

# № 68 ВАЛДАЙСКИЕ ЗАПИСКИ

Июнь, 2017



**Валдай** | Международный  
дискуссионный клуб

[www.valdaiclub.com](http://www.valdaiclub.com)

## КИБЕРБУНТ, КОТОРОГО НЕТ (ПОКА)

Жульен Носетти  
Елена Черненко

## Об авторах:

---

### **Жульен Носетти**

*научный сотрудник Французского института международных отношений (IFRI)*

### **Елена Черненко**

*кандидат исторических наук, руководитель отдела внешней политики газеты «Коммерсантъ», член Президиума Совета по внешней и оборонной политике, член рабочей группы ПИР-Центра по международной информационной безопасности и глобальному управлению интернетом*

*Данный текст отражает личное мнение авторов, которое может не совпадать с позицией Клуба, если явно не указано иное.*

## Кибербунт, которого нет (пока)

---

*Все условия для глобального хакерского бунта созданы, но пользователи не спешат объединяться в «виртуальный интернационал»: нет общей цели, но есть неудачный опыт первых попыток поднять «восстание машин».*

В последние месяцы и дня не проходит, чтобы СМИ не сообщили о новых – все более масштабных и изощренных – хакерских атаках. Это наводит на мысль, что речь идёт о глобальном бунте пользователей сети против властей.

Однако дело обстоит с точностью до наоборот. На протяжении многих лет казалось, что государства в *мультистейкхолдерной* (термин режет слух, но при переводе теряются нюансы) модели управления интернетом действуют лишь на вторых ролях, а тон задают бизнес и гражданское общество. Но сегодня уже нет сомнений, что именно государства выходят на первый план. Они научились по максимуму использовать возможности киберпространства для своих целей – внутренне- и внешнеполитических, разведывательных, военных. А теперь договариваются друг с другом о введении правил поведения в сети – при минимальном вовлечении бизнеса и граждан.

С учётом все более активного наступления государств на права и свободы пользователей, будь то посредством цензурных ограничений или слежки, можно было бы предположить, что глобальный хакерский бунт неизбежен. Тем более если принимать во внимание растущее в «оффлайне» недовольство устоявшимися политическими силами и институтами, что в последнее время особенно ярко проявляется как в США и странах ЕС, так и на постсоветском пространстве.

Но наблюдаемая сегодня «кибервакханалия» – это еще не политически мотивированный бунт. По большей части это результат работы обычных кибермошенников и кибервандалов, операций спецслужб и разборок внутри IT-индустрии.

В этом плане весьма показательна история с атрибуцией крупнейшей за 2016 год DDoS-атаки (Distributed denial of service, «Распределенная атака типа отказ в обслуживании»), когда в результате диверсии в отношении крупного американского провайдера доменных имен Дун «полегло» более 80 популярных новостных порталов, социальных сетей, стриминговых сервисов, включая сайты The New York Times, CNN, Amazon, Twitter, Reddit, PayPal, Airbnb, Pinterest, Netflix и Soundcloud.

Атака была произведена в три волны при помощи ботнета, включавшего в себя более 100 тысяч зараженных вирусом устройств. Причем инфицированы были не столько и даже не столько компьютеры, сколько устройства из «интернета вещей» – телевизионные приставки, камеры, принтеры и даже видеоняни. 4% скомпрометированных аппаратов находились в России. Некоторые специалисты утверждают, что все вместе эти зараженные устройства передавали данные на серверы Дун со скоростью 1,2 Тбит/с – невиданный доселе показатель для подобного рода диверсии. Ущерб от атаки оценивается в \$110 млн.

Представители скандально известного сайта WikiLeaks, специализирующегося на обнаружении секретных документов, объявили, что атака на Дун – это месть их

сторонников. Симпатизанты WikiLeaks якобы мстили за то, что создателю портала Джулиану Ассанжу, с 2012 года скрывающемуся в посольстве Эквадора в Лондоне, отключили интернет. Однако эксперты в области кибербезопасности сомневаются, что за этой атакой стояли политически мотивированные хакеры – хактивисты, тем более что представители WikiLeaks никаких доказательств своей версии не представили.

Исследователи полагают, что речь может идти либо о кибервандалах, либо о коллегах Дун. В пользу первой версии говорит тот факт, что исходный код вредоносной программы Mirai, использованной для создания ботнета, активно обсуждался на форумах хакеров-любителей, кроме того, созданная при помощи Mirai инфраструктура ранее использовалась для атаки на популярный портал видеоигр. В пользу второй версии говорит тот факт, что на Дун как раз незадолго до атаки ополчилось несколько компаний из сферы IT, поскольку аналитики провайдера выпустили доклад, в котором утверждалось, что некоторые фирмы, продающие антивирусные программы сотрудничают с хакерами, создающими искусственные угрозы.

Между тем все технические условия для глобального хакерского бунта есть. Есть и политическая мотивация.

## Источники недовольства

---

Целое поколение активистов, по сути простых граждан, стремится использовать интернет как цель и средство поступательной «демократизации». Действуют они при этом достаточно сумбурно, но при этом непоколебимо, создавая и преумножая различные дискуссионные площадки. Это необратимый процесс, который неизбежно ставит под сомнение существующие институты и позиции. Если исходить из слов американского политического теоретика немецкого происхождения Ханны Арендт о необходимости «действовать сообща», нельзя не признать, что цифровые технологии создают для этого неограниченные возможности. Рост популярности слова «empowerment», которое достаточно сложно поддается переводу на другие языки, но, по сути, означает расширение прав и возможностей людей, отражает появление возможности у отдельных людей и групп, а также их готовность реагировать на окружающую их политическую и экономическую действительность. Это касается всего общества в целом и угрожает всем символическим крепостям, включая такие неприкосновенные области, как внешняя политика, оборона и безопасность.

В западном обществе с нарастающей очевидностью развивается двоякий процесс. С одной стороны, растет недовольство населения политической системой, с которой люди перестают себя идентифицировать, а с другой – политические институты уже не способны адекватно реагировать на этот вызов. На фоне этого многоликого

кризиса «нашей» системы интернет стал орудием, площадкой и средством для выражения индивидуальных и коллективных чаяний, создавая новые возможности для восстановления доверия между гражданами и властями и для эффективного функционирования институтов.

*Использование цифровых инструментов как следствие разочарования в политике?* Охвативший западные демократии глубокий кризис по своей сути многогранен. Это и кризис участия, проявляющийся в росте абсентеизма и распространением экстремальных проявлений электорального поведения, и кризис представительства, который заключается в охватившем многих чувстве, что власть узурпирована кастой политиков, которые перестали понимать своих сограждан. Имеет место и кризис легитимности власти, а также кризис институтов, которые кажутся слишком громоздкими и непонятными. Наконец, существует кризис «эффективности», из-за которого политика перестала восприниматься как средство обеспечения поступательного развития (как личного, так и коллективного).

*Демократический ресурс?* Социальные сети заняли доминирующее положение в общении людей и в их отношениях с властями. Twitter, Facebook, ВКонтакте и их многочисленные приложения дают возможность всем получать и распространять информацию в режиме реального времени. С утверждением социальных сетей в этой роли произошёл окончательный разрыв между печатным и написанным от руки словом, показав, что виртуальная близость больше не подразумевает близости пространственной. Интернет обеспечивает наглядность, дает возможность наблюдать, осуждать и преследовать, тем самым превращаясь в «пространство» меняющегося баланса сил между отдельными субъектами, группами, властями и компаниями. Интернет играет все большую роль в процессе выборов. Так, использование обычными людьми и журналистами хештегов может иметь решающее значение для мобилизации оппозиции по проблеме безработицы или коррупции.

Действительно, на фоне кризиса и его разрушительных последствий именно социальные сети способствовали появлению таких протестных проявлений, как антикапиталистическое движение *Indignados* («Возмущенные») в Испании в мае 2011 года или движения *Occupy Wall Street* («Захвати Уолл-Стрит») в сентябре 2011 года в Нью-Йорке. Такие движения характеризуются преобладанием горизонтальных связей, сетевой структурой, неинституциональным и ненасильственным характером, что отличает их от политических партий и профсоюзов. Неизбежно появляются новые способы использования цифровых технологий в целях протеста, и власти по всему миру вынуждены к этому приспосабливаться. Так, социальные сети используются для координации протестных действий, организации флешмобов или в целях «массовых самокоммуникаций», как писал видный испанский социолог Мануэль Кастельс. Речь идет о возможности отдельного человека обратиться к глобальной аудитории, например, разместив видео на YouTube или отправив электронные письма широкому кругу адресатов. Пример устроенной гонконгскими студентами зимой 2014 года «революции зонтиков» показал возможность массового и творческого использования цифровых технологий в политических целях. Сетевые технологии также позволяют предотвращать замалчивание актов насилия. В 2015 году жестокие действия полиции в американском Балтиморе были засняты на мобильные

телефоны и мгновенно оказались в социальных сетях. Такие репортеры/активисты формируют собственный нарратив о протесте, создавая побуждающие к действиям хештеги, например, #Ferguson или #ICantBreathe («Не могу дышать»), которые распространяются по всему миру. Некоторые такие хештеги, например, #BlackLiveMatters (лозунг «Жизнь чёрных имеет значение») даже попали на обложку журнала *Time*.

Нельзя сказать, что выступающим против установившихся порядков людям совершенно чужды соображения идеологического характера. В основе присущих интернету либертарианских общих ценностей лежит требование обеспечения «прозрачности»<sup>1</sup>. Крупнейшие цифровые компании также возвели прозрачность в разряд своих основных принципов, хотя ее достижение подчас остается невозможным. Не они ли положили в основу своих отношений с пользователями принцип «взаимной прозрачности»?

Неудивительно, что в основе создания физической и программной инфраструктуры интернета лежала популярная в те времена либеральная идея «свободного обмена информацией». Пожалуй, наиболее важным элементом дискурса США стало увязывание свободного обмена информацией и открытости интернета с необходимостью защиты и поощрения всеобщих прав человека на свободу слова и самовыражение. Представители администрации как Буша, так и Обамы постоянно подчеркивали взаимосвязанность идеи свободного обмена информацией со свободой выражения мнений и правами человека<sup>2</sup>. Этим объясняется укоренившееся в некоторых странах мнение, что официальный дискурс США по вопросу о свободном интернете не может не влиять на общественное мнение и отдельных граждан во всём мире, хотя обнародованная Эдвардом Сноуденом и WikiLeaks информация основательно подорвала моральный авторитет США как гаранта свободы интернета.

## Новая угроза

---

Методы деятельности могут быть разными, в зависимости от того, желает ли человек или организация оставаться в рамках закона или считают необходимым выйти за его пределы.

Например, сложно сравнивать действия WikiLeaks, Anonymous («Анонимы») и Telecomix. В этой связи необходимо понять политическую мотивацию, стоящую за деятельностью различных групп или проектов.

---

<sup>1</sup> Turner F. *From counterculture to Cyberculture* / S. Brand // *The whole Earth network and the rise of Digital Utopianism*. Chicago: University of Chicago Press, 2006.

<sup>2</sup> Mccarthy D. *Power, information technology and international relations theory* / *The Power and politics of US foreign policy and the Internet*. Basingstoke: Palgrave Mcmillan, 2015.



В настоящее время проект WikiLeaks завязан на Джулиане Ассанже, который вот уже как семь лет не может покинуть посольство Эквадора в Лондоне, а также на Челси Мэннинг (ранее известной под именем Брэдли Мэннинг), которая была приговорена к 35 годам лишения свободы в августе 2013 года за организацию утечки секретных документов. WikiLeaks без зазрения совести отвергает принцип «государственного интереса», выступая в качестве контрвласти. События 2010 года ознаменовались целым рядом «нестыковок»: между притязаниями привилегированной элиты на конфиденциальность и требованием прозрачности со стороны масс, между монополией на процесс принятия политических решений и желанием построения более открытого демократического общества, а также между скрытной правящей кастой и молодым поколением, для которых Facebook задал новую матрицу восприятия окружающей реальности.

Примечательно при этом, что сам факт публикации на сайте WikiLeaks секретных документов о военных операциях США в Ираке и Афганистане, а также переписки американских дипломатов в итоге не привел к существенным изменениям в мировой политике. Между тем, когда WikiLeaks только приступил к обнародованию оказавшихся в его распоряжении бумаг, многим казалось, что сдвиги будут титаническими. Самая яркая формулировка тех дней принадлежит бывшему главе МИД Италии Франко Фраттини: «Публикации WikiLeaks станут 11 сентября для мировой дипломатии». Да и сам Джулиан Ассанж утверждал, что разоблачения «взорвут мир». Однако в итоге ни одна страна не разорвала отношения с другой, и ни одно правительство не ушло в отставку. С тех пор было еще несколько масштабных утечек секретных данных (и они продолжаются), но на мировую политику и они повлияли в куда меньшей степени, чем можно было бы ожидать. Так, например, канцлер ФРГ Ангела Меркель не перестала ездить в США, узнав, что американские спецслужбы на протяжении долго времени прослушивали ее мобильный телефон. А высокопоставленные представители стран «Группы 20» не отказались от проведения саммитов этой структуры, несмотря на то, что порой хозяева используют подобные мероприятия для того, чтобы получить доступ к компьютерам и гаджетам членов делегаций (как делали британцы в 2009 году). В целом же можно сказать, что государства уже выработали устойчивость к подобного рода утечкам.

Однако у подобных разоблачений всё же был неоспоримый эффект: они ещё больше усилили недоверие граждан к политическим лидерам и институтам. Недовольство сложившейся ситуацией и желание хотя бы защитить свое право «знать» – раз уж на мировую политику или практики спецслужб повлиять невозможно – привели самых продвинутых из них в ряды хактивистов.

Группа Anonymous («Анонимы») – самое известное из хактивистских движений – представляет собой широкий спектр сообществ интернет пользователей, выступающих в роли защитников права свободно выражать свое мнение в интернете и за его пределами. Но на современном этапе эта «галактика», похоже, уделяет больше внимания выявлению уязвимостей в компьютерных системах организаций, нежели преследованию каких-либо политических целей. Хотя именно Anonymous пока по сути можно назвать единственным реальным примером глобального кибербунта. WikiLeaks и Anonymous поддержали Эдварда Сноудена, нашедшего временное убежище в России в июле 2013 года. В Россию он приехал в сопровождении юридического консультанта WikiLeaks

Сары Харрисон. Крупнейшие международные газеты решили опубликовать предоставленную Сноуденом информацию. Действия Telecomix освещались в СМИ гораздо меньше. Эта организация пыталась восстанавливать возможность пользоваться социальными сетями и средствами связи в странах, где такие ресурсы были «отключены» властями для противодействия протестным выступлениям, например, в Тунисе, Египте и Сирии.

Интернет-культура зародилась во второй половине 1960-х годов. При этом с самого начала в ее основе лежали два, казалось бы, совершенно разных источника, которые, однако, тесно переплетаются, учитывая специфику организации исследовательской деятельности в США. Первый источник представляет собой оборонный исследовательский проект по созданию компьютерной сети Agranet, а второй источник представлен культурой протеста, в частности, против военных действий США во Вьетнаме. Интернет-культура напоминает контркультуру, основанную на принципах обмена и взаимодействия. Она очень разнообразна. Ее проводниками являются истинные либералы (в том смысле, который в этот термин вкладывают в США), либертарианцы, радикальные анти-капиталисты, анархисты, компьютерные фанатики или, попросту говоря, интернет-пользователи, поставившие своей целью отстаивать свободу слова, общения и организации<sup>3</sup>. В этом отношении можно было бы провести историческую параллель между делом Сноудена и делом о «Документах Пентагона» (*Pentagon Papers*). Именно анализ ситуации с публикацией «Документов Пентагона» навел Ханну Арендт на мысль о «процессах, в которых сочетаются решения властей» и механизмы, с помощью которых ответственные за принятие решений вводят людей в «заблуждение»<sup>4</sup>. В 1971 году аналитик корпорации RAND Даниэль Эллсберг передал 7 000 страниц секретной информации о действиях США во Вьетнаме газете *The New York Times*. Естественно, впоследствии он поддержал Джулиана Ассанжа и Челси Мэннинг. В опубликованной в 2013 году статье Даниэль Эллсберг заявил, что возможности разведывательных служб США по вторжению в частную жизнь «значительно расширились по сравнению с доцифровой эпохой». По его мнению, Эдвард Сноуден раскрыл информацию о нарушении основополагающих личных и общественных свобод «с риском для своей жизни», что должно послужить примером для тех, «кто обладает подобной информацией и испытывает такое же чувство долга и патриотизма для проявления гражданского мужества»<sup>5</sup>. В конце сентября 2013 года Конгресс США дал старт реформе Агентства национальной безопасности с целью ограничить программы наблюдения, не подрывая их «эффективности».

Разведывательным службам как в авторитарных, так и в демократических странах следует опасаться возникновения «цифровой волны». С 11 сентября 2001 года мировое общественное мнение постоянно убеждали, что основной угрозой является международный терроризм в лице «Аль-Каиды». Дело Сноудена привело к смене парадигмы, однако, эта проблема не стала предметом обсуждения среди широких слоев населения<sup>6</sup>.

<sup>3</sup> Foust J. *The Geek Awakening, Edward Snowden is the vanguard of a broader challenge* // *Medium.com*. - 2013. - 4 July.

<sup>4</sup> Arendt H. *Crises of the republic*. New York: Mariner Books, 1972.

<sup>5</sup> Ellsberg D. *Aux Etats-Unis, une cybersurveillance digne d'un Etat policier* // *Le Monde* - 2013. - 26 July.

<sup>6</sup> Gomart T. *Aux démocraties de montrer l'exemple* // *Le Monde*. - 2013. - 30 October.



## Первая волна

Но пока только одну такую волну можно назвать настоящим глобальным хакерским бунтом. Речь о движении Anonymous периода 2010–2011 годов. Тогда тысячи хакеров, да и обычных пользователей со всего мира, объединили свои усилия, чтобы отомстить властям США и ряда других стран за давление на WikiLeaks. Основатель WikiLeaks Джулиан Ассанж многими воспринимался как главный борец за свободу слова, а его детище – как символ новой эпохи, при которой государства не смогут утаивать информацию от граждан. Возмущенные утечкой в сеть сотен тысяч секретных документов, власти США пытались заставить компании отказаться от сотрудничества с Wikileaks. Под давлением Вашингтона контракты с порталом разорвали несколько крупных платежных систем и хостинговых сервисов. Джулиану Ассанжу стало куда сложнее принимать пожертвования и поддерживать доступность портала.

За Wikileaks вступилось хактивистское движение Anonymous. К рубежу 2010–2011 годов оно уже существовало несколько лет, но было известно лишь в узких кругах – в основном за счет нескольких успешных взломов электронных ресурсов Саентологической церкви, а также активными действиями в поддержку торрент-трекера Pirate Bay («Пиратская бухта»). Объявив о начале Operation Payback («Операция Возмездие») анонимусы стали собирать под своими знаменами тысячи неравнодушных пользователей со всего мира. Их девизом стали слова Джона-Перри Барлоу, одного из создателей правозащитной организации Electronic Frontier Foundation («Фонд электронных рубежей»): «Первая серьезная информационная война началась. Поле битвы — WikiLeaks. Солдаты — это вы»<sup>7</sup>.

Принять участие в наступлении на недружественные Wikileaks сайты мог каждый желающий: пошаговые инструкции по тому, как осуществить DDoS-атаку при помощи простой программы (Low Orbit Ion Cannon или LOIC, «Низкоорбитальная ионная пушка»), распространялись в тематических чатах и в сети микроблогов Twitter. В итоге к атакам на сайты Mastercard, Visa, Paypal и Amazon присоединились пользователи со всех континентов. Абсолютное большинство из них никогда раньше хакерством не занимались.

Массовость обеспечила успех кампании – несколько правительственных и коммерческих ресурсов удалось на время вывести из строя. В 2012 году американский журнал Time включил Anonymous в список ста наиболее влиятельных людей года.

Многие эксперты тогда сочли, что хактивизм будет только набирать обороты, и что впредь политически мотивированные пользователи будут подобным образом реагировать на любую несправедливость<sup>8</sup>. Однако вскоре эта волна стихла и в таком масштабе больше не повторялась.

<sup>7</sup> Твит Джона-Перри Барлоу опубликован 3 декабря 2010 года на его странице в Twitter @JPBarlow.

<sup>8</sup> См. например: Mikhaylova G. *The Anonymous movement: hacktivism as an emerging form of political participation: thesis* // Texas State University. – 2014. URL: <https://digital.library.txstate.edu/bitstream/handle/10877/5378/MIKHAYLOVA-THESIS-2014.pdf?sequence=1>; McLaughlin V. *Anonymous: What do we have to fear from hacktivism, the lulz, and the hive mind? : thesis* // University of Virginia. – 2012. URL: [https://pages.shanti.virginia.edu/Victoria\\_McLaughlin/files/2012/04/McLaughlin\\_PST\\_Thesis\\_2012.pdf](https://pages.shanti.virginia.edu/Victoria_McLaughlin/files/2012/04/McLaughlin_PST_Thesis_2012.pdf)

Причин тому, что за первым кибербунтом не последовали другие, несколько. Во-первых, у движения Anonymous не было лидера или хотя бы некоего ядра, которое взяло бы на себя координацию совместных действий и мотивировало бы участников на продолжение борьбы. В прессе от имени движения мог выступить любой из его членов. В чатах, где обсуждались цели и время атак, также все происходило достаточно хаотично, а после первых успешных диверсий там начались ожесточенные споры относительно дальнейших мишеней. В то время как большинство «анонимов» с Запада продолжали дисциплинированно атаковать сайты отказавшихся от сотрудничества с Wikileaks платежных систем, среди русскоязычных хактивистов начали раздаваться призывы «ударить по Пентагону».

Во-вторых, многие из тех, кто изначально симпатизировал Джулиану Ассанжу, вскоре разочаровались в нем. Одних отпугнули предъявленные ему обвинения в сексуальных домогательствах. Других смутило, что Wikileaks начали один за другим покидать ключевые сотрудники, обвинившие Ассанжа в нецелевом расходовании многомиллионных пожертвований. Третьи не согласились с решением Джулиана Ассанжа выкладывать в сеть секретные документы «без купюр», то есть со всеми именами и адресами, несмотря на то, что это создавало угрозу жизни для некоторых из упомянутых лиц (например, информаторов американских войск в Афганистане).

В-третьих, как только Anonymous начали активно рекрутировать сторонников в Facebook и Twitter, их аккаунты были заморожены, а несколько их сайтов (например Anonops.net) сами подверглись атаке и надолго «легли на дно». Лишенные площадки для общения «анонимы» долго не могли собраться с силами. Среда, благодаря которой хактивисты появились на свет, оказалась их ахиллесовой пятой.

Ну и наконец, угасанию бунта явно способствовало преследование членов движения со стороны правоохранительных органов США. После нескольких громких арестов и показательных судебных процессов количество желающих поучаствовать в атаках заметно поубавилось. Примечательно, что действия хактивистов осудил и их кумир Джон-Перри Барлоу, назвавший DDoS-атаки «ядовитым газом киберпространства».

Anonymous осуществили еще несколько «операций», уже не связанных с Wikileaks, однако ни одна из них не была столь успешной, как «Возмездие». Сегодня под брэндом Anonymous действует несколько разрозненных хакерских группировок, однако они все больше занимаются взломами «just for the lulz» – ради развлечения.

Угасание первой волны хактивизма не означает, что не будет второй и третьей. Судьба этого общественного феномена будет во многом зависеть от того, найдется ли такой же мощный объединяющий фактор, каким в свое время было желание поддержать Wikileaks и тем самым отстаивать свое право на доступ к информации. Можно предположить, что при наличии общей цели объединить людей в следующий раз будет даже проще, поскольку они уже знают, каких результатов можно добиться сообща. И не факт, что бунтовщики ограничатся одними лишь DDoS-атаками.

До того, как движение сошло на нет, наиболее активные его члены обсуждали возможность совместных действий иного плана. Например, предполагалось, что опытные хакеры будут менять внешний вид сайтов при помощи defacement-атак («искажение»), оставляя на них призывы к протестам и другую подобную информацию, а хактивисты-любители будут помогать «раскручивать» эти акции в социальных сетях, через мессенджеры и т.п. Или же что обладающие хакерскими навыками активисты будут взламывать почтовые серверы официальных лиц и государственных структур, скачивать переписку, а рядовые члены будут изучать ее на предмет компромата и помогать распространять его. Несколько таких диверсий Anonymous даже смогли осуществить – в частности, они взломали почтовый сервер частной американской разведывательно-аналитической компании Stratfor и «слили» переписку (200 гигабайт информации) Wikileaks. Таким же образом в распоряжении Wikileaks появилась переписка людей из окружения сирийского президента Башара Асада.

Впрочем, в случае со взломом почтового сервера Национального комитета Демократической партии США и людей из окружения экс-кандидата в президенты Хиллари Клинтон Джулиан Ассанж дал понять, что это дело рук не хактивистов и не российских спецслужб (как то утверждают американские власти): информацию якобы предоставил инсайдер.

**#Valdaiclub**

 ValdaiClubRu

 ValdaiClubRu

[ru.valdaiclub.com](http://ru.valdaiclub.com)

[valdai@valdaiclub.com](mailto:valdai@valdaiclub.com)

ISBN 978-5-906757-52-4



9 785906 757524



СОВЕТ ПО ВНЕШНЕЙ И ОБОРОННОЙ ПОЛИТИКЕ



Российский совет  
по международным  
делам



МГИМО  
УНИВЕРСИТЕТ



НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ  
УНИВЕРСИТЕТ