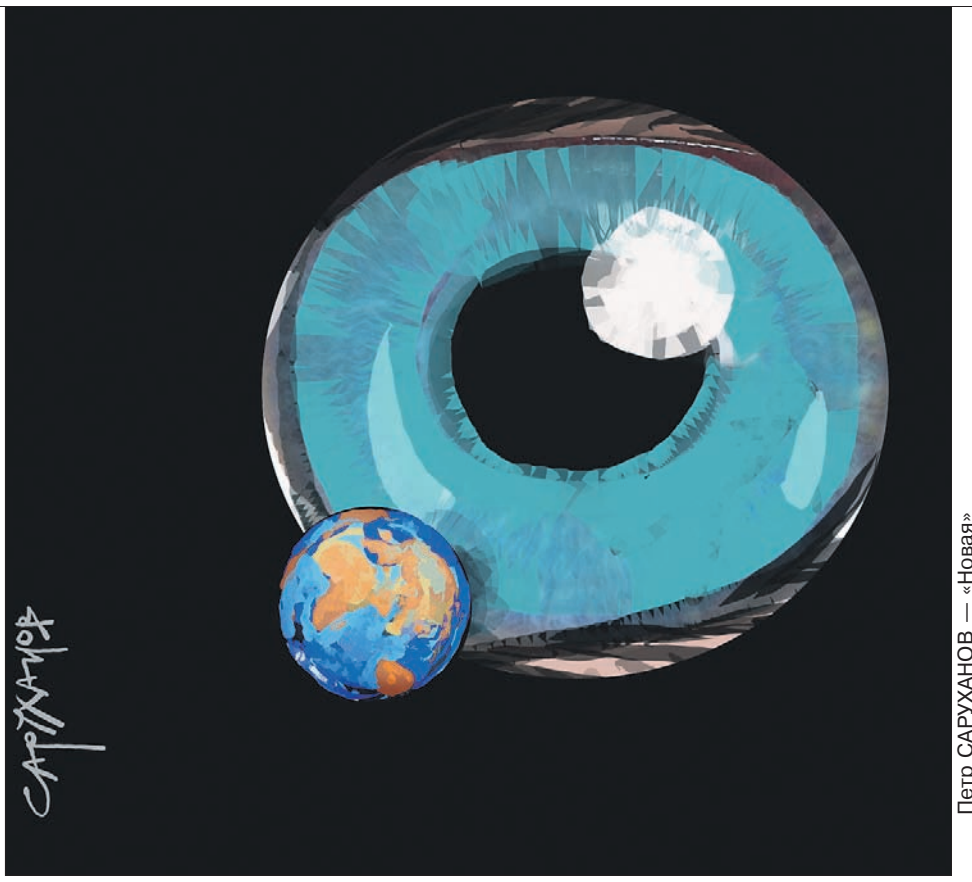
Сергей ГОЛУБИЦКИЙ
для «Новой»



Петр САРУХАНОВ — «Новая»

Как медиа сделали сенсацию из отраслевого слива от DigitalRevolution

Хакеры без головы

Помню, в моем советском детстве активно глушили радио «Свобода», «Голос Америки» и даже «Радио Тирана», а вот Би-би-си не глушили. Эфир был чистым-чистым, даже когда джингл с народным хором предупреждал об очередной порции ядовитых хохм Севы Новгородцева. Уж не знаю, какие такие особые договоренности существовали между Великобританией и СССР, но *неглушение* Би-би-си находилось в согласии с популярным у обывателя мифом: все *вражеские голоса клевещут*, и только британская радиостанция информацию подает взвешенно и беспристрастно.

В наше время Би-би-си строит работу на приоритетах, единственно, похоже, обеспечивающих выживание СМИ в эпоху Post Truth: потребителя информации следует ошарашивать так сильно, чтобы у него отпадало всякое желание что-то анализировать.

Портал bbc.com, в истории под ироничным названием «Россия пытается взломать анонимный браузер Tor», поведал миру о том, как хакеры взломали сервер российской АйТи-компании «Сайтэк» — предположительно, подрядчика российских военных и разведывательных ведомств. Британских коллег поддержали журналисты Forbes, которые перенесли акценты в сюжете на самого Воланда: «Взломано секретное разведывательное ведомство России — крупнейшая утечка информации в истории». Куда делся «подрядчик ФСБ»? А бог его знает, куда. Предполагается, видимо, что англоговорящий обыватель либо не понимает разницы между подрядчиками и заказчиками, либо ему без разницы.

Британский заголовок про взлом анонимного Tor меня заинтриговал, поскольку давно изучаю эту тему и даже делился с читателями «Новой» своими наблюдениями («Мухоловка Даркнета»). Посему решил проверить сенсацию, благо хвастливые хакеры обставили свои «подвиги» комфортно для анализа: передали материалы «старшим товарищам» — группе DigitalRevolution, а те, облагородив подгон этикеткой «борьбы с кремлевским беспределом», выложили у себя в твиттере линки на «компромат».

Более провального слива затрудняюсь даже припомнить. Назвать «компроматом» огромный ворох маркетинговых наработок, платежных ведомостей и корпоративной почты, не защищенной никакими грифами секретности, можно только с одной целью — одурачить тех, кто априори готов потреблять пропагандистское сусло без разбора.

Чем оправдывает Forbes контаминацию «подрядчика ФСБ» с самим ФСБ? Видимо, таким аргументом: «Проекты «Сайтэк» заказывало воинское подразделение 71330, входящее в состав 16-го Управления ФСБ, которое занимается радиотехнической разведкой, — то же подразделение обвинялось во внедрении шпионских программ в почтовые программы офицеров украинской разведки в 2015 году». Несостоятельность подобной логики, на мой взгляд, выдает содержание самого «компромата». Содержание это, кстати, еще и объясняет, как хакерам в принципе удалось увести этот ворох макулатуры: украли, потому что никто не озаботился полноценной защитой. По понятной причине — там нечего было защищать.

Милые презентации в PowerPoint, обширные подводки к темам явно википедийного происхождения, анонсы намерений и постановка задач — «компромат» не выдает ничего, кроме рутинной работы рядовой российской АйТи-компании. Специализация «Сайтэк» — программная автоматизация алгоритмов изыскания, обработки и анализа информации, находящейся в открытом доступе (в первую очередь — в социальных сетях). На незаконное проникновение в приватные данные (частную почтовую переписку, сообщения в мессенджерах) в «компромате», украденном группой 0v1ru$, нет и намека. Заказчиков, заинтересованных в выполнении подобных действий, тоже нет. Криминал в избытке присутствует лишь в действиях самих «разоблачителей».

Конек «Сайтэк» — структурирование и анализ данных из социальных сетей, которые, с одной стороны, доступны для ознакомления любому желающему, а с другой — лишены интерфейсов глобального поиска. Создание подобного интерфейса позволило бы трансформировать big data в аналитический инструмент безграничных возможностей. Увлекательность и масштаб такого вызова понятен любому специалисту в области информатики, и уж тем более — госструктурам, которым сам бог велел заключить соглашение с АйТи-компанией, обещающей разработать практические решения.

Судя по всему, «Сайтэк» обещала. И получила заказы. Мы не знаем, удалось ли компании создать аппаратно-программный комплекс для семантического анализа дискретной информации, извлекаемой из социальных сетей. Если удалось, то «Сайтэк» заслуживает Нобелевской премии. Потому что одно дело — извлечь ценные данные из дискретных, однако же публичных источников, и совсем другое — выкрасть, подслушать и взломать.

Тем более что у нас уже есть мировой чемпион криминальных рекордов — электронно-разведывательный комплекс «Эшелон» Агентства национальной безопасности США, который, задействуя сотни спутников-шпионов, наземных станций слежения и подслушивания, перлюстрирует на уровне исходных протоколов и кода всю электронную почту, мобильную связь, факсы и телексы, вылавливает ключевые слова, сопоставляет голоса, координирует перемещения в пространстве тысяч и тысяч интересных для государства персон с их индивидуальными профилями, в которых географическое позиционирование дополняется данными о частной жизни, профессиональной и финансовой активности. Вот уж где размах, так размах. Вот где у нас Левиафан, достойный самого пристального изучения со стороны мировой общественности.

> «Мы имеем дело не с огневым рубежом идеологического противостояния России и Запада, а с местью местечковых конкурентов из отечественного АйТи-бизнеса»

Впервые беспрецедентный криминал на государственном уровне («Эшелон» курируют т.н. «Пять глаз», консорциум разведведомств США, Великобритании, Австралии, Канады и Новой Зеландии) попытался расследовать еще в 2000 году Европейский парламент, но потерпел сокрушительную неудачу. О способах отваживания можно лишь догадываться, если даже после разоблачений Сноудена, представившего в 2015 году документальные доказательства работы «Эшелона», мировая общественность предпочитает делать вид, что ничего не знает о присутствии в нашей жизни государственных систем слежения, которые ежедневно на протяжении 40 лет попирают все мыслимые права и свободы личности.

Оно понятно: комфортнее и безопаснее бороться с «кремлевским беспределом», высмеивая попытки российских АйТи-компаний найти уязвимые места в браузере Tor. Так и подмывает рекомендовать «Сайтэк» не тратить времени на координацию данных из выходных узлов луковой маршрутизации с данными интернет-провайдеров в надежде случайно соединить IP-адрес пользователя с заказом на каком-нибудь подпольном развале наркотиков в Даркнете. Гораздо продуктивнее было бы пробить через «нашего Трампа» стажировку в любом из американских государственных ведомств, курирующих и финансирующих Tor Project. Бэкдорами они, конечно, не поделятся, но много неожиданного о подлинном устройстве «анонимного» браузера рассказать смогли бы.

Есть, однако, в «компромате», украденном 0v1ru$, нюанс, который теоретически мог бы расширить обвинительную базу хакеров-кремлеборцев, Би-би-си и Forbes. В частности, многие суждения, подаваемые подрядчиком под соусом перспективных ноу-хау, гуглятся за 10 секунд. Скажем, сентенции об алгоритмах информационного анализа социальных сетей или возможных способах распутывания луковой маршрутизации Tor — это трюизмы, явно не тянущие на гриф «конфиденциально». А раз так, то можно предположить, что смысловая подоплека договоров «Сайтэк» — отнюдь не в желании государственных структур самообразоваться по части устройства Facebook и Tor, а в откатах.

Гипотезу эту, однако, развенчали сами же хакеры, опрометчиво дополнившие «компромат» платежными ведомостями. Документы эти выдают столь скромные финансовые потоки (типичные для российской АйТи-индустрии и недостойные внимания уважающего себя мздоимца, сидящего на госсинекуре), что впору начинать волноваться о своевременной оплате аренды офиса и раздаче зарплаты сотрудникам. Какие уж тут откаты.

Мы уже говорили, что хакерский взлом стал возможен, скорее всего, потому, что компания вообще не озаботилась защитой серверов, на которых хранился «компромат». И такую беспечность несложно понять: большую часть украденных материалов можно смело выкладывать в открытом доступе на собственном портале в качестве рекламы проводимых НИОКР.

Все эти детали и обстоятельства, помноженные на лингвистический анализ риторики группы DigitalRevolution, позволяют предположить, что мы имеем дело не с огневым рубежом идеологического противостояния России и Запада, а с местью местечковых конкурентов из отечественного АйТи-бизнеса.

Дабы не заканчивать на неприятной ноте, предлагаю внести конструктивный элемент непосредственно в тему исследований «Сайтэк» — технику сбора и анализа информации из дискретных неструктурированных открытых источников. Меня удивила прямо-таки магическая вера в панацею аппаратно-программных решений поставленных проблем. Вот, мол, автоматизируем сбор данных и получим чудо-результаты. Мой скромный опыт подсказывает, что успех анализа информации обеспечивается не столько софтом и железом, сколько умением операторов (то есть живых людей!) делать умозаключения на «последней миле».

Лучшее доказательство моих слов — работа горячо нелюбимого в России Billingcat, который безо всяких «Натисков», «Орионов» и «Наутилусов» создает из открытых дискретных данных пошаговые и поминутные реконструкции событий частной жизни. Работая лишь руками и головой.