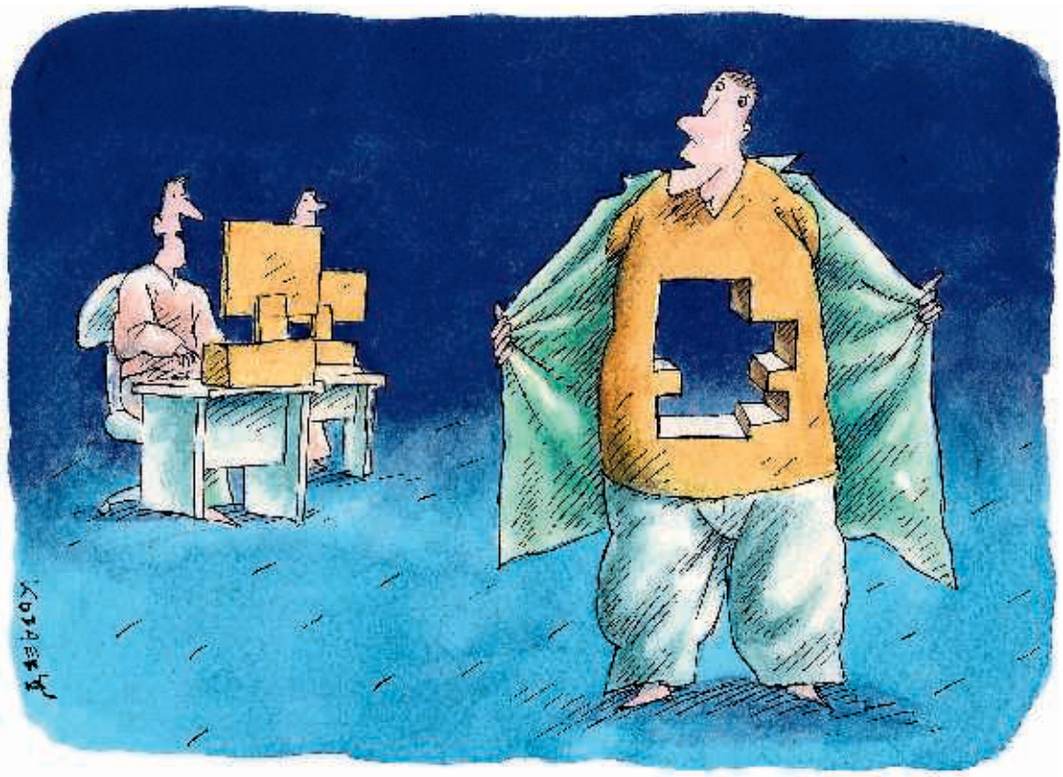
Мегабайты зла



В Интернете начался глобальный передел мира. Скандал с WikiLeaks — видимая часть этого айсберга. А что скрыто?

Елена Покатаева

ДАЙ ПОРУЛИТЬ

Итальянская редакция журнала Rolling Stone назвала Джулиана Ассанжа, владельца скандального сайта WikiLeaks, рок-звездой года и изобразила его на обложке в облике героя Дэвида Боуи из фильма «Человек, который упал на землю». Настоящая, дескать, звезда по размаху дерзаний. Правда, это мог быть и последний «звездный» полет данной персоны. Более прагматичный журнал Time, почти купившийся на имидж безумного ученого, вступившего в неравный бой с циничной мировой политикой, в последний момент передумал и назвал Человеком года Марка Цукерберга, основателя социальной сети Facebook. И правильно сделал, поскольку личный ум и масштаб содеянного Цукербергом вызывают уважение, а вот филиппики в отношении Ассанжа стоит произносить осторожно. Это становится очевидным, если проанализировать проект WikiLeaks с позиций здравого, скажем сугубо технологического, смысла.

Оседлавший облако

Возьмем, например, миф о техническом гении Джулиана Ассанжа и его выдающихся хакерских способностях. Опрос IT-специалистов показал, что построенная Ассанжем техническая система не представляет собой ничего выдающегося. «Это стандартное, простое и легко тиражируемое техническое решение, — говорит Руслан Заединов, заместитель генерального директора компании КРОК. — Мы такие используем в своих внутренних проектах, поскольку они позволяют легко и удобно создавать нужные в данный момент системы коммуникаций». Большой и сложной системы хранения данных не требуется, достаточно одного-двух стандартных серверов. Причем их вовсе не нужно размещать во всех точках присутствия WikiLeaks. «Достаточно арендовать несколько виртуальных серверов, лучше у разных провайдеров, в разных странах мира и разместить контент удаленно на каждом из них», — рассказывает Павел Поддубный, начальник отдела развития сервисов сети группы компаний «Оверсан». Этот подход давно известен и называется облачными вычислениями.

«Облачные технологии позволяют создавать копии для резервного хранения, держать отдельные части контента на разных серверах, затрудняя несанкционированный доступ к полному материалу и предотвращая угрозу уничтожения информации, — поясняет Кристина Танцюра, ве-

Кто стоит за WikiLeaks?

Руслан Заединов,
заместитель генерального директора компании КРОК
До сих пор появление данных носило случайный характер. Если судить по внешним признакам, техническая инфраструктура не всегда была готова к обработке новых порций. Интересно, на какие темпы роста закладывались руководители проекта изначально. Если рост объемов «ворованных» данных продолжится с такой же силой, думаю, можно будет сказать, что помыслы Ассанжа не совсем чисты, то есть «сливы» организуются при содействии владельцев этой информации.

Алексей Воронцов,
ведущий эксперт компании «Инфосистемы Джет»
Большая часть данных, опубликованных на WikiLeaks, — это инсайдерская информация. Но краеугольный камень архива «слитой» информации — это обеспечение доверия к ресурсу не только со стороны читателей, но и потенциальных поставщиков информации. Думаю, что большая часть материалов передана WikiLeaks теми, кто имел легальный доступ к правительственным системам. И не исключено, что часть утечек согласована с теми или иными политическими структурами.

Максим Тимонов,
политолог, специалист по интернет-технологиям
Это широкомасштабный информационный проект, который можно использовать для проведения глобальных информационно-военных операций. При таких объемах материалов всерьез говорить о «независимости» как-то даже неприлично. Просто потому, что тогда пришлось бы допустить существование некоей транснациональной организации, чьими агентами влияния пронизаны Пентагон, Белый дом и т. п. Но этот вариант скорее проходит по ведомству Жюля Верна и Яна Флеминга.

дущий специалист по маркетингу и продажам компании CA. — Ведь даже при полном уничтожении информации на одном из серверов или его физическом повреждении при помощи «суммы» копий на других серверах можно легко восстановить исходную информацию». Более того, загружать новую порцию информации можно через любой сервер, и она будет автоматически копироваться на все остальные. Сервисы облачных технологий, позволяющие синхронизировать данные через Интернет, сегодня доступны любому пользователю. По оценкам Танцюры, такой сервис для хранения данных объемом 100 Гб обойдется в 50 долларов в год.

«Эту информацию можно «размазать» по миллиону компьютеров и собирать для громких публикаций в любом удобном месте, — резюмирует Андрей Колесников, директор Координационного центра домена RU. — Ассанж использует бренд WikiLeaks для удобства и раскрутки проекта». Иными словами, широко известное сегодня имя сайта является только единой точкой входа в данный проект. Дело в том, что у любого ресурса есть уникальный физический IP-адрес сервера, на котором размещены данные. Правда, пользоваться им не очень удобно, потому что он представляет собой не запоминаемые обычным человеком группы цифр, разделенных точками. А вот доменное имя (DNS-имя) типа wikileaks.org — оно, конечно, связано с IP-адресом, но удобнее для запоминания — не зависит от физического местоположения сервера. Ресурс может переехать на другой сервер в другую страну, при этом физический IP-адрес поменяется, а DNS-имя — нет.

Это свойство адресов удобно использовать для повышения отказоустойчивости всей системы. Интернет-провайдеры предлагают такую возможность в виде отдельной услуги. О том, как она работает, рассказывает Павел Поддубный: «Допустим, пользователь запрашивает адрес wikileaks.org. Запрос отправляется на DNS-сервер, который выбирает один сервер из подготовленного заранее списка и сообщает его компьютеру пользователя». И, кроме того, распределенная система серверов ресурса позволяет бороться с DDoS-атаками, ведь «сила» атаки, ведущейся по адресу wikileaks.org, распыляется между множеством серверов, поддерживающих ресурс.

Для технической реализации такой информационной системы быть продвинутым айтишником вовсе не обязательно, достаточно привлечь в проект профессионального системного администратора. А можно просто обратиться в коммерческий центр обработки данных (ЦОД). По оценкам Руслана Заединова, аренда IT-систем проекта WikiLeaks обойдется в 5—7 тысяч долларов в год. А можно не гнаться за дешевизной и потратить более серьезную сумму (но вовсе не астрономическую), заказав в ЦОДе максимального уровня надежности услугу стопроцентного аутсорсинга всех ресурсов (как технических, так и людских) с гарантией простоя не более 24 минут в год. Может быть, Ассанж так и сделал? Говорят, что он электронные документы так припрятал, что никаким правоохранительным органам до них нипочем не добраться.

Действительно, в мире есть ЦОДы, которые предоставляют клиентам такие гарантии. В Голландии, например, в качестве ЦОДа используется подземный бункер, бывший военный объект, который владелец центра выкупил вместе с землей. И объявил себя независимым государством, где не действуют никакие международные законы, касающиеся раскрытия данных клиентов. Но у профессионалов подобные гарантии тайны ничего, кроме улыбки, не вызывают. «Хранение тайны клиентов работает лишь до определенного момента, — поясняет Олег Наскидаев, руководитель департамента маркетинга и развития компании DEAC. — У любого государства в мире есть соответствующие рычаги, чтобы повлиять на любой внешний ЦОД. Вопрос лишь в том, есть ли желание этот ресурс закрыть». Amazon.com, уверен эксперт, не просто так выселил WikiLeaks со своих ресурсов — произошло реальное административное давление на руководство.

В общем, самое худшее, что может ожидать клиента ЦОДа, нарушившего законодательство той страны, где он публично размещает данные, это отключение ресурса от Интернета и преследование по закону. Поскольку прегрешения Ассанжа перед законом исчерпываются невнятной историей с двумя шведскими барышнями, сайт WikiLeaks без всяких преследований спокойно переехал в Европу. «Это не такая большая проблема, как может показаться,— говорит Руслан Заединов. — Оборудования-то всего — максимум стойка 1,5x1,5x2,0 метра весом полторы тонны. Такой контейнер DHL за несколько дней доставит с максимальными предосторожностями в любую точку планеты».

Иными словами, хранение сенсационных материалов не доставляет Ассанжу никакой головной боли. А вот как он обеспечивает заметное присутствие материалов в Интернете?

Все страньше и страньше

Для масштабного тиражирования информации давно применяется подход, называемый «зеркалированием» содержимого исходного сайта на ресурсах сторонников проекта. «Технически это сделать просто, — рассказывает Сергей Рыжиков, генеральный директор «1С-Битрикс». — Администратор сайта-сподвижника просто предоставляет сотрудникам WikiLeaks доступ к своему сайту с помощью системы удаленного управления серверами, а те закачивают на этот сервер свои материалы». Хоть гигабайтами. При использовании облачных технологий и виртуальных серверов создать зеркало сайта — вопрос одного часа, так что получить к середине месяца почти 2200 зеркал — задачка простая, были бы сочувствующие. Если к зеркалам добавить систему балансировки нагрузки, например, на основе DNS-сервера или системы распределения запросов по странам, это еще более повысит устойчивость проекта. По-научному такое техническое решение называется системой доставки контента. Оно также типовое и используется многими поставщиками контента в разных странах.

А как насчет необыкновенных технологий, которые позволяют Ассанжу получать краденые данные от своих источников, сохраняя их анонимность? Это давно известная технология по имени Tor. Она подробно описана в «Википедии», причем данной статье народной энциклопедии, гово-

ЭКСПЕРТ

Между строк

Наталья Касперская,
генеральный директор InfoWatch

Есть во всей истории с WikiLeaks один интересный вопрос: зачем Джулиану Ассанжу понадобилось вываливать в Интернет такое огромное количество информации? Чтобы поглумиться над спецслужбами, пытающимися очистить ресурсы Сети от «слива»? Но «зачистить» однажды опубликованную в Сети информацию практически невозможно. Любые удаления информации с сайтов рассчитаны только на широкую и технически не просвещенную аудиторию. Любой человек, владеющий искусством составления поисковых запросов, без особого труда найдет нужную ему информацию. Тем более найдет аналитик, оснащенный специализированными программами поиска.

За шпионаж и разглашение гостайны владельца WikiLeaks привлечь невозможно, поэтому вся суета вокруг сайта несет исключительно пропагандистский характер. Правда, идея реализации не то чтобы очень оригинальная — подобных проектов всегда было в избытке. Но до сих пор их популярность была невысока, поскольку капитализировать компромат в Сети очень сложно. Сайт, как правило, живет за счет рекламы, но ее с трудом хватает на покрытие затрат хостинга. WikiLeaks вышел в «хэдлайнеры» благодаря ударной дозе «рекламы» от Пентагона и Госдепа США, которые начали преследование владельца данного ресурса. А вот по умыслу или же неведению они сделали это — вопрос остается открытым.

Аналогичное по масштабу коммерческое продвижение любому другому сайту обошлось бы в миллионы долларов, поэтому ожидать лавинообразного «клонирования» и серии новых «разоблачений» от потенциальных конкурентов WikiLeaks не стоит. И еще потому, что оглашенные утечки — очевидный результат злонамеренных действий инсайдера. Но вот как он добрался до секретных баз? Известно, что доступ к данным был открыт инсайдеру по должностному статусу, однако полномочия рядового Мэннинга небезграничны. Это и настораживает...

рят специалисты, можно вполне верить. Tor еще называют «луковой» маршрутизацией, так как она использует шифрование пакетов передаваемых данных на трех уровнях, причем на каждом уровне расшифровывается одна «чешуйка» луковицы, которая сообщает, куда передать пакет дальше. Технология была разработана сотрудниками исследовательской лаборатории Военно-морских сил США по федеральному заказу. В 2002 году ее рассекретили, и с тех пор она живет и здравствует в виде свободного ПО, дистрибутив которого поддерживает известная американская организация по защите гражданских свобод Electronic Frontier Foundation. Это ПО весьма популярно не только в журналистской среде и среди организаций, работающих за границей с деликатными миссиями, но и, скажем, для общения социальных служб с жертвами насилия, беженцами и т. д.

Разработчики любого коммерческого ПО обычно оставляют «черные входы» (доступные только им) в свои творения, а уж военные — точно. Потому обычному интернет-провайдеру разыскать источник данных, пользующийся технологией шифрования Tor, будет действительно непросто. Но не спецслужбам, знающим «черный вход», — нужно только желание добраться до этого адресата.

Так что с точки зрения IT ничего уникального в проекте WikiLeaks нет. Но вот что действительно удивляет, так это темпы роста его популярности. Конечно, дело в секретных документах. Но с ними связано много странностей.

Так, в США подавляющее большинство государственных и коммерческих компаний давно обзавелось специальными системами обнаружения утечек данных (DLP-системами). Они, рассказывают специалисты компании InfoWatch, умеют многое. Например, отличать целенаправленный поиск информации от ее неразборчивого «слива»; работу с документами из своей области интересов от залезания в «чужие» категории; чтение/просмотр глазами от автоматизированного копирования; статистику типичного клерка или аналитика от статистики робота. Они в состоянии дать необходимый доступ всем легальным пользователям, но блокировать при этом массовые, нетипичные обращения к базе или «не по интересам». Таких продуктов на рынке немало, их может приобрести любой заказчик.

Получается, что DLP-системы Пентагона и Белого дома, которые должны быть на порядок внимательнее и умнее, чем их гражданские собратья, проморгали утечку миллионов документов?

«Если принять версию Ассанжа, это означает либо полную и тотальную коррупцию на всех уровнях, причем коррумпированные чиновники готовы сдавать документы за кружку пива, — говорит Максим Тимонов, политолог и специалист по интернет-технологиям. — Либо же в США предреволюционная ситуация, и офицерский корпус вместе с чиновниками готов перейти на сторону восставшего народа. Не похоже на правду. Следовательно, можно усомниться в бескорыстии и анонимности источников».

Анонимности в Интернете сегодня не может быть даже для обычных граждан, не то что для шпионов. А электронная почта, утверждают специалисты по информационной безопасности, это самый ненадежный и неанонимный канал связи. Они уверены, что свои материалы информаторы присылают обычной почтой — высокие технологии для этих целей не годятся.

В общем, «герой» Ассанж может существовать только в контексте мифа об Интернете как территории свободы и анонимности. А может быть, сам Джулиан Ассанж — тоже миф? Ведь даже если бы такого реального персонажа не существовало, его следовало бы придумать. Потому что его проект WikiLeaks очень нужен. Именно сегодня. Но совсем не тем энтузиастам свободы и открытости, о которых нам уже прожужжали все уши.

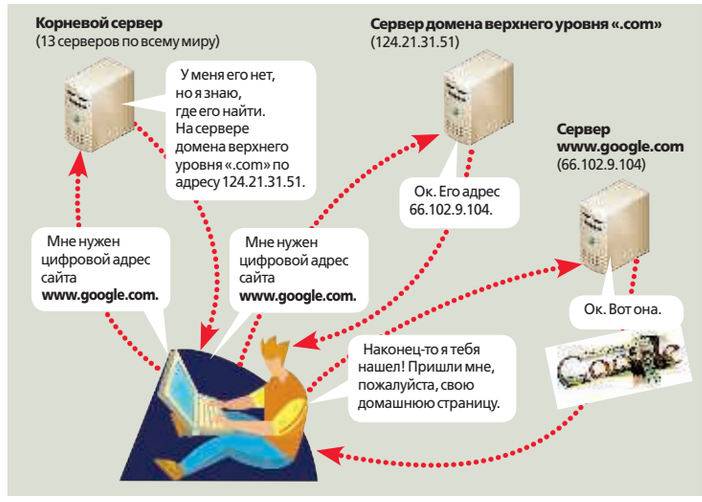
Высокие ставки

Вот еще один миф — о том, что Интернет абсолютно децентрализован и по своей сути неконтролируем. Увы, это не совсем так. Для того чтобы сонмы компьютеров могли свободно общаться каждый с каждым, придумана жесткая структура управления именами в Интернете (см. рисунок), в центре которой 13 корневых серверов имен. Когда пользователь заходит на какой-нибудь веб-сайт, эти корневые серверы соотносят введенное доменное имя с соответствующим IP-адресом, либо напрямую, либо передают задание поиска этого адреса одному из DNS-серверов верхнего уровня, каждый из которых отвечает за определенный тип сайтов, например com, org, ru, eu и т. д. А те уже ищут среди «своих» нужный IP-адрес. Когда мы приобретаем у компании-регистратора новое доменное имя, мы фактически сообщаем всей этой системе о появлении нового элемента. IP-адрес любого устройства, присоединенного к Сети, уникален, так что система управляющих серверов знает, как найти каждого из них.

Именно система доменных имен — главная ценность Интернета, но до сих пор мир спорит, кто должен ею владеть. Точнее, факт «общественного достояния» никто на словах не отрицает. Соединенные Штаты считают, что создание в 1998 году международной организации ICANN — Интернет-корпорации по присвоению имен и адресов в Интернете (Internet Corporation for Assigned Names and Numbers) уже и так означает их добровольный отказ от контроля над системой доменных имен. Правда, некоторые страны усматривают и в этом хитрый ход Вашингтона, который сохранил свою гегемонию, передав управление Интернетом — через ICANN — в американский частный сектор. Ведь корневая зона — единственный источник данных, используемый всеми корневыми серверами, — это серверные мощности, управляемые VeriSign, известной американской компанией из сферы информационной безопасности, и контролируемые США через комиссию Минторга.

Нынешней осенью наблюдалось очередное сезонное обострение этих противоречий (которое чудесным образом совпало с активизацией WikiLeaks). Причем, замечает Андрей Колесников, если прежде США подчеркивали ценность саморегулирования, то есть «общественного» управления в сфере адресации Интернета, то ныне дебаты идут о возрастающей роли государств и правительств в управлении им. Вопрос ставится ребром: нужно ли из соображений повышения эффективности управле-

Как работает Интернет?



ИСТОЧНИК: ЛОВАН КУРБАЛИЯ

ТЕХНО-МОДА

Не узнаю вас в гриме...

Компания Symantec сообщила на днях, что наблюдает волну спама, имитирующего сообщения от WikiLeaks. Падкий на сенсации интернет-пользователь, конечно, обратит внимание на тему электронного письма — ИРАНСКАЯ ядерная БОМБА! А когда увидит, что в поле «ОТ» указан отправитель по имени Wikileaks.org, он, безусловно, захочет почитать, что новенького «слил» Ассанж про ядерные программы Ирана. Пользователь даже сможет прочитать какой-то текст. Правда, он не имеет никакого отношения к документам, выложенным на WikiLeaks. На самом деле в теле письма содержится веб-ссылка, которая загружает и запускает совсем другой сайт, но с похожим названием — Wikileaks.jar. В результате на компьютер пользователя попадает вредоносное ПО, причем ранее неизвестное антивирусным аналитикам. Этому неизвестному науке зверю обнаружившие его специалисты Symantec дали наименование W32.Spyrat.

ния Интернетом делегировать эти полномочия правительствам разных стран или все-таки оставить при руле и общественные объединения интернетчиков?

В том, что намерения правительств самые серьезные, сомневаться не приходится — слишком уж значимой силой стал Интернет. Помните, что сказал генерал-лейтенант ВВС США Роберт Элдер-младший по поводу вируса Stuxnet? «Нашим приоритетом станет деятельность в киберпространстве, которая в случае необходимости будет сопровождаться действиями в воздушном пространстве и на земле». А страны НАТО обсуждают, пора ли записать в своей стратегии развития в явном виде, что агрессивные действия в Интернете рассматриваются как основание для нанесения совместного военного удара.

В этом контексте проект WikiLeaks активизировался как нельзя кстати — в самое горячее время дискуссий, наглядно показав, что нынешняя система управления неспособна наладить трансграничные механизмы борьбы с киберпреступниками. И объект нападок Ассанжа понятен — затронуты интересы разных правительств мира. И гигантские объемы «слива» тогда тоже находят объяснение — «грязного белья» должно быть как можно больше. Но это еще не все.

«С точки зрения технологий управления Интернет — это мощный инструмент трансграничного влияния, позволяющий связывать уровень информационного суверенитета участников Сети, в том числе национальных сегментов, — поясняет Александр Венедюхин, главный редактор журнала «Доменные имена». — Но к настоящему моменту главный «инструмент» влияния — система управления Интернетом — потерял былую эффективность». Точнее, у него появился конкурент. В конце ноября (опять в тот же период «осеннего обострения» — к чему бы это?) Петер Зунде, основатель и совладелец торрент-трекера The Pirate Bay, заявил в своем микроблоге о намерении создать альтернативный Интернет, неподконтрольный ICANN. И ведь может — подходящие технические решения уже используют BitTorent и Kad. Так что основы привычного виртуального мира могут обрушиться. Напрашивается вывод:

TOBY MELVILLE/REUTERS

ДЛЯ ЖУРНАЛИСТОВ АССАНЖ — НЕИССЯКАЕМЫЙ ИСТОЧНИК ИСТОРИЙ, МИФОВ И ЛЕГЕНД

нужно решительно положить конец этим происками. Например, решением какого-нибудь «интернет-совбеза» ООН.

И управа на пиратов найдется. «Это превентивное внедрение криптографических механизмов, которые позволят построить над любой новой распределенной системой устройств строгую иерархию управления», — рассказывает Александр Венедюхин. В ночь с 15 на 16 июля нынешнего года корневую зону DNS подписали настоящим криптографическим ключом и опубликовали открытые ключи для проверки подлинности электронных подписей по протоколу DNSSEC. Держатель ключей — все та же компания VeriSign.

Получается, что США выгодны два варианта развития событий: либо сохранение status quo нынешнего управления Интернетом, либо модернизация системы DNS в сторону более гибкой децентрализованной системы, но под присмотром своих криптотехнологий для «опознавания» пользователей. Дополнительной остроты этой схватке, безусловно, добавляет то, что оба варианта открывают огромные коммерческие перспективы, в первую очередь для США, поскольку предполагают изменения ПО и на компьютерах пользователей. Но пользователей нужно «обработать» быстро, пока это не сделали «альтернативные» образования под эгидой пиратов.

Скажем, система Master Card, или PayPal, или какая другая, столь же глубоко внедрившаяся в экономики разных стран мира, в целях повышенной безопасности клиентов — исключительно! — откажется работать с теми, кто не обменял старые карты на новые — улучшенные в соответствии с новыми стандартами. Но обе системы точно начнут действовать активнее, если помимо соображений коммерческой выгоды получат указание от «интернет-совбеза» ООН. Кстати, следующий объект «разоблачений», которые готовит Ассанж, — банки. Что логично: нужно тряхнуть финансовое лобби, чтобы оно возмущенно потребовало от правительств защиты, а заодно дало денег на модернизацию инфраструктуры до безопасного уровня.

Интернет вокруг нас необратимо меняется. И проект WikiLeaks — это асимметричная провокация в пользу «политического» управления Интернетом с доминированием технологий безопасности, контролируемых США. «Главный механизм этого проекта находится не в правовом или силовом поле, а в поле информационного воздействия, — уверен Максим Тимонов. — Грубо говоря, выиграет тот, у кого больше информационных ресурсов и возможностей для переключения внимания публики с реальной проблемы на яркую обложку».

Так кто там, говорите, спустился с неба? Джулиан Ассанж? Кто вспомнит имя одной из легиона пешек в большой интернет-игре через пару лет? Наверняка будут и новые — не только провокаторы и страшилы, но и более приятные персонажи, ведь к новому мировому интернет-порядку нужно приучать не только кнутом, но и пряником. ■

Подарок себе любимому

В этом году Никита Михалков решил сделать подарок самому себе. Ну надоело ему одаривать других, тем более что его щедрость мало кто ценит. Вот, скажем, за «Предстояние» неблагодарный зритель так и не проголосовал. Так что пришлось Михалкову голосовать за себя самого — рублем. Отныне производители и импортеры любых носителей информации будут отчислять ведомству, учрежденному тщанием Никиты Сергеевича, один процент доходов. В блогах интересуются: когда Союз писателей в свою очередь потребует авторский процент с чистой бумаги включая туалетную?