УДК 327; 351.72

СОТРУДНИЧЕСТВО МЕЖДУ КРЕМНИЕВОЙ ДОЛИНОЙ И ВАШИНГТОНОМ: ЧТО ПРЕПЯТСТВУЕТ ЕГО РАЗВИТИЮ

© 2015 г. **Е.А. Роговский***

Статья поступила 22.06.2015 г.

Статья посвящена экономическим и политическим проблемам взаимоотношений администрации США и расположенного в районе Сан-Франциско высокотехнологичного бизнеса (так называемая Кремниевая долина). Рассматриваются причины незаинтересованности этого бизнеса в сотрудничестве с Пентагоном. Особое внимание уделяется проблеме информационной уязвимости государственных структур и стратегии сдерживания кибератак.

Ключевые слова: *высокотехнологичный бизнес; проблемы с инновациями Пентагона; информационная уязвимость государственных структур; стратегия сдерживания кибератак.*

Администрации США и расположенные в районе Сан-Франциско высокотехнологичные компании Кремниевой долины всегда поддерживали друг друга. Но в последнее время в американской прессе появилось немало материалов, освещающих возникшие в их отношениях проблемы.

Вопрос о разногласиях между Вашингтоном и Кремниевой долиной становится всё более актуальным в контексте надвигающихся президентских выборов в 2016 г. Несмотря на остающиеся позитивными взаимоотношения Кремниевой долины и администрации Обамы, за последний год они стали заметно прохладнее. Ухудшение отношений федерального правительства с местными высокотехнологическими компаниями в апреле 2015 г. признал Министр внутренней безопасности США Дж. Джонсон [5].

Американское государство и развитие Кремниевой долины

Между Кремниевой долиной, иногда называемой «островом предпринимательского капитализма и настоящей свободы», и Вашингтоном, олицетворяющим государственную бюрократию США, в настоящее время разворачиваются настоящие драмы.

* **РОГОВСКИЙ Евгений Александрович – кандидат экономических наук, руководитель Центра военно-промышленной политики Института США и Канады РАН (ИСКРАН).** Российская Федерация, 121069, Москва, Хлебный пер., 2/3 (Rogowsky@mail.ru).

Необходимо признать, что инновационный бизнес Кремниевой долины в ключевые моменты своего развития всегда пользовался поддержкой Белого дома, который стремился облегчить вывод на рынок новых коммуникационных услуг, т.е. снизить порог вхождения в бизнес для новых фирм – стартапов (*Start-ups*).

Такая политика американского государства лежала в основе информационно-технологической революции в США. Вспомним в этом контексте получивший в своё время широкую известность так называемый «налог Гора», который (помимо прочего) обеспечил переизбрание демократического президента У. Клинтона в 1996 году.

«Налогом Гора» либерально-рыночные противники тогдашнего вице-президента США назвали 254-й раздел (*Section 254*) закона «О телекоммуникациях» 1996 г. (*Telecommunications Act of 1996 – P.L. 104–104*). Этот раздел создавал систему перекрёстного субсидирования, подобную существовавшей внутри корпорации АТТ (*AT&T).* Однако если в АТТ это было внутренним делом корпорации, то в рамках закона «О телекоммуникациях» 1996 г. такую систему можно было трактовать как незаконное налогообложение межрегиональных телекоммуникационных услуг. В самом деле закон 1996 г. ввёл специальный налог (названный в законе «вкладом») на провайдеров этих услуг, целью которого являлось финансирование широкого распространения телекоммуникационных услуг.

При этом величина этого специфического налога-«вклада» определялась Федеральной комиссией по связи (ФКС) в обход Конгресса США (!), что является прямым нарушением американской Конституции. Налог на доходы компаний Кремниевой долины был повышен всего на 1% – с 35 до 36%, но это позволило правительству дополнительно изъять у местных высокотехнологичных компаний миллиарды долларов (более 400 млн. долл. у одной только «Интел» (*Intel*) и профинансировать программы, стимулирующие распространение телекоммуникаций в Соединённых Штатах. В частности, речь шла о четырёх секторах сети: 1) обеспеченных пользователях телекоммуникационных услуг высокой стоимости, 2) пользователях телекоммуникационных услуг с низкими доходами, 3) школах и библиотеках, 4) телекоммуникациях, связанных с развитием сельского здравоохранения. Таким образом был сформирован дополнительный («стимулирующий») спрос на телекоммуникационные услуги, обеспечивший так называемый синергетический эффект от резкого увеличения количества пользователей сетью.

Понятно, что множество компаний Кремниевой долины к «налогу Гора» отнеслись позитивно, хотя некоторые из них требовали возвращения изъятых у них денег. В дальнейшем, по мере распространения в США информационно-коммуникационных технологий (ИКТ), возникли многочисленные подозрения в отношении того, что такая система перекрёстного субсидирования ИКТ-услуг страдает от нецелевого использования средств и поражена коррупцией.

Ещё один пример касается стимулирования развития Интернета. В 2012 г. Белый дом помог Кремниевой долине одержать победу над антипиратским законопроектом (*Stop Online Piracy Act – SOPA*), лоббировавшимся киноиндустрией. Главы таких компаний, как «Гугл», «Яху», «Википедиа» и «Мозилла»

(*Google, Yahoo, Wikipedia* и *Mozilla*) встретились с чиновниками Белого дома и убедили их в том, что этот законопроект предполагает закрытие ряда вебсайтов и может привести к цензуре интернет-трафика. Их позицию поддержали миллионы пользователей сети, которые направили законодателям соответствующие голосовые сообщения и е-мейлы (в том числе молодые люди, составляющие критически важную часть избирателей Демократической партии). В конечном счёте в начале 2012 г. Белый дом, который ранее в целом «голливудскую реформу» (законопроект о копирайте) поддерживал, изменил точку зрения и в отношении к этому законопроекту встал на позицию Кремниевой долины.

Комментируя это решение, Дж. Экил (*Josh Ackil*), соучредитель фирмы «Фрэнклин скваэр групп» (*Franklin Square Group*), лоббирующей развитие и распространение высоких технологий и представляющей интересы «Эппл», «Гоупро», «Юбер» и «Сиско» (*Apple, GoPro, Uber* и *Cisco*), с удовлетворением констатировал, что «администрация продемонстрировала понимание важности вопросов технологии и инноваций для роста экономики в целом» [19].

В этом контексте можно также вспомнить, что президент Б. Обама поддержал иммиграционную реформу, лоббируемую такими высокотехнологическими фирмами, как «Фейсбук», «Майкрософт» и «Яху» (*Facebook, Microsoft, Yahoo*) и порицаемую профсоюзами. Он также проталкивал реформу патентов, за которую ратовали «Эппл» и «Гугл».

Ещё один свежий пример. Совсем недавно и Кремниевая долина, и Вашингтон придерживались «мантры» «Интернет регулировать не надо!» Но времена изменились – инновационному интернет-бизнесу понадобился действительно свободный (недискриминационный) доступ к широкополосным коммуникациям. В этой связи федеральное правительство США решило ввести так называемые правила «нейтральности сети» (*Network Neutrality*), которые осенью 2014 г., после завершения дорогостоящей и длительной лоббистской войны, предложил председатель ФКС Т. Уиллер (*Tom Wheeler*).

Ранее эти правила обсуждались на встречах, в которых помимо правительства участвовали три стороны: адвокаты, защищающие интересы общественности; руководители интернет-компаний (многие из которых были малыми стартапами); представители традиционных кабельных и телекомовских фирм. После этих встреч экономические советники Белого дома помогли подготовить видеообращение президента в поддержку «самой строгой версии правил». Обама заявил, что хочет видеть в телекоммуникационной политике такие существенные изменения, которые сделают услуги провайдеров широкополосного Интернета подобными такому благу, как привычная телефонная связь. Эту позицию президента можно считать очевидной победой передового интернет-бизнеса Кремниевой долины, одержанной над старыми технологиями связи.

Правила «нейтральности сети» регулируют использование широкополосных каналов для организации интернет-трафика [9]. Однако они подрывают конкурентную среду на рынке подобных услуг, поскольку запрещают провайдерам широкополосных услуг какую бы то ни было дискриминацию интернет-трафика (в частности, взимание платы за ускоренное приоритетное обслуживание привилегированных партнёров).

Это – запрет хорошего (успешного) бизнеса ради достижения целей федерального правительства, а именно, всемерного расширения открытости рынка услуг широкополосных интернет-коммуникаций, а также ускорения его глобального распространения. Интересно, что и сегодня, как это в своё время было с «налогом Гора», множество интернет-компаний Кремниевой долины эти правила искренне поддерживают.

Политика в отношениях Кремниевой долины с Вашингтоном

Ещё в самом начале XXI века в материалах Института САТО появился текст некоего Т. Роджерса (*T.J. Rodgers*), освещающий причины, вследствие которых Кремниевая долина не должна стремиться к нормализации отношений с федеральной властью Соединённых Штатов [17]. Первой из упомянутых причин, был назван «коллективизм» – самый страшный враг истинного капитализма. Некоторые американские экономисты, а также СМИ называли такой капитализм «дружеским капитализмом» (*Crony Capitalism*). По мнению Т. Роджерса, «дружеский капитализм» представляет собой некую мутацию, препятствующую реализации права американцев на свободное предпринимательство. Фактически Т. Роджерс, придерживаясь откровенно либеральной точки зрения, полностью отверг право государства на проведение промышленной политики, исходя из посылки, что в ***современной динамичной мировой экономике административно-силовые структуры не могут принимать решения настолько эффективно, насколько это могут делать структуры свободного рынка.***

В связи с введением правил «сетевой нейтральности» некоторые американские наблюдатели подняли шум об очередном проникновении «коллективизма» в Кремниевую долину, утверждая, что для бизнеса тем лучше, чем меньше в него вмешательство в интересах государства, но политикам, борющимся за поддержку избирателей, без коллективизма нельзя.

Высокотехнологические фирмы сыграли ключевую роль в быстром развитии политической судьбы Б. Обамы. По сведениям внепартийного исследовательского Центра ответственной политики (*Center for Responsive Politics*), компьютерные и интернет-компании внесли в его предвыборную кампанию (2012 г.) около 7,8 млн долл., что более чем вдвое превышает средства, собранные в этой отрасли республиканским кандидатом М. Ромни.

Корпорации Кремниевой долины хорошо понимают необходимость политического лоббирования. «Мы не хотим просто так дарить деньги политикам, не выросшим в технологической отрасли и не понимающим, насколько это важно, насколько это хрупко, насколько это сложно», – считает Р. Хастингс (*Reed Hastings*), президент «ТекНет» (*TechNet)*, ассоциации, лоббирующей высокотехнологический бизнес.

Тесные связи Б. Обамы с Кремниевой долиной раздражают некоторых консервативно настроенных бизнесменов, которые говорят, что высокотехнологические компании выросли слишком сильно и стали неконтролируемыми. С другой стороны, в отношениях с Вашингтоном появились нотки политиче-

ских разногласий – после разоблачений Э. Сноудена корпорации Кремниевой долины начали протестовать против деятельности АНБ. М. Лофгрен *(Mike Lofgren)*, бывший член Республиканской партии, 28 лет проработавший в бюджетных комиссиях Палаты представителей и Сената США, в своей получившей широкую известность книге «Игра окончена: как республиканцы сошли с ума, демократы стали бесполезными, а средний класс был обманут»[13] отмечает: «Агентство национальной безопасности и ЦРУ не могли бы заниматься тем, чем они занимаются, без Кремниевой долины. Де-факто она стала частью деятельности АНБ». Обнародование примеров подобного тесного сотрудничества, раскрывающих, как правительство использует их разработки, вызвало резкое раздражение у руководства некоторых компаний долины, они даже иногда пытаются скрывать эти факты.

Высокотехнологичное бизнес-сообщество Кремниевой долины было, например, потрясено тем, что президент США поддержал военные действия в Сирии. В частном порядке руководители американских интернет-компаний признаются, что они «просто стонут от раздражения», когда обнаруживается, что АНБ использует их технологические разработки для слежки за американскими гражданами. Кроме того, большое раздражение поддерживающих Демократическую партию компаний-доноров вызвал явно непрофессиональный запуск (в рамках правительственного проекта) веб-сайта медицинского страхования «*HealthCare.gov*».

Можно предположить, что Р. Хастингс также имел в виду то, что Вашингтону следовало бы обновить своё представление о реальных нуждах бизнеса Кремниевой долины. В этом контексте уместно подчеркнуть: в 2009 г. кризис резко сократил венчурные инвестиции в эти компании, в частности:

в биотехнологии – на 24 %,
в электронику – на 37%,
в информационные технологии – на 42%,
в том числе софт – на 32%,
производство полупроводников – на 49%,
телекоммуникации – на 62%.

После кризиса 2008–2009 гг. многие высокотехнологичные компании стали буквально демонстрировать своё пренебрежение к реальным социальным проблемам, присущим современным США. Большинство венчурных капиталистов, сверхбогатых инвесторов-«ангелов» и руководителей стартапов сфокусировались на разработке и продажах зачастую бессмысленных приложений для мобильных социальных сетей, на расширении сферы «привилегированного комфорта для богатых».

Вашингтону пора бы заметить, что современная Кремниевая долина уже не является крупным поставщиком правительства и в основном продаёт свою продукцию не военным, а частным лицам и компаниям. Более того, местные высокотехнологические компании уже успели «привыкнуть» к специфическому информационно-технологическому рынку, где потребитель не является строптивым заказчиком, а, наоборот, под воздействием агрессивной рекламы, раскупает качественно новую продукцию «как горячие пирожки». Таким компаниям «не удобны» чрезмерно жёсткие регламенты федеральной кон-

трактной системы, они просто не желают связываться с государственными заказами [12].

Молодому высокотехнологичному бизнесу Кремниевой долины стало неприлично иметь федеральное правительство в качестве заказчика и сталкиваться с «удушающей бюрократией» и чрезмерной требовательностью и волокитой. Р. Хэнкок (*Russell Hancock*), президент бесприбыльной независимой организации «Группа экономического развития венчурных предприятий Кремниевой долины» уверен, что для работы в рамках «разочаровывающе архаичного» пентагоновского закупочного процесса «у менеджмента высокотехнологичных стартапов просто не хватает терпения».

Для того, чтобы составить себе представление о глубине различий и связанной с этим напряжённостью, достаточно обратить внимание на то, как принадлежащая Э. Маску (*Elon Musk*) частная космическая компания «СпейсЭкс» (*SpaceX*) конфликтует с Пентагоном в отношении контрактов на доставку на орбиту военных спутников. Миллиардер Э. Маск, соучредитель таких корпораций как «Тесла», «ПейПэл» (*Tesla, PayPal*), воплощающий скорость и целеустремлённость Кремниевой долины, ведёт судебное преследование ВВС США, утверждая, что «СпейсЭкс» должно быть разрешено конкурировать за такие контракты. При этом он продолжает неустанно критиковать «болезненно медленный процесс сертификации» ракет своей компании.

Располагая собственными исследованиями и разработками, военные привыкли вести за собой многие американские технические инновации – от разработки Интернета до глобальной системы позиционирования. Однако сейчас ситуация кардинально изменилась: многие из достижений рождаются в частных коммерческих компаниях в ходе работ, к организации и финансированию которых американское правительство не имело и не имеет никакого отношения. Как отмечает бывший заместитель министра обороны У. Линн (*W.P. Linn III)*, за последние десятилетия именно частный сектор «смог предоставить американским военным самые передовые технологии, создавшие для них явное преимущество». Более того, с нашей точки зрения после кризиса 2008–2009 гг. ситуация на рынке государственных заказов обострилась: теперь зачастую ведущим частным высокотехнологичным инновационным компаниям деньги правительства даже не нужны!

Им не нужны ***подотчётные бюджетные деньги, которыми нельзя многократно рисковать, а также федеральные контракты с жёстко заданными функциональными параметрами конечных изделий. Инновационные компании Кремниевой долины зачастую просто не хотят иметь с правительством ничего общего.***

Проблемы военного руководства

У Минобороны возникли серьёзные проблемы с разработкой новых оружейных систем и технологий. И главная состоит в том, что в этой области оно «движется слишком медленно».

По мнению упомянутого У. Линна, «время, которого требуют процедуры заказа, создания и внедрения ИКТ, должно соответствовать реальному циклу

обновления таких технологий, т.е. от 12 до 36 месяцев, а не 7–8 лет, что типично для сформировавшихся в настоящее время бюрократических процедур оформления и реализации государственных заказов и контрактов на вооружения и военную технику» [14]. В начале XXI века для внедрения той или иной инновационной компьютерной системы, с учётом времени, необходимого для принятия решения о финансировании её создания, требуется в среднем 81 месяц. Это более чем в 3 раза превышает сроки создания популярного «Айфон» (*iPhone)*. С учётом стремительных темпов развития компьютеров и иной ИКТ-продукции к моменту, когда технологии внедряются в МО, они оказываются уже сильно устаревшими по отношению к тем гражданским моделям, которые могут быть доступны потенциальному противнику. Особенно острые проблемы возникают в отношении разработок по кибербезопасности – в этой сфере отставание от потенциального противника особенно опасно.

Важно также подчеркнуть, что закупочные конкурсы Федеральной контрактной системы, как правило, требуют соблюдения принципа минимальной цены при заданных целевых параметрах конечного изделия (разработки). Однако в этих целевых параметрах зачастую в должной мере не учитывают актуальных требований информационной безопасности, которые заранее, на этапе оформления контрактных спецификаций, ещё не известны.

Проблемам работы Министерства обороны с ИКТ-бизнесом был посвящён подготовленный в марте 2012 г. доклад комитета по вооружённым силам Палаты представителей Конгресса Соединённых Штатов «Вызовы ведению бизнеса с Министерством обороны США» [2].

Для ускорения внедрения инноваций и максимального использования имеющегося ИКТ-потенциала МО США рекомендовано выработать новый подход к сфере исследований и разработок, провести значительные изменения в системе государственных военных закупок. В частности, необходимо в максимально возможной степени отказаться от «специальных заказов» на новые ИКТ и использовать уже существующие готовые *(of-the shelf*) разработки; тщательно согласовывать и взаимоувязывать (интегрировать) различные информационные системы; избегать одномоментного введения в эксплуатацию каких-либо сверхсложных информационных систем (их «мгновенного внедрения») и поэтапно внедрять различные модульные элементы, поддерживая, таким образом, военную информационную инфраструктуру в состоянии перманентной модернизации и обновления.

Однако этого оказалось явно недостаточно. В ноябре 2014 г. в «Вашингтон пост» появился материал Д. Стейнбока (*Dan Steinbock)* под названием «Проблемы американских военных инноваций» [20]. В нём констатируется, что американские оборонные инновации, несмотря на их всемирное превосходство, в настоящее время подвержены «структурной эрозии». Д. Стейнбок утверждает, что «дни массивного военно-технического лидерства США и существенного вклада военных инноваций в американскую экономику и её глобальную конкурентоспособность прошли», и призывает федеральные власти проводить в этой сфере целенаправленную государственную политику. Такая промышленная политика должна стимулировать инновации, связанные с оборонкой. Если же американские инновации будут продолжать развиваться исключительно

под действием «рыночных сил частного сектора», то сокращение военной поддержки технического развития обязательно приведёт к потерям в конкурентоспособности американской экономики и эрозии военного превосходства США.

По нашему мнению, именно на основе этого доклада была сформирована принципиально новая позиция Минобороны, с которой впервые за последние 20 лет его глава Э. Картер (*Ashton Carter*) в апреле 2015 г. отправился в Кремниевую долину [6], чтобы предложить бизнесу государственную помощь. Он выступил с речью в Стэнфордском университете, а также встретился с венчурными капиталистами и руководителями высокотехнологичных компаний. Картер объявил о «новом партнёрстве» своего ведомства с компаниями Кремниевой долины и о том, что Министерству обороны очень нужна помощь таких «профессиональных инноваторов», каких можно найти в ведущих корпорациях вроде «Эппл», «Фейсбук», «Гугл» (*Apple, Facebook, Google*) и других, не только для защиты от киберугроз, но также для ускорения темпов изобретения, развития и внедрения новых видов кибероружия.

Проблемы федерального правительства

Однако, выступая в Кремниевой долине министр обороны не затронул ключевого вопроса, определяющего, как нам представляется, отношение частных инновационных компаний к Вашингтону. Это вопрос об уровне информационной безопасности (а правильнее – небезопасности!) структур федеральной власти США.

Современный бизнес Кремниевой долины свои секреты ценит выше государственных тайн и очень ревниво относится к вопросам защиты коммерческой тайны, интеллектуальной собственности, а также данных о сотрудниках. Бизнес-сообществу хорошо известно, что, во-первых, в структурах федерального правительства слишком много инсайдеров (*см. ниже*), и во-вторых, что эти структуры слишком уязвимы для хакеров. Как нам представляется, именно это обстоятельство имел в виду президент ассоциации «ТекНет» Р. Хастингс, сетуя на то, что «Вашингтон просто не понимает, насколько это важно, насколько это хрупко, насколько это сложно» [17].

В самом деле, действующими правилами федеральной контрактной системы всем сотрудникам, участвующим в работах по военному контракту, предписывается оформление индивидуальных допусков к секретным работам (*Security Clearance*). В США оформлением таких допусков на уровне федерального правительства занимается Управление кадровой службы (*Office of Personnel Management*) – УКС.

Как оказалось, именно эта организация весьма уязвима для зарубежных хакеров (см. ниже). Но УКС не является исключением. Количество кибератак на федеральные структуры только нарастает [3]. Недавно о крупной краже персональных данных на американских налогоплательщиков сообщило Министерство финансов США [4].

Особая проблема – инсайдеры. Она обострилась на фоне «вращения кадровых дверей», отражающего тесные связи Кремниевой долины и Белого дома [19]. Вот несколько примеров. Бывший пресс-секретарь Джей Карни (*Jay Car-*

ney) стал старшим вице-президентом компании «Амазон». Руководитель избирательной кампании Б. Обамы и его бывший старший советник Дэвид Плуфф (*David Plouffe)* стал старшим вице-президентом компании «Юбер». Бывший заместитель помощника президента Обамы по науке и технологической политике Эндрю МакЛафлин (*Andrew McLaughlin*) стал вице-президентом компании «Гугл» (потом перешёл на другую работу). Бывшая заместительница МакЛафлина Николь Уонг (*Nicole Wong*) перешла на работу в «Гугл» и «Твиттер». Бывший торговый представитель США Деметриос Дж. Марантис (*Demetrios J. Marantis*) возглавил отдел международных связей в компании «Скваэр». И наоборот. Меган Смит (*Megan Smith*), одна из вице-президентов «Гугл», стала помощником президента Обамы по науке и технологической политике, сменив на этой должности Тодда Парка (*Todd Park*), который стал технологическим представителем (советником) администрации Обамы в Кремниевой долине [10].

Выступая в апреле 2015 г. на конференции в Сан-Франциско, министр внутренней безопасности Дж. Джонсон (*Jeh Johnson*) пригласил «талантливых сотрудников» долины «провести пару лет в Вашингтоне, работая на правительство» [5].

Известный специалист в области оценки роли государства в экономике США Дж. Айсенах (*Jeffrey Eisenach*) в этой связи подчёркивает: «Конечно, президент Б. Обама тесно связан с Кремниевой долиной, так же, как Дж. Буш-мл. был тесно связан с нефтяной и обрабатывающей промышленностью» [19].

Первоапрельский сувенир Б. Обамы

Итак, федеральное правительство не может обещать венчурному бизнесу Кремниевой долины ни баснословных прибылей, ни даже сохранности их коммерческих секретов.

На что же надеется Вашингтон, предлагая бизнесу* Кремниевой *долины сотрудничество?

Как нам представляется, упор делается на силу. Например, правительство может ***создавать условия для подавления конкурентов***. В этих целях, в частности, может использоваться Указ президента Обамы от 1 апреля 2015 г. (ЕО 13694) «О блокировке собственности лиц, причастных к значительной враждебной деятельности в киберпространстве» [7] (указ не требует одобрения Конгресса и уже вступил в силу).

В этом указе президент объявил, что враждебная деятельность в киберпространстве, осуществляемая из-за пределов США, представляет собой чрезвычайную угрозу национальной безопасности страны. Согласно указу, такая деятельность включает в себя взлом или нарушение работы компьютерных сетей, критической инфраструктуры, а также кражу коммерческой тайны американских компаний или личной информации американских граждан.

Вопреки действующим международным нормам, президент наделил министра финансов США правом (при согласовании с Генеральным прокурором и Госсекретарем) признавать ***виновным*** в такой деятельности любое иностранное лицо (или организацию), которые, по его мнению, прямо или косвенно к

такой деятельности ***причастны***, блокировать счета этих лиц (или организаций), а также отказывать им в доступе к находящемуся на территории США имуществу (отказывать во въезде в США). Более того, согласно этому указу, министр финансов может передать право введения такого рода экономических санкции другим федеральным ведомствам (в том числе силовым).

Фактически этот указ создаёт новую палитру нерыночных методов ведения конкурентной борьбы, с помощью которых правительство США может оказывать давление на зарубежных партнёров в интересах американских компании.

Комментируя подписание этого указа в своём письме к руководству Конгресса и Сената, президент Б. Обама признал, что этот документ должен стать своего рода предупреждением (сдерживанием) для тех, кто намерен нанести ущерб национальной безопасности или экономике США [1].

Другим «сувениром» стала новая киберстратегия Министерства обороны США [11], которая тоже была представлена общественности в апреле 2015 г. Суть этого документа – определение направлений развития американского кибероружия, укрепления кибероборонь страны, а также подхода к сдерживанию кибератак. Этот документ сфокусирован на реализации ряда задач Министерства обороны в сфере кибербезопасности. В его новой киберстратегии в качестве одной из важнейших задач обозначена защита национальных интересов США от кибератак, «имеющих серьёзные последствия», и при этом недвусмысленно обсуждаются возможные меры возмездия. (Хотя в стратегии ещё остаётся некоторая неясность в отношении того, какие случаи Соединённые Штаты будут считать достаточно критическими для немедленного применения намеченных мер возмездия).

Крупнейшая кибератака

Как бы проверяя решимость администрации Обамы применить в отношении «агрессора» военные или финансово-экономические меры возмездия, в середине июня 2015 г. в СМИ появились сообщения о том, что хакеры весь последний год имели незаконный доступ к засекреченным персональным данным 4-х млн.(!) действующих и бывших сотрудников силовых и разведывательных служб Соединённых Штатов. В частности, хакеры сумели получить доступ к анкетам и специальным формам № 86, которые американские государственные служащие заполняют при оформлении допусков к секретным работам и сведениям. В этих документах содержится чувствительная персональная информация – о болезнях, различных психологических расстройствах, наркотической и алкогольной зависимости человека. Кроме того, в анкетах имеются сведения о кредитной истории, местах прежней занятости, номере соцстрахования, а также контактная информация о ближайших друзьях и родственниках в США и за рубежом [16].

После такой гигантской кражи персональных данных стало ясно, что мер, предпринятых в сфере информационной безопасности мало, и что, добиваясь транспарентности всего остального мира, США сами остаются весьма уязвимыми для кибератак. Похищение персональных данных на миллионы феде-

ральных служащих США означает, что американское правительство десятилетиями пренебрегало безопасностью своих компьютерных систем. Об этом заявила глава УКС К. Арчулита (*Katherine Archuleta*). По её словам, ущерб от этой хакерской атаки может быть весьма масштабным (по официальным сообщениям, количество «пострадавших» может составить 22 млн. человек).

Этого кибервторжения не избежали и военные ведомства. После произошедшей летом 2015 г. масштабной кражи данных надо было как можно быстрее классифицировать нанесённый ущерб и принять решение об ответных мерах (например, о нанесении ответного кибердара).

После 30-дневного разбирательства в отношении гигантской летней кражи персональных данных из УКС, она была классифицирована как беспрецедентный по масштабу шпионаж, который, однако, не был разрушительным и не привёл к краже какой-либо интеллектуальной собственности. Было решено, что возможные негативные последствия этой кибератаки будут нивелированы с помощью существенного усложнения процедур онлайновой идентификации в органах федеральной власти Соединённых Штатов (в том числе для привилегированных пользователей).

В самом конце июля 2015 г. газета «Нью-Йорк таймс» опубликовала весьма содержательную статью своего вашингтонского корреспондента Д. Сэнджера (*David E. Sanger)*, посвящённую последствиям масштабной кражи персональных данных государственных служащих США [18]. В статье отмечается, что Соединённые Штаты видят различие между кибервторжениями, направленными на нанесение ущерба национальной безопасности (на эти вторжения должна реагировать контрразведка), и кибератаками, ориентированными на сбор данных в коммерческих целях (на которые должны реагировать правоохранительные органы). Один из руководителей американской разведки дал понять, что «размах произошедшего прецедента меняет его сущность». Такие прецеденты явно выходят за рамки и уголовных правонарушений, и даже традиционного шпионажа.

Д. Сэнджер обращает внимание на то, что США начали всерьёз обсуждать, как отомстить хакерам, атакующим Америку в киберпространстве, на государственном уровне. Так, продолжая идею упомянутого выше указа президента Обамы, адмирал М. Роджерс *(Michael S. Rogers*), совмещающий должности директора АНБ и шефа Киберкомандования, подчеркнул необходимость нанести «нападавшим» лицам или организациям, ответственным за вторжение, существенный ущерб.

При этом американцы ни с кем не хотят разговаривать «на равных». В статье говорится, что Соединённым Штатам нужно уметь останавливать и сдерживать всё то, что их враги делают в киберпространстве, а это означает потребность в широкой палитре инструментов обоснования (легендирования) ответных действий.

В статье Д. Сэнджера утверждается, что в рамках американского разведывательного сообщества обсуждаются возможные ответные «операции мщения». Одним из наиболее «инновационных» направлений назван поиск способов взлома так называемой «Великой защитной стены» (*Great Firewall*) – комплексной сети цензуры и контроля, которой Китай окружил своё информаци-

онное пространство для пресечения диссидентского движения внутри страны. Идея такой мести призвана убедить китайских лидеров в том, что если они не умерят своих атак на США, то могут лишиться одной из главных внутриполитических ценностей Китая – абсолютного контроля над политическим диалогом в стране [18].

Соответствуют ли такие инновации нравам современной Кремниевой долины? Ответ даст только время.

Выводы

1. Одной из наиболее важных причин для разногласий Т. Роджерс из Института CATO считает то, что ***понятия, которыми руководствуются вашингтонские политики, являются враждебными как для высокотехнологического капитализма, так и в целом для всего современного процесса создания реального богатства*** [17]. Свобода остаётся сутью инноваций в сердце Кремниевой долины, которая является островом капитализма в море коллективизма; это остров меритократии, где элиту составляют способные люди, независимо от их социального происхождения и финансового достатка.

2. Но этот остров окружён морем силовой борьбы, «большим правительством», «большими профсоюзами», «большими медиа» и «большими статичными корпорациями». А потому Вашингтон и Кремниевая долина неминуемо столкнутся. Нравится это последней или нет, но высокотехнологичное сообщество просто не способно осуществлять свой бизнес без многоплановых регулирующих воздействий американского правительства. Однако при этом важно учитывать, что такие регулирующие воздействия должны быть адекватными сложной и хрупкой природе Кремниевой долины.

3. Многие фирмы Кремниевой долины отказываются раскрывать государственным чиновникам персональные данные своих сотрудников (пол, раса, возраст и проч.) и вообще оформлять молодым инноваторам из перспективных стартапов индивидуальные допуски к режимным работам. Такого рода информационный барьер становится реальной преградой для развития сотрудничества Министерства обороны США с частным бизнесом Кремниевой долины.

4. Другой барьер – экономический. Современному инновационному бизнесу Кремниевой долины нужны ***другие деньги*** – не столько тщательно контролируемые бюджетные ассигнования, сколько «мягкие» средства частных инвесторов. Это не деньги вашингтонских церберов, интересы которых лежат, прежде всего, в регулировании финансовых потоков (в том числе лоббировании). Это капиталы так называемых инвесторов-«ангелов», глубоко убеждённых в перспективности конкретной идеи и заинтересованных в её реализации (т.е. не в процессе разработки, а в достижении результатов).

5. Представляется весьма вероятным, что некоторые из будущих предпринимательских инноваций «выйдут за рамки дозволенного» (с государственной точки зрения). Как оказалось, инновации в Интернете – это обоюдоострый меч, такие инновации легко могут обернуться против федеральной власти Соединённых Штатов (одним из примеров такого рода инноваций можно считать электронную криптовалюту «биткойн» – *см. ниже*).

Это касается и политических амбиций. Б. Обама может остаться в истории США как первый высокотехнологичный лидер, ставший президентом вместе с появлением смартфонов «БлэкБерри» (*BlackBerry*) и активно содействовавший ИКТ-отрасли, которая развилась в мощную политическую силу.

Ещё в конце 2013 г. газета «Уолл-стрит джорнел» опубликовала мнение авторитетного исследователя Стэнфордского университета и успешного бизнесмена-генетика Б. Шринивасана (*Balaji S. Srinivasan*), полагавшего, что Кремниевая долина претендует на то, чтобы быть лидирующим национальным центром силы, тогда как все остальные (не-технические) центры можно считать «неважными с точки зрения будущего страны». Его поддержали и другие специалисты, утверждающие, что основные ценности теперь создаются не в Нью-Йорке, не в Вашингтоне, и даже не в Лос-Анжелесе, а именно в Кремниевой долине, высокотехнологичные компании которой стали эпицентром инноваций и могут сыграть важнейшую роль в решении глобальных проблем.

6. В основе решимости администрации Обамы применить в отношении «киберагрессора» военные или финансово-экономические меры возмездия лежит созданный на базе передовых ИКТ-разработок доминирующий информационный потенциал. Такая ситуация дистабилизирует сложившиеся правовые основы международных отношений.

В дополнение – о биткойне

Одна из главных проблем современных США – их финансовая система. В Соединённых Штатах разворачивается напряжённая борьба за то, какой она может быть. Здесь противостоят два принципиально разных направления её развития – транспарентное и анонимное.

В рамках транспарентного направления речь идёт о развитии технологий сбора и обработки больших массивов данных, иначе говоря, о возможностях американского правительства контролировать финансовые операции бизнеса (в частности, уплату налогов) и в конечном счёте весь комплекс отношений между государством и людьми.

Напротив, направление, предусматривающее развитие анонимности, ориентируется на инновации, повышающие уровень конфиденциальности финансовых операций (например, прямые контакты между пользователями информационных сетей, а также анонимная криптовалюта типа «биткойн»).

Стоит подчеркнуть, что с информационно-технической точки зрения платёжно-расчётная система биткойн – это интернет-протокол, созданный на базе анонимайзеров системы «Тор» (*Tor*). В своё время эта система была разработана по заказу американского правительства и использовалась для распространения в зарубежных странах программных кодов, позволяющих обходить государственную цензуру. Сегодня такого рода программные коды стали основой создания эффективных инструментов ухода от налогов (иначе говоря, подрыва экономического благополучия государства).

Во всём, что касается биткойна и связанных с ним технологий, Кремниевая долина явно опережает федеральное правительство США. Политики в Вашингтоне к биткойну ещё не привыкли и пока не видят возможностей его ис-

пользования для роста своего благополучия – в лучшем случае они считают его не очень надёжным спекулятивным финансовым инструментом, и только. Поэтому Вашингтон старается сдержать рост и экспансию биткойна.

Напротив, среди предпринимателей Кремниевой долины биткойн уже пользуется постоянно растущей популярностью, они считают его воплощением высшей технологии, которая, безусловно, будет господствовать в будущем. Достаточно высокая популярность биткойна среди клиентов ведущих компаний «Делл», «Майкрософт», «Оверсток» (*Dell, Microsoft, Overstock*), побудила их принимать биткойны в оплату за свою продукцию. Многие фирмы Кремниевой долины, убеждённые в том, что именно сейчас формируется тенденция роста покупательной способности этой цифровой валюты, инвестировали в неё миллионы долларов.

Более того, в начале апреля 2015 г. глобальный телекоммуникационный гигант «Оранж» (*Orange*) объявил о намерении открыть в Кремниевой долине специальную компанию для работы с биткойнами.

Судя по всему, президент Б. Обама оказался перед трудным выбором. Он привык поддерживать Кремниевую долину со всеми её инновациями. Однако, по сути своей должности, он не может поддерживать формирование и развитие неконтролируемой валютной системы, подрывающей основы налоговой системы американского государства. По нашему мнению, уже ***в самой ближайшей перспективе отношения между Вашингтоном и Кремниевой долиной во многом будут зависеть от того, сможет ли правительство США контролировать оборот виртуальной валюты.***

По сообщениям прессы, корпорация ИБМ (*IBM*) намерена создать на основе технологии биткойна новую ***виртуальную валюту, контролируемую государством***. Судя по всему, именно такая валюта (заменив доллар!) сможет занять на американском денежном рынке доминирующее положение.

Список литературы

1. Barack Obama's Letter "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities" (https://www.whitehouse.gov/the-press-office/2015/04/01/letter-blocking-property-certain-persons-engaging-significant-malicious).-

2. Challenges to Doing Business with the Department of Defense (http://armedservices.house.gov/index.cfm/files/serve?File_id=f60b62cb-ce5d-44b7-a2aa-8b693487cd44).

3. Chinese hack of federal personnel files included security-clearance database (http://www.washingtonpost.com/world/national-security/chinese-hack-of-government-network-compromises-security-clearance-files/2015/06/12/9f91f146-1135-11e5-9726-49d6fa26a8c6_story.html?wpisrc=nl_headlines&wpmm=1http://www.washingtonpost.com/opinions/hitting-an-agency-where-it-hurts/2015/06/17/ffca6c6a-1512-11e5-9ddc-e3353542100c_story.html?wpisrc=nl_headlines&wpmm=1).

4. Cyber Attacks Likely to Increase
(http://www.pewinternet.org/2014/10/29/cyber-attacks-likely-to-increase/).

5. Department of Homeland Security opening Silicon Valley office
(http://www.siliconbeat.com/2015/04/22/department-of-homeland-security-opening-silicon-valley-office/).

6. Ewing Philip. Ash Carter's appeal to Silicon Valley: We're 'cool' too
(http://www.politico.com/story/2015/04/ash-carter-silicon-valley-appeal-117293.html).

7. Executive Order 13694 of April 1, 2015 Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities
(http://www.treasury.gov/resource-center/sanctions/Programs/Documents/cyber_eo.pdf).

8. Federal Eye. Officials: Chinese had access to U.S. security clearance data for one year (http://www.washingtonpost.com/blogs/federal-eye/wp/2015/06/18/officials-chinese-had-access-to-u-s-security-clearance-data-for-one-year/?wpisrc=nl_headlines&wpmm=1).

9. *Furchtgott-Roth H.* In a regulated Internet, consumers lose because businesses get ahead by pleasing politicians (http://www.marketwatch.com/story/in-net-neutrality-the-only-winner-is-washington-2015-02-27).

10. IRS Theft Affects Over 100 000 Taxpayers
(http://www.liveandinvestoverseas.com/news/irs-theft-affects-over-100000-taxpayers/).

11. DoD CYBER STRATEGY
(http://www.defense.gov/home/feature/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf)

12. Letter. Progressive Kristallnacht Coming? 24.01.2014.
(http://www.wsj.com/articles/SB10001424052702304549504579316913982034286)

13. *Lofgren Mike*. The Party Is Over: How Republicans Went Crazy, Democrats Became Useless and the Middle Class Got Shafted, 2012
(http://www.human-crisis.com/2014/04/blog-post_8898.html).

14. *Lynn William III.* Defending a new domain // Foreign Affairs, Sept./Oct. 2010.

15. *Lynn William III*. The Pentagon's Cyberstrategy, One Year Later. Defending Against the Next Cyberattack. Foreign Affairs. Sept. 2011.

16. *Manjoo Farhad.* Silicon Valley Has an Arrogance Problem (updated 3.11.2013)
(http://www.wsj.com/articles/SB10001424052702303661404579175712015473766).

17. *Rodgers T.J.* Why Silicon Valley Should Not Normalize Relations With Washington, D.C.
(http://object.cato.org/sites/cato.org/files/pubs/pdf/silvalley.pdf).

18. *Sanger David E.* U.S. Decides to Retaliate Against China's Hacking // The New York Times, 31.07.2015.

19. Why Silicon Valley is the new revolving door for Obama staffers
(http://www.washingtonpost.com/business/economy/as-obama-nears-close-of-his-tenure-commitment-to-silicon-valley-is-clear/2015/02/27/3bee8088-bc8e-11e4-bdfa-b8e8f594e6ee_story.html).

20. Why the Pentagon is wooing Silicon Valley (and the valley is playing hard to get)
(http://www.washingtonpost.com/news/checkpoint/wp/2015/04/23/why-the-pentagon-is-wooing-silicon-valley-and-the-valley-is-playing-hard-to-get/?wpisrc=nl_headlines&wpmm=1).

Silicon Valley and Washington: Cooperation and Challenges

(USA ❖ Canada, 2015, No.12, p. 53-68)
Received 22.06.2015.

ROGOVSKY Evgeny Alexandrovich, Institute of USA and Canada Studies, Russian Academy of Sciences (ISCRAN), 2/3, Khlebny per., Moscow, 121069, Russian Federation (e-mail: Rogowsky@mail.ru).

This article is devoted to economic and political problems of interrelations between U.S. federal administration and high technological business situated in San-Francisco region of Silicon Valley. The reasons why this business is not of great interest to be contracting with Pentagon are under consideration. The author put main accent to information vulnerability of government agencies and deterrence strategy of cyberintrusions. **Keywords***: High technology business; innovation problems of Pentagon; information vulnerability; deterrence strategy of cyberintrusions.*

About the author:
ROGOVSKY Evgeni Alexandrovich, Cand. Sci. (Economy), Head of the Center for military-industrial policy.