампанией»[45]. Подобная формулировка была весьма расплывчатой, что объяснялось сложным положением президента США в условиях внутриполитической борьбы.

Директор ФБР Джеймс Коми в ходе слушаний о вмешательстве России в выборы, проходивших в Комитете палаты представителей по разведке в марте 2017 г., говорил о причастности России как о доказанном факте. Однако никакой информации, подтверждающей обвинения, не было представлено. Большая часть выступлений касалась переговоров между сторонниками Трампа и российскими высокопоставленными лицами в период его предвыборной компании[46].

Вместе с тем в апреле 2017 г. в США был принят законопроект «О создании независимой комиссии для изучения и представления отчетов о фактах, касающихся масштабов российских официальных и неофициальных кибероперациий и других попыток вмешательства в национальные выборы в Соединенных Штатах в 2016 году, а также для других целей»[47]. В документе говорилось о расширении действий оборонительного и наступательного характера, направленных против России.

По мнению Национального центра кибербезопасности Великобритании, «ГРУ» почти наверняка являлось так называемым виновником данных преступлений. «ГРУ» якобы стояло за хакерскими

---

[45] Priebus says Democrats to blame for email hack, thinks Trump accepts intel findings // FoxNews.com. URL: http://www.foxnews.com/politics/2017/01/08/priebus-says-democrats-to-blame-for-email-hack-thinks-trump-accepts-intel-findings.html (дата обращения: 15.10.2022).

[46] Full transcript: FBI Director James Comey testifies on Russian interference in 2016 election // The Washington Post. March 20, 2017. URL: https://www.washingtonpost.com/news/post-politics/wp/2017/03/20/full-transcript-fbi-director-james-comey-testifies-on-russian-interference-in-2016-election/ (дата обращения: 15.10.2022).

[47] S.27 — A bill to establish an independent commission to examine and report on the facts regarding the extent of Russian official and unofficial cyber operations and other attempts to interfere in the 2016 United States national election, and for other purposes // U.S. Congress. URL: https://www.congress.gov/bill/115th-congress/senate-bill/27/ (дата обращения: 15.10.2022).

группировками, такими как APT 28, Fancy Bear, Sofacy, Pawnstorm, Sednit, CyberCaliphate, Cyber Berkut, Voodoo Bear, BlackEnergy Actors, STRONTIUM, Tsar Team, Sandworm[48]. Правительство Великобритании, руководствуясь политическими соображениями, голословно возложило ответственность за киберпреступления на правительство России.

Однако обвинения в адрес России продолжали поступать. Так, в 2018 г. в США были выдвинуты «официальные обвинения» против 12 сотрудников российской военной разведки в связи с упомянутыми кибератаками[49]. В обвинительном документе были названы их имена и должности. Приводился алгоритм их действий и способы распространения в сети полученной информации. В документе фигурировала уже упомянутая выше программа X-Agent, используемая для кражи информации. В документе нет какой-либо информации, подтверждающей столь громкие обвинения. Данные обвинения нашли отражение в сообщениях информационных агентств Росси и США. Так, портал РБК опубликовал статью под названием «12 'друзей' Хиллари: в чем обвиняют США 'хакеров из ГРУ'»[50], в которой перепечатал список лиц, представленный Минюстом США и изложил ход расследования спецпрокурора США Роберта Мюллера, не касаясь вопроса кибербезопасности и технического аспекта проблемы информационной безопасности в период выборов 2016 г. Однако некоторые американские и проамериканские СМИ, например интернет-издание The Bell[51], пытались провести собственное расследование, опираясь на информацию «СПАРК-Интерфакс»[52]. В качестве аргумента приводился тот факт, что один из обвиняемых защитил кандидатскую диссертацию на тему: «Восстановление параметров дискретных устройств, основанное на

---

[48] Reckless campaign of cyber-attacks by Russian military intelligence service exposed // The National Cyber Security Centre. URL: https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed (дата обращения: 15.10.2022).

[49] United States District Court for the District of Columbia, "US v Viktor Borisovich Netyksho, et al – Indictment", July 13 2018. Unclassified // National Security Archive. https://nsarchive.gwu.edu/document/16702-indictment (дата обращения: 15.10.2022).

[50] *Солопов М., Серков Д., Пудовкин Е. Романов В., Химшиашвили П.* «12 'друзей' Хиллари: в чем обвиняют США 'хакеров из ГРУ'» // РБК. URL: https://www.rbc.ru/politics/14/07/2018/5b48f20c9a794783815ef67d (дата обращения: 15.10.2022).

[51] 01 апреля 2022 г. основательница The Bell Осетинская Е.Н. и главный редактор издания Малкова И.В. были внесены в реестр иностранных средств массовой информации, выполняющих функции иностранного агента.

[52] *Солопов М., Серков Д., Пудовкин Е. Романов В., Химшиашвили П.* «12 'друзей' Хиллари: в чем обвиняют США 'хакеров из ГРУ'» // РБК. URL: https://www.rbc.ru/politics/14/07/2018/5b48f20c9a794783815ef67d (дата обращения: 15.10.2022).

переоценке вероятностей с использованием действительных пороговых соотношений»[53]. Исходя из области научных интересов диссертанта, делался вывод о подтверждении официальных обвинений. Подобная аргументация представляется неубедительной. Стоит отметить, что программа X-Agent была широко известна уже в 2015 г.[54], а хакерами использовалась с 2012 г. (вероятно, еще раньше). Следовательно, обнаружить и защититься от нее в 2016 г. было вполне возможно. Словацкая компания ESET утверждала, что хакерами запутывание кода или «обфускация[55] была применена только к коду, специфичному для Xtunnel, в то время как статически связанные библиотеки остались нетронутыми»[56].

Детальное изучение данного документа позволяет сделать вывод, что предполагаемые хакеры активно использовали бесплатные ресурсы транснациональных компаний Google, Microsoft и Amazon, не пытаясь скрыть свои личности или делая это нерегулярно. Соответственно, американские IT корпорации активно участвовали в следственных мероприятиях и предоставили детальную информацию. Предполагаемые хакеры использовали для «фишинга»[57] и обмена информацией публичные e-mail адреса, шифруя собственную переписку. Представляется весьма странным, что хакеры, которые использовали «продвинутые инструменты» для взлома, не умели скрыть свою личность и проявляли некомпетентность в использовании простых инструментов администрирования (искали инструкцию к Power Shell в обычной поисковой системе), демонстрируя плохие знания английского языка. Можно сделать вывод, что данный документ в большей степени рассчитан на обывателя, которому достаточно показать большой объем технических деталей

---

[53] *Нетыкшо В.Б.* Восстановление параметров дискретных устройств, основанное на переоценке вероятностей с использованием действительных пороговых соотношений: дисс. … канд. техн. н. М., 2003. // Российская государственная библиотека. URL: https://search.rsl.ru/ru/record/01002627379 (дата обращения: 15.10.2022).

[54] *Hacquebord F., Fernando M.* Pawn Storm Update: iOS Espionage App Found // Trend Micro. URL: https://www.trendmicro.com/en_us/research/15/b/pawn-storm-update-ios-espionage-app-found.html?linkId=12146208 (дата обращения: 15.10.2022).

[55] От англ. obfuscate (делать неочевидным, запутанным, сбивать с толку) — приведение исходного текста или исполняемого кода программы к виду, сохраняющему ее функциональность, но затрудняющему анализ, понимание алгоритмов работы и модификацию при декомпиляции.

[56] ESET (October 2016). "En Route with Sednit" // WeLiveSecurity. https://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part-2.pdf (дата обращения: 15.10.2022).

[57] От англ. fishing «рыбная ловля, выуживание», тип киберпреступления, при котором преступники выдают себя за надежный источник в сети Интернет.

расследования, для того, чтобы убедить в существовании некого «заговора». Кроме того, отдельные фрагменты текста плохо согласуются друг с другом по содержанию, складывается ощущение, что текст готовили параллельно несколько команд, либо неумело подгоняли так называемые «факты». Стоит отметить, что значительная часть информации, упомянутая в данном отчете, не могла быть получена исключительно с помощью технических средств. Текст также не дает ответа на вопрос: «Каким образом были идентифицированы упомянутые лица, каковы доказательства связи хакеров с российским правительством или конкретным подразделением спецслужб?».

В августе 2020 г. Комитетом по разведке Сената США была опубликована пятая часть доклада о расследовании вмешательства РФ в президентские выборы[58]. Этот 966-страничный документ должен был поставить точку в расследовании. Вместе с тем большая часть документа была посвящена предполагаемой ранее связи Трампа с Россией. В докладе детально описывались интересы соратников Трампа в России, а также аналогичные интересы властных структур и бизнес элиты нашей страны в США. Как и в предшествовавшем ему докладе Мюллера, следствием не было обнаружено преступного сговора между Россией и командой Трампа. Доклад не содержит доказательств вины России. Несмотря на это, авторы сделали вывод, что «российское правительство предприняло агрессивные и разносторонние усилия, чтобы повлиять или попытаться повлиять на исход президентских выборов 2016 года»[59], а взлом компьютерных сетей был произведен по личному распоряжению президента В.В. Путина.

Детальное изучение документов позволяет прийти к выводу, что американская сторона с самого начала расследования была сосредоточена на решении двух основных проблем: во-первых, это внутренние политические вопросы, связанные с компанией против Трампа[60]; а во-вторых, геополитическое противостояние с Россией. Несмотря на сходство в подходах к решению проблем кибербе-

---

[58] Russian Active Measures Campaigns and Interference in the 2016 U.S. Election (Part 1 of 2): Volume 5: Counterintelligence Threats and Vulnerabilities // U.S. Senate Select Committee on Intelligence. URL: https://www.intelligence.senate.gov/sites/default/files/documents/report_volume5.pdf (дата обращения: 15.10.2022).

[59] Ibid.

[60] *Борисова А.Р.* США: президент под расследованием // Год планеты: Ежегодник / Национальный исследовательский институт мировой экономики и международных отношений имени Е.М. Примакова Российской академии наук (ИМЭМО РАН) Primakov National Research Institute of World Economy and International Relations, Russian Academy of Sciences (IMEMO). М.: Идея-Пресс. 2019. С. 174–184; *Кошкин П.Г.* «Российское досье» как внутриполитический фактор в

зопасности России и США[61] и расхождении в их реализации[62], в рамках данного инцидента наладить сотрудничество не удалось. Обвинения в адрес России позволили Трампу продолжить работу, направленную на усиление Киберкомандования. В 2017 г. оно было преобразовано в самостоятельное боевое командование[63]. Перспективы сотрудничества в рамках группы правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности представляются также туманными[64].

Литература

Богатуров А.Д. Попытка перестроить мир «по-американски» // Вестн. МГИМО-Университета. М. 2021. № 14 (5). С. 49–64.

Борисова А.Р. США: президент под расследованием / А.Р. Борисова // Год планеты: Ежегодник / Национальный исследовательский институт мировой экономики и международных отношений имени Е.М. Примакова Российской академии наук (ИМЭМО РАН) Primakov National Research Institute of World Economy and International Relations, Russian Academy of Sciences (IMEMO). Москва: Идея-Пресс. 2019. С. 174–184.

Бухарин В.В. Актуальные аспекты законотворческой деятельности российской федерации в области укрепления информационной безопасности в условиях COVID-19 // Вестн. Моск. ун-та. Сер. 21. Управление (государство и общество). 2023. № 1. С. 113–136.

Бухарин В.В. Компоненты цифрового суверенитета Российской Федерации как техническая основа информационной безопасности // Вестн. МГИМО-Университета. М. 2016. № 6 (51). С. 76–90.

США // Россия и Америка в XXI веке. Спецвыпуск. 2019. URL: https://rusus.jes.su/s207054760005318-6-1/ (дата обращения: 15.10.2022).

[61] *Манойло А.В.* Современные стратегии кибербезопасности и кибероборонны НАТО // Актуальные проблемы Европы. 2020. № 3 (107). С. 160–184.

[62] *Бухарин В.В.* Актуальные аспекты законотворческой деятельности российской федерации в области укрепления информационной безопасности в условиях COVID-19 // Вестн. Моск. ун-та. Сер. 21. Управление (государство и общество). 2023. № 1. С. 113–136; *Бухарин В.В.* Сравнительный анализ нормативной базы по обеспечению информационной безопасности в США и РФ (конец XX — начало XXI в.) // Вестн. Иркутского гос. технического ун-та. 2016. Т. 20, № 12 (119). С. 101–108.

[63] Statement by President Donald J. Trump on the Elevation of Cyber Command. August 18, 2017 // The White House. URL: https://trumpwhitehouse.archives.gov/briefings-statements/statement-president-donald-j-trump-elevation-cyber-command/ (дата обращения: 15.10.2022).

[64] Remarks by Homeland Security Advisor Thomas P. Bossert at Cyber Week 2017. June 26, 2017 // The White House. URL: https://trumpwhitehouse.archives.gov/briefings-statements/remarks-homeland-security-advisor-thomas-p-bossert-cyber-week-2017/ (дата обращения: 15.10.2022).

Бухарин В.В. Сравнительный анализ нормативной базы по обеспечению информационной безопасности в США и РФ (конец XX — начало XXI в.) // Вестн. Иркутского гос. технического ун-та. 2016. Т. 20, № 12 (119). С. 101–108.

Вольф М. Огонь и ярость. В Белом Доме Трампа. М.: Издательство АСТ: COPRUS, 2018. 448 с.

Горбатюк Н.В. WikiLeaks. Разоблачения, изменившие мир. Россия: Эксмо. 2022. 367 с.

Душенко К.В. «Мировая закулиса»: истоки концепции // Россия в глобальной политике. 2022. Т. 20. № 4. С. 178–186.

Кошкин П.Г. «Российское досье» как внутриполитический фактор в США // *Россия и Америка в XXI веке.* Спецвыпуск. 2019. URL: https://rusus.jes.su/s207054760005318-6-1/

Манойло А.В. Современные стратегии кибербезопасности и кибероборонь НАТО // Актуальные проблемы Европы. 2020. № 3 (107). С. 160–184.

Самуилов С.М. Внешняя политика Д. Трампа: предвыборные обещания, противоречивые шаги, угроза импичмента // США и Канада: экономика, политика, культура. 2017. № 8 (572). С. 27–44.

Самуйлов С.М. Внутренние проблемы администрации Д. Трампа и российско-американские отношения // США и Канада: экономика, политика, культура. 2018. № 6 (582). С. 5–22.

Шариков П. Информационный суверенитет и вмешательство во внутренние дела в российско-американских отношениях // *Международные процессы.* 2018. Т. 16. № 3 (54). С. 170–188.

Diesen G. Russophobia: Propaganda in International Politics. Switzerland: Springer Nature Singapore, 2022. 307 p.

Miller G. The Apprentice: Trump, Russia and the Subversion of American Democracy. United States: HarperCollins. 2020. 448 p.

Pontell H.N., Tillman R., Ghazi-Tehrani A.K. In-your-face Watergate: neutralizing government lawbreaking and the war against white-collar crime. Crime Law Soc Change. 2021. 75. P. 201–219.

Stone R. The Myth of Russian Collusion: The Inside Story of How Donald Trump REALLY Won. United States: Skyhorse. 2019. 416 p.

ИНФОРМАЦИЯ ОБ АВТОРЕ:

Бухарин Владислав Викторович — к.и.н., доцент факультета государственного управления МГУ имени М.В. Ломоносова, Москва, Россия; *e-mail:* Bukharin@spa.msu.ru

ABOUT THE AUTHOR:

Bukharin V. — PhD, Associate Professor, School of Public Administration, Lomonosov Moscow State University, Moscow, Russian Federation; *e-mail*: Bukharin@spa.msu.ru