ЕЛЕНА ЛАРИНА
ВЛАДИМИР ОВЧИНСКИЙ

# КИБЕРВОЙНЫ XXI ВЕКА

## О ЧЕМ УМОЛЧАЛ ЭДВАРД СНОУДЕН

Елена Ларина
Владимир Овчинский

# КИБЕРВОЙНЫ XXI ВЕКА

## О ЧЕМ УМОЛЧАЛ ЭДВАРД СНОУДЕН

Москва • Книжный мир • 2014

Елена Ларина, Владимир Овчинский
**Кибервойны XXI века. О чем умолчал Эдвард Сноуден.** – М.:Книжный мир, 2014. – 352 с.

**ISBN 978-5-8041-0723-0**

Мир на пороге великих перемен, имя которым – Третья производственная революция. И как любая другая революция, эта сопровождается войнами, переделом собственности и сменой господствующих элит. Только это – кибервойны, которые ведутся в Сети кибероружием за господство в будущем кибермире. Сможет ли Россия осуществить прорыв и сотворив «Русское чудо XXI века», занять достойное место в новом, цифровом мироустройстве или потерпит сокрушительное поражение на виртуальных полях сражений незримой Третьей мировой кибервойны и канет в Лету? Будущее покажет.

А каким это будущее может быть, читатель узнает из новой книги эксперта по конкурентной разведке Елены Лариной и известного российского криминолога, генерал-майора милиции в отставке, доктора юридических наук Владимира Овчинского.

ЗАО «Книжный мир»
Тел.: (495) 720-62-02
www.kmbook.ru

**ISBN 978-5-8041-0723-0**

# Введение
# КАРТОГРАФИЯ ЦИФРОВОЙ СРЕДЫ

Цифровая среда включает в себя все многообразие информационных технологий и киберпространство. Киберпространство в строгом смысле этого слова представляет собой ту часть цифровой среды, где происходит управление различного рода объектами физического мира, посредством передачи программ в виде сигналов по Интернету, другим сетям и телекоммуникационным каналам.

Цифровая среда имеет собственные:

• инфраструктуру. Она включает в себя, во-первых, телекоммуникационные и интернет линии (оптоволоконные кабели и т.п.), во-вторых, вычислительные комплексы различной размерности – от суперкомпьютеров до смартфонов и планшетных компьютеров, и, в-третьих, вычислительные управляющие встроенные блоки в различного рода объекты физического мира, начиная от производственных линий, заканчивая кроссовками и майками;

• структуру. Она состоит, во-первых, из сетевых программных протоколов, обеспечивающих передачу информации по различным сетям, включая интернет, корпоративные сети, одноранговые сети (типа Tor) и т.п., во-вторых, программы и программные платформы, осуществляющие хранение, переработку и представление информации – от баз данных до привычных всем операционных систем, типа Windows, Linux и т.п., и, наконец, в-третьих, программы-интерфейсы, обеспечивающие восприятие информации конечными пользователями (интерфейсы сайтов, блогов, порталов, приложений, различного рода программ и т.п.);

• ультраструктуру. Она представляет собой инфосферу, где содержатся воспринимаемые человеком прямые и скрытые смыслы, выраженные в текстах, таблицах, видео- и аудиоконтенте. Ультраструктура включает в себя, во-первых, общедоступные сетевые ресурсы, типа сайтов, блогов, порталов, социальных сетей и т.п., во-вторых, защищенные, доступные только для определенных категорий пользователей информационные ресурсы государственной и корпоративной принадлежности, в-третьих, общедоступные ресурсы с платным контентом.

За почти 25-летнюю историю развития общедоступных коммуникационных сетей, с 1991 г., когда к закрытой сети получили возможность подключаться все желающие, сложилось два принципиально различных их типа:

• Интернет, а также внутренние государственные и корпоративные сети, недоступные для сторонних пользователей. Эти сети построены по иерархическому принципу. В сетях существует несколько уровней иерархии, которые аккумулируют и передают информацию. Соответственно, права и возможности регулирования информации на каждом уровне зависят от его положения в иерархии, чем выше уровень, тем больше возможностей и прав.

• так называемые пиринговые, или одноранговые сети. Наиболее популярные из них в настоящее время – коммуникационная сеть Tor и платежная сеть «Биткойн». В одноранговых сетях информация передается между компьютерами пользователей, которые имеют абсолютно равные права и возможности в передаче информации. Но за равенство надо платить. Поэтому одноранговые сети работают, как правило, медленнее, чем привычный Интернет.

Указанные типы сетей функционируют независимо друг от друга. Соответственно ресурсы одной сети не обнаруживаются и не находятся поисковыми системами

другой сети. При этом в каждой из сетей предусмотрены специальные порталы, которые облегчают пользователям использование ресурсов в другой сети.

Интернет имеет следующую картографию:

• web 1. Это наиболее старый, сложившийся сегмент сети. Он включает в себя правительственные, корпоративные, общественные, персональные порталы, сайты, блоги, он-лайн СМИ. Ресурсы этого сегмента сети легкодоступны при помощи поисковых систем (типа Google, Yandex и проч.);

• web 2. Это так называемый социальный веб, или веб социальных сетей и платформ. Здесь расположены такие ресурсы, как «В Контакте», Facebook, Twitter и проч. Контент в этом сегменте интернета создается в основном самими пользователями, поэтому он получил название социального веба. Из-за политики собственников платформ и социальных сетей, а также требований приватности они лишь частично видимы для поисковых систем. В этом сегменте ускоренными темпами растет доля видео- и фотоконтента;

• web 3. Этот сегмент интернета появился в последние 2–3 года и растет наиболее быстрыми темпами. Это так называемый «веб мобильных приложений». Интерфейсы приложений размещаются на экранах планшетных компьютеров, смартфонов. Соответственно пользователи работают с приложениями без обращения к поисковым системам, просто устанавливая связь между своим гаджетом и ресурсом (сервисом, порталом и т.п.) через Интернет;

• невидимый Интернет. Невидимый интернет – это ресурсы, которые не обнаруживаются поисковыми машинами, а также порталы, сайты и т.д., доступ к которым предполагает либо платный характер, либо наличие специального разрешения на использование ресурсов. По имеющимся данным, в невидимом интернете находится порядка 90% всего ценного научно-технического, техно-

логического, финансово-экономического и государственного открытого контента. Объемы невидимого интернета постоянно растут. Он развивается более быстрыми темпами, чем web1 и web 2. Главными причинами опережающих темпов являются с одной стороны – стремление к архивации всех доступных данных корпоративными пользователями, а с другой – желание обладателей ресурсов вывести их из общедоступного пользования в платный сегмент, т.е. монетизировать.

• интернет вещей. Представляет собой соединенные через интернет с управляющими центрами встроенные информационные блоки самых различных объектов физического мира, в том числе производственной, социальной, коммунальной инфраструктуры. Так, например, к нему относятся подсоединенные к всемирной сети технологические линии, системы управления водо- и теплоснабжением и т.п. Буквально в последние год-два обязательным требованием по умолчанию стало подключение к интернету всех типов домашнего оборудования, бытовой техники, вплоть до холодильников, стиральных машин и т.п.

• бодинет. Со стремительным развитием микроэлектроники появилась возможность встраивать элементы, передающие информацию в предметы гардероба (кроссовки, майки и т.п.), а также широко использовать микроэлектронику в новом поколении медицинской техники, реализующей различного рода имплантаты – от чипов, контролирующих сахар в крови до искусственного сердца и т.п. Кроме того, тенденцией последних месяцев стало создание распределенного компьютера, который предполагает, что отдельные его элементы распределяются по человеческому телу – фактически человек носит на себе компьютер и взаимодействует с ним круглые сутки.

Большую часть одноранговых сетей относят к так называемому «темному вебу» (dark web). Своему на-

званию этот сегмент сети обязан широким использованием своих ресурсов различного рода преступными, незаконными группами и группировками. Основными сегментами этого веба являются сеть Tor, созданная в 2002 г. военно-морской разведкой США и платежная сеть «Биткойн». В настоящее время сети используются преимущественно для противоправной деятельности, киберпреступности, торговли наркотиками, оружием и т.п., а также осуществления целенаправленных акций по подрыву государственного суверенитета.

Особый сегмент сети, частично располагающийся в сети интернет, частично – в специально созданных одноранговых сетях, составляет так называемые «сети денег». Общемировой тенденцией является сокращение наличного платежного оборота и переход к электронным деньгам во всех их видах. Сети денег включает в себя специализированные телекоммуникационные расчетные сети, связывающие крупнейшие банки, типа SWIFT, а также платежные системы, использующие интернет, типа PayPal, «Яндекс.Деньги» и т.п. Отдельным, быстро развивающимся сегментом денежных сетей являются специализированные платежные системы, базирующиеся на одноранговых сетях и зашифрованных сообщениях. Наиболее известная из этих систем – это платежная система «Биткойн».

Таким образом, цифровая среда имеет сложную картографию, где отдельные сегменты развиваются по собственным, независимым от общих закономерностей, трендам. При этом целый ряд основополагающих тенденций являются общими для всех сегментов цифровой среды.

Первой основополагающей тенденцией цифровой среды является информационный взрыв. В последнее время объем информации удваивается каждые два года. По данным компании Cisco объем сгенерированных данных в 2012 году составил 2,8 зеттабайт и увеличится

до 40 зеттабайт к 2020 г. Примерно треть передаваемых данных составляют автоматически сгенерированные данные, т.е. управляющие сигналы и информация, характеризующие работу машин, оборудования, устройств, присоединенных к Интернету. На 40% ежегодно растет объем корпоративной информации, передаваемой и хранящейся в сети Интернет.

Число пользователей интернета в мире к концу 2013 года составило 2,7 млрд. человек, или 39% населения земли, а к 2016 году эта доля составит 65-75% населения по данным Центра новостей ООН. Как ожидается, количество корпоративных пользователей Интернета во всем мире увеличится с 1,6 миллиарда в 2011 году до 2,3 миллиарда в 2016 году.

Если в 2012 году более 90% пользователей выходили в сеть с компьютеров всех типов, и лишь 10% – с мобильных устройств, то к 2016 году доля планшетников, смартфонов и других гаджетов увеличится как минимум до 45-50%.

Россия входит в число ведущих стран по числу пользователей Интернетом. В настоящее время более 55% населения взаимодействует с Интернетом. В крупных городах им охвачено более 75% населения. Происходящее из года в год снижение стоимости широкополосного доступа в интернет, переход на новые стандарты мобильной связи, обеспечение доступа в интернет жителям ранее не охваченных им районов страны, открывают принципиально новые возможности для экономического, общественного и социального развития.

Прежде всего, появляются возможности для создания общегосударственной и корпоративных систем непрерывного дистанционного образования и целевого формировании компетенций по наиболее востребованным, в том числе ранее не существовавшим профессиям и специальностям. Не меньшие возможности открываются перед интернет-медициной, которая в последние несколько лет получила широчайшее распространение

в США, Западной Европе, ряде других стран. При этом следует отметить, что в России еще в конце 90-х – начале 2000-х годов в системе РЖД была создана охватывающая всю территорию страны система интернет-медицины, которая с учетом новых технологических возможностей может быть использована как в общегосударственном масштабе, так и в масштабе отдельных регионов, либо крупных корпораций.

Огромные возможности имеются у российской интернет-коммерции. По своим объемам она в 2013 году занимала 13 место в мире. Но по темпам роста она первенствует в Европе. Ключевыми вопросами для устойчивого роста интернет-торговли является опережающее развитие безналичного платежного оборота в виде электронных платежей по кредитным картам и т.п. Развитию российской интернет-коммерции будут способствовать также соответствующие международному законодательству меры по недопущению демпинга со стороны внешних рынков электронной коммерции. Подобные меры в настоящее время действуют в Германии, Великобритании, других странах.

Исторически Интернет формировался как свободная среда информационного взаимодействия при неформальном, но реализованном через жесткие технологические программные и организационные способы контроле со стороны Соединенных Штатов Америки – страны-создателя всемирной паутины. В результате, к настоящему времени сложилось парадоксальное положение. В интернет в значительной степени переместились торговля, финансовые операции, политическая и социальная активность, т.е. ключевые сферы жизнедеятельности каждого государства. Между тем в интернете, в отличие от физической реальности, не признаны поствестфальские принципы международного права. Безусловно, обеспечение «цифрового суверенитета», совместное международное управление интернетом и

распространение принципов поствестфальской международной системы на интернет с учетом его особенностей являются важными направлениями внешнеполитической активности России и все большего числа стран, придерживающихся сходных взглядов на принципы международно-правового регулирования Интернета.

Второй важнейшей тенденцией изменения цифровой среды становится формирование Интернета вещей. Интернет вещей – это самые разнообразные технологические, производственные, инфраструктурные устройства, приборы, приспособления и т.п., имеющие блоки контроля, передачи информации и управления, соединенные с интернетом. В настоящее время к интернету уже подключено более 17 млрд. устройств.

Согласно сделанному IDS прогнозу к интернету вещей к 2020 году будет подключено 212 миллиардов устройств, а денежная ёмкость этого рынка I составит 8,9 трлн. долларов. Причём в интернете вещей образца 2020 года окажется 30,1 млрд. автономных устройств, от автомобилей до пылесосов.

Развитие интернета вещей открывает поистине безграничные перспективы и возможности для российской и мировой экономики. Анализ данных, поступающих от соединенных с интернетом инфраструктурных объектов, позволяет, как показывает мировой опыт, на 20-30% сократить время, проводимое на перегруженных автомобильных трассах, более чем на 15% сократить непроизводительные расходы воды и электроэнергии в жилых и производственных зданиях и т.п. Как свидетельствует опыт Финляндии и Норвегии, использование технологии «умных домов» и «умных кварталов», предусматривающей, в том числе подсоединение к интернету системы как поквартирного, так и централизованного тепло- и энергоснабжения позволяет на 12-17% уменьшить расходы на отопление при сохранении неизменной температуры в жилых помещениях. Понятно, что

в условиях нашей страны использование интернета вещей в подобных сферах даст еще более впечатляющий эффект. Этот эффект может быть связан, во-первых, с природно-климатическими особенностями нашей страны, во-вторых, со значительным отставанием реализации программ экономии различных, в том числе, коммунальных ресурсов, и, в-третьих, с достаточным и все возрастающим количеством мегаполисов и агломераций, где он проявляется наиболее сильно и масштабно.

Как правило, угрозы, связанные с интернетом вещей сводят к различным видам киберпреступности и даже к кибертерроризму. Понятно, что в условиях, когда вся инфраструктура населенных центров, отдельных жилых кварталов, домов и просто жизнедеятельности каждого человека полностью завязана на интернет вещей, злонамеренное вторжение в Интернет вещей может привести к трудно предсказуемым последствиям. Поэтому первостепенной задачей государств с высоким уровнем интернетизации населения и доходов, позволяющих приобретать предметы со встроенным интернетом, становится налаживание теснейшего международного сотрудничества по борьбе с киберпреступностью и кибертерроризмом. Причем, уже сегодня ясно, что это сотрудничество не должно ограничиваться принятием соответствующих юридических актов, но и должно предполагать каждодневный обмен информацией и эффективным инструментарием борьбы против киберпреступности и кибертерроризма. Более того, заслуживает внимания предложение о создании объединенных добровольных международных сил по противодействию трансграничным киберпреступным и кибертеррористическим группировкам. Россия, располагающая первоклассными специалистами и имеющая целый ряд компаний-резидентов, являющихся лидерами в сфере индивидуальной и корпоративной информационной безопасности, несомненно, может сыграть в этой работе заметную роль.

Существует еще одна в должной мере неосознаваемая угроза цифровому суверенитету России, связанная с интернетом вещей. В настоящее время поисковые системы и платформы социальных сетей, такие, как Facebook, Twitter и др. позволяют анализировать поведение пользователей, объединяемых в самые различные группы, их предпочтения, активности, связи и т.п. С появлением интернета вещей такой мониторинг в режиме он-лайн может вестись уже не в отношении интернет-активности, а в отношении реальной жизнедеятельности населения, функционирования предприятий, организации работы городских и иных структур. Дело в том, что в рамках интернета вещей информация передается в компании-производители изделий, соединенных с интернетом, либо, в компании-поставщики чипов, микропроцессоров. Соответственно именно в этих компаниях, наряду с индивидуальными, корпоративными или государственными пользователями систем, оснащенных интернетом вещей, оказывается полная информация о реальном мире в режиме он-лайн. Именно поэтому ведущие интернет-компании, например, Google начали заключать сделки ценой от сотен до миллиардов долларов по приобретению компаний, связанных с интернетом вещей. Этой угрозы можно избежать двумя способами. Радикально – развив собственную микроэлектронную промышленность, производящую чипы для приборов, оборудования и систем, подсоединенных к интернету вещей. Паллиативно, установив в качестве обязательного условия для продажи на территории РФ предметов, оборудования и устройств, подключенных к интернету, наличие на территории РФ и подпадающих под его юрисдикцию центров обработки данных (ЦОД) соответствующей компании.

Буквально на наших глазах рождается нательный, носимый интернет, или как его еще называют «бодинет». Этот фрагмент сети складывается из трех сегмен-

тов. Прежде всего, появились уже первые предвестники эры распределенных компьютеров, типа очков Google Glass. Вторым сегментом являются предметы гардероба, т.е. повседневная одежда, обувь и т.п., соединенная с интернетом и контролирующая, как правило, состояние здоровья или иных параметров обладателя гардероба. Наконец, наиболее активно в перспективе будет развиваться сегмент, связанный с электронными компонентами микроустройств и микроприспособлений, непосредственно имплантированных в тело человека. Так, на сегодняшний день уже около миллиона американцев имеют медицинские имплантаты, подсоединенные к интернету, в основном связанные с кардиоконтролем, а также контролем за состоянием сахара в крови. Ежегодно цена на такого рода имплантаты падает не на проценты, а в разы. Также по экспоненте увеличивается количество такого рода имплантатов, в значительной мере порожденных достижениями биотехнологий и микроматериаловедения. Есть основания полагать, что в ближайшие 5-7 лет встроенные в человеческое тело имплантаты, соединенные с интернетом, из экзотики превратятся в обыденность практически во всех развитых странах мира.

При общем отставании в лечебном, в том числе коммерческом использовании такого рода имплантатов, российские исследователи имеют целый ряд впечатляющих разработок и в целом входят в число мировых лидеров в сфере медицинских кибертехнологий. Соответственно при должной организации взаимодействия частного бизнеса и государства в этой сфере отечественный высокотехнологичный бизнес не только может сохранить за собой значительную долю внутреннего рынка, но и имеет хорошие шансы выдержать конкуренцию в отдельных сегментах глобального рынка высоких медицинских интернет-технологий.

Широкое распространение бодинета порождает принципиально новые типы угроз, связанные с возмож-

ностью осуществления киберпреступлений, вплоть до нанесения тяжелых телесных повреждений и убийств, а также целевого точечного кибертерроризма. В Соединенных Штатах данная угроза рассматривается как актуальная, и как на государственном уровне, так и на уровне частных компаний разрабатываются конкретные меры по противодействию ей. Принимая во внимание признанную во всем мире высочайшую квалификацию российских специалистов в сфере тестирования на несанкционированное проникновение (этичные хакеры) есть отличный шанс превратить угрозу в возможность для российского бизнеса, и опосредованно для российского государства. Для реализации этой возможности надо в кратчайшие сроки выступить с российской частно-государственной инициативой на международной арене по созданию единого пула производителей медицинских имплантатов, микроэлектронной техники и компаний в сфере информационной безопасности и тестировании несанкционированного проникновения. Такой пул может в перспективе стать надежным щитом для массовой киберпреступности, связанной со злонамеренным вмешательством в работу имплантатов, соединенных с интернетом.

# Глава 1
# КИБЕРВОЙНЫ XXI ВЕКА

В выступлении на Генеральной Ассамблее ООН, посвященном событиям в Сирии, Барак Обама сказал об исключительности Америки и ее праве на военное насилие: «Я считаю, что Америка – исключительная страна: отчасти потому, что все видели, как мы проливаем кровь и не жалеем средств, отстаивая не только свои узкие интересы, но также и всеобщие интересы... Будут ситуации, когда международному сообществу придется признать, что во избежание наихудшего развития событий может потребоваться многостороннее военное вмешательство». Такой подход несомненно еще более дестабилизирует и без того сложную международную геополитическую обстановку и толкает цифровой мир к эпохе кибервойн.

Реально ведущаяся кибервойна, воспринимаемая до последнего времени некоторыми политиками и аналитиками и в России, и за рубежом как некая экстравагантная тема, приобрела в августе 2013 года реальное воплощение. Связано это с документами, которые оказались доступными для журналистов и аналитиков, благодаря Эдварду Сноудену. Речь идет отнюдь не о программах Prism и XKeyskore, или тотальной прослушке мобильных операторов, и даже не о доступе АНБ к серверам Google, Microsoft, Facebook, Twitter, международной сети банковских транзакций SWIFT, процессинговым система Visa, MasterCard и т.п.

Самыми интересными и пока недостаточно оцененными стали документы в составе досье Сноудена, полу-

чившие название – «файлы черного бюджета американского разведывательного сообщества». Российские СМИ, да и экспертное сообщество ограничились обсуждением 231 наступательной кибероперации и броской цифры – 500 млрд. долларов расходов на разведку в США за 2001-2012 гг.

Эти документы, опубликованные газетой Washington Post, дают большую пищу для по-настоящему серьезного анализа. В отличие от слайдов презентаций и мало кому интересных списков IP адресов, аналитики получили в свое распоряжение множество сухих бюджетных цифр и сопровождающие их пояснительные документы, излагающие бюрократическим языком факты, замечания и предложения, касающиеся настоящих, а не медийных секретов американской разведки и армии.

Анализ этих документов позволяет сделать вывод, что в мире уже ведется необъявленная крупномасштабная цифровая, или кибервойна. Единственно остающийся вопрос: когда в этой войне появятся первые человеческие жертвы и масштабные разрушения крупных материальных объектов?

### 1.1.Феномен кибервойн

Термин «кибервойны» прочно вошел не только в лексикон военных и специалистов по информационной безопасности, но и политиков, представителей экспертного сообщества. Он стал одним из мемов, активно поддерживаемых и распространяемых СМИ всех форматов. Более того, кибервойны стали одной из наиболее обсуждаемых тем в социальных сетях, на интернет-площадках и т.п.

Между тем, существует достаточно серьезное различие в понимании кибервойн, что называется на бытовом уровне и в популярных СМИ, и определением кибервойн профессионалами информационной безопасности и военными.

Среди политиков, медиатехнологов, в СМИ весьма популярна расширительная трактовка кибервойн. Фактически, под ними понимается любое противоборство в кибер- или интернет-пространстве. Некоторые специалисты и эксперты к кибервойнам относят многоаспектные и сложные информационные компании, нацеленные на изменения ценностных ориентаций, политических предпочтений, а иногда даже культурных кодов. Наконец, в разряд кибервойн попадают и репутационные войны, которые ведутся между различными бизнес-группами, компаниями, корпорациями, получившие название «войн брендов».

Такое понимание связано в значительной степени с историей развития информационных технологий вообще и интернета в частности. Первоначально в лексикон военных вошел термин «информационная война». Его ввела в оборот корпорация RAND в 1990 г. Чуть позднее ведущий сотрудник этой корпорации Мартин Либитски опубликовал книгу «Что такое информационная война». Примерно 10 лет его точка зрения была общепринятой. По М. Либитски эта война имеет семь типов: командно-управляемый, разведочный, психологический, хакерство, экономический, электронный и киберборьба. Свою точку зрения автор продолжает отстаивать до сегодняшнего дня. При этом, несомненное первенство он отдает психологическому воздействию, в первую очередь, дезинформации, PR-компаниям и специальным информационным операциям.

Однако с активным развитием информационных технологий возникла естественная потребность вычленять из общего отдельные направления. Впервые это было сделано американскими военными Джоном Аркуилла и Дэвидом Ронфилдом в статье «Cyberwar is Coming!», опубликованной весной 1993 г. в одном из ведущих журналов американских вооруженных сил Comparative Strategy (т. 12, №2). В сфере информационной безопас-

ности термин «кибервойны» стал широко использоваться с 2007 г.

С конца первого десятилетия нынешнего века четкое разделение информационных и кибервойн стало общепринятым стандартом для военных, специалистов в сфере информационных технологий и информационной безопасности. В первую очередь это произошло в тех странах, которые оказались во главе начавшейся гонки кибервооружений, прежде всего США, Китая, Израиля и т.п.

В то же время в России некоторые аналитики продолжают отождествлять информационные и кибервойны. Они рассматривают их, прежде всего, под углом зрения воздействия информационных потоков на коллективную психику и сознание человека. Такая спутанность понятий, объяснимая в первую очередь текущей политической ситуацией и историей нашей страны, несомненно, повлияла на то, что Россия, обладая огромным потенциалом в сфере информационных технологий, должным образом не оценила опасности, риски и угрозы, связанные именно с кибервойнами.

Информационные и кибервойны разделяются по объектам и средствам боевого воздействия.

Информационные войны – это контентные войны, имеющие своей целью изменение массового, группового и индивидуального сознания, навязывание своей воли противнику и перепрограммирование его поведения. В процессе информационных войн идет борьба за умы, ценности, установки, поведенческие паттерны и т.п. Информационные войны велись задолго до интернета, насчитывают историю, измеряемую даже не сотнями, а тысячами лет. Интернет просто перевел эти войны на качественно иной уровень интенсивности, масштабности и эффективности. Объектом воздействия информационных войн являются самые различные субъекты – от небольших групп до целых народов и населения целых

стран. Средством боевого воздействия являются специально созданные семантические сообщения в виде текстов, видео- и аудиорядов, рассчитанные на восприятие сознанием, обработку мышлением и эмоциональный отклик со стороны групп различной размерности.

Что же касается кибервойн, то это целенаправленное деструктивное воздействие информационных потоков в виде программных кодов на материальные объекты и их системы, их разрушение, нарушение функционирования или перехват управления ими.

Бывший высокопоставленный чиновник, а ныне эксперт по безопасности Правительства США Ричард А. Кларк в своей книге «Кибервойна» (2010 г.) дал такое определение: «Кибервойна – это действие одного национального государства с проникновением в компьютеры или сети другого национального государства для достижения целей нанесения ущерба или разрушения».

Генеральный Секретарь ITU Хамадун И.Туре в докладе «В поисках кибермира», опубликованном в 2012 г., писал: «Понятие кибервойны охватывает не только опасности для военных систем и средств, но также и для жизненно важной общественной инфраструктуры, включая интеллектуальные энергосети, сети диспетчерского управления и сбора данных SCADA, которые позволяют им работать и осуществлять самозащиту».

По де-факто сложившемуся, но юридически не закрепленному мнению подавляющего большинства военных и специалистов по информационной безопасности (вне зависимости от их страновой принадлежности), под кибервойнами понимаются целенаправленные действия по причинению ущерба, перехвату управления или разрушению критически важных для функционирования общества и государства сетей и объектов, производственной, социальной, военной и финансовой инфраструктуры, а также роботизированных и высокоавтоматизированных производственных, технологических

линий. Средством боевого воздействия в кибервойнах является программный код, нарушающий работу, выводящий из строя, либо обеспечивающий перехват управления различного рода материальными объектами и сетями, оснащенными электронными системами управления.

Информационные и кибервойны представляют собой две разновидности войн, ведущихся в сетевом электронном пространстве, которое охватывает не только интернет, но и закрытые государственные, военные, корпоративные и частные сети. Для каждого из этих двух типов войн свойственны свои инструментарии, методы, стратегии и тактики ведения, закономерности эскалации, возможности предупреждения и т.п.

Кибервойны тесно связаны с кибершпионажем, киберпреступностью и кибертерроризмом. При этом, необходимо подчеркнуть, что также как и в материальном мире, в электронном пространстве все эти феномены тесно переплетены и взаимодействуют между собой. Это взаимодействие характерно как для взаимной переплетенности атакующих субъектов, так и объектов, подвергаемых атакам. Эти виды преступного поведения используют зачастую схожие программные средства, имеют сходные режимы их применения и т.п.

Есть все основания полагать, что в течение ближайших двух-трех лет сформируются инструментарии и технологии для электронных войн третьего типа, в каком-то смысле объединяющих информационные и кибервойны. Речь идет о том, что в лабораториях уже прошли практическую апробацию аппаратные и программные средства, обеспечивающие прямую и обратную связи между изменениями психики, или как еще говорят идеального или субъективного, и преобразованием реального мира, соответственно, материи, материальных объектов, их систем, сетей и т.п. Первые публикации на этот счет появились в США и России в этом году. В них говорится о пси-войнах, нейровойнах и т.п.

### 1.2. История кибервойн

Как известно, история в современном мире является в значительной степени инструментом информационного противоборства. Не избежала этой доли и весьма короткая история кибервойн. Например, в электронном журнале «Вестник НАТО», в статье «История кибератак: хроника событий» история кибервойн начинается с якобы имевшей место в апреле 2007 г. атаки на эстонские государственные сайты и сети со стороны неизвестных иностранных злоумышленников. Вторым ключевым событием кибервойн журнал считает взлом и вывод из строя иностранными злоумышленниками Интернет-сетей в Грузии в августе 2008 г.

При этом и в первом и во втором случаях, вне зависимости от их реальности имели место кибератаки, никак не связанные с нарушением работы критически важных инфраструктурных сетей и объектов. В этом смысле четкое понимание кибервойн, как воздействия из киберпространства на материальные объекты, сети, системы является чрезвычайно важным.

Исходя из этого, большинство экспертов считает, что установленные случаи использования кибероружия, т.е. фактически кибервойны, связаны с деятельностью Соединенных Штатов и Израиля. А в части кибершпионажа несомненное первенство держит Китай.

Первое задокументированное использование кибероружия в ходе крупномасштабных военных действий связано с применением программ, блокирующих работу сирийских ПВО и радиоэлектронной разведки во время проведения так называемой операции «Оливы» в 2008 г.

Масштабное применение кибероружия впервые имело место по данным «Лаборатории Касперского» в Иране в 2010 г. В отличие от обычных вредоносных программ, работающих в популярных операционных системах, примененный против Ирана вирус Stuxnet был

специально создан для проникновения в автоматизированные системы, регулирующие и управляющие определенным типом оборудования, связанным с конкретными технологическими цепочками в атомной промышленности. Первоначально никто не брал на себя ответственность за создание и использование этого вируса, однако, не так давно американские официальные лица подтвердили, что он был создан в системе АНБ с участием израильских компаний для противодействия иранской атомной программе. Еще более сложная, многокомпонентная боевая программа была применена американцами и израильтянами против нефтяных терминалов и нефтеперерабатывающих заводов все того же Ирана.

Кроме того, были зафиксированы случаи использования компьютерных вирусов для вывода из строя систем SCADA крупнейшей саудовской нефтяной и катарской газовой компаний.

Серьезным уроком краткой истории кибервойн является тот факт, что некоторые страны быстро поняли, что кибероружие является дешевым и эффективным способом противодействия высокотехнологичным вооружениям. Характерным примером использования кибероружия является перехват системы управления новейшим американским беспилотником и его принудительная посадка на территории Ирана.

По данным ведущих компаний в сфере информационной безопасности в последние год-два наблюдается буквально эскалация кибервооружений. В последнее время были обнаружены такие многофункциональные программы слежения, шпионажа и доставки боевых вирусов, как Flame и Jaiss. По мнению «Лаборатории Касперского», поддержанному крупнейшими экспертами самых различных стран, разница между Stuxnet и обнаруженными новыми многофункциональными программами кибервойны примерно такая же, как между рядовым эсминцем и самым современным авианосцем.

Еще одним уроком кибервойн является тот факт, что согласно данным печати и отдельным отрывочным заявлениям официальных лиц, над этими и другими видами кибервооружений в виде целевых вирусов и многофункциональных программ непосредственно трудились частные компании, а иногда даже группы специально нанятых хакеров. Такой подход полностью соответствует принятому, например, США активному привлечению частных компаний к выполнению функций внутри военных и разведывательных структур. Подобная тактика позволяет государствам отмежевываться от актов кибераграссий и кибертерроризма.

В этой связи наводят на размышления факты, всплывшие в ходе скандала со Э. Сноуденом. Например, выяснилось, что, в АНБ до 70% не только исследовательских, но и текущих оперативных работ выполняется частными подрядчиками. По имеющимся данным такая же картина характера для Великобритании, Израиля и ряда других стран.

### 1.3. Реалии кибервойн

Короткая история киберагрессий, а также анализ кибершпионажа и крупномасштабной киберпреступности дают достаточно материалов для выделения основных черт кибервойн, в корне отличающих их от всех других типов военных действий.

Прежде всего, несомненным является высокий уровень анонимности кибервойн. Он связан с трудностями определения киберагрессора. Частично эти трудности сопряжены с самой природой кибервойны, как воздействий в системе компьютер/компьютер через многослойные и запутанные сети электронных коммуникаций. Кроме того, имеются многочисленные, постоянно совершенствующиеся программные средства установления помех, затрудняющих обнаружение хакерских программ, находящихся на вооружении боевых подразделений,

разведывательных структур и преступных группировок. Достаточно привести пример крупнейшей кибершпионской сети Red October, которая беспрепятственно действовала в киберпространстве с 2007 по 2012 гг., когда не без труда была обнаружена экспертами «Лаборатории Касперского».

Поскольку между шпионским и боевым софтом нет принципиальной разницы, за исключением функционала основной программы (в первом случае, нацеленной на выкачивание файлов из различного рода сетей и ресурсов и отслеживание действий на компьютерах пользователей, а во втором случае – на разрушение/перехват подсистем автоматического управления теми или иными объектами или сетями), то приведенный пример является весомым аргументом в пользу высокой степени анонимности кибервойн.

Другой отличительной особенностью кибервойн является неопределенность времени их начала. Все привычные человечеству виды войн начинались с хорошо фиксируемых материальных действий и соответственно имели четкую временную привязку. Многокомпонентные программы, как основное оружие кибервойн, могут проникать в сети и управляющие системы разнообразных военных и гражданских объектов и инфраструктур заблаговременно. В этом случае фактическим началом войны будет проникновение этих программ в сети, а фиксируемым моментом начала боевых действий станет активация указанных программ в целях разрушения, либо перехвата управления над инфицированными сетями и объектами.

Уникальной особенностью кибервойн является их потенциальная бесследность. Любое известное вооружение имеет ярко выраженные признаки применения, которые позволяют с уверенностью говорить о начале, ходе и последствий военных действий. Хорошо известно, что с первых дней разработки различного рода ха-

керского софта одной из главных задач было обеспечение необнаруживаемости последствий его использования. В этом направлении, как свидетельствует практика незаметного преодоления систем информационной безопасности как крупных корпораций, так и государственных сетей различных стран, достигнуты большие успехи. Соответственно, очевидно, что при разработке боевого софта особое внимание будет уделяться маскировке последствий его использования под имитацию обычных технических отказов, сбоев в работе, либо последствий ошибок со стороны обслуживающего персонала. По мнению и российских, и зарубежных экспертов в области информационной безопасности, все необходимые предпосылки для решения подобных задач имеются уже на сегодняшний день.

Еще одной отличительной чертой кибервойн является отсутствие в этих войнах таких привычных понятий, как «фронт», «тыл». Фактически в кибервойнах потенциальным фронтом, т.е. местом боевых действий являются любые – и военные, и гражданские компьютерные сети и завязанные на них объекты и инфраструктуры.

Следует честно признать и такую крайне неприятную черту кибервооружений, как чрезвычайная сложность их контроля со стороны государственных систем разведки и безопасности. Как полагают многие специалисты, в наиболее изощренных вариантах по своим последствиям кибероружие сравнимо с применением ядерных боевых зарядов. В этом плане есть смысл сравнить возможности контроля над боевым софтом и производством ядерных вооружений. Как известно из многих отчетов на эту тему, насчитывается около 50 перекрестно подтвержденных случаев попыток завладения расщепляющими материалами, либо технологиями, связанными с производством атомного оружия со стороны террористических группировок и государств, не обладающих атомным оружием. Все подобные попытки были пресечены, поскольку спец-

службы уже давно научились контролировать трафик радиоактивных материалов, отслеживать производителей соответствующего оборудования и выявлять логистику практически в режиме реального времени.

Прямо противоположная ситуация складывается с контролем за производством боевого софта. Главное, что требуется для его изготовления – это высококвалифицированные программисты и аппаратная часть, которая может быть собрана своими силами из комплектующих, массово продаваемых на открытом рынке. Отследить таких производителей является крайне сложной задачей. Разработка боевого софта сегодня доступна не только для государств и крупных корпораций, но и для небольших, хорошо финансируемых групп. А деньги, как хорошо известно, являются едва ли не самым малодефицитным ресурсом в современном мире. Практическим доказательством данного тезиса являются многочисленные факты вывода из строя (либо задание ложных целей) путем целенаправленного программного воздействия американских вооруженных беспилотников в ходе боевых действий в Афганистане.

Наконец, нельзя не сказать о такой отличительной черте кибервойн, как отсутствие для них каких-либо рамок международного регулирования. На первый взгляд на такие рамки может претендовать так называемое Таллиннское руководство по ведению кибервойны (The Tallinn Manual on the International Law Applicable to Cyber Warfare). Однако Руководство не является официальным документом ни НАТО, ни стран, которые входят в НАТО. Это всего лишь частная точка зрения участников рабочей группы, которая написала Руководство в значительной степени в методологической и учебных целях.

Как правило, отсутствие правового регулирования кибервойн связывают с непроработанностью юридических аспектов вследствие новизны вопроса. Однако, на наш взгляд, проблема гораздо глубже и серьезнее. На

сегодняшний день интернет управляется организацией ICANN, фактически подконтрольной США и ее ближайшим союзникам. Однако в самые последние месяцы в значительной степени под воздействием разоблачений Эдварда Сноудена даже ближайшие союзники США в Европе, Латинской Америке, Азии требуют интернационализации управления интернетом. В частности, это нашло свое отражение в документах состоявшейся в 2013 г. в Монтевидео очередной конференции ICANN. На этой конференции было принято решение дистанцироваться от Правительства США и вывести всех его представителей из руководящих органов ICANN.

Важно, что регулирование осуществляется в рамках парадигмы «один мир – один интернет». При таком подходе вообще невозможны какие-либо привычные в военном праве межгосударственные соглашения. Дело в том, что ICANN отрицает право государств так или иначе регулировать, а значит, и нести ответственность за тот или иной сегмент интернета. Таким образом, имеет место парадокс. Де факто интернет и другие сети имеют наднациональный характер, а боевые действия в киберпространстве ведутся в отношении конкретных национальных государств и их структур. В рамках сложившейся ситуации, никакие юридические, и шире – согласительные механизмы профилактики и предотвращения кибервойн просто не могут действовать.

Таким образом, приведенные характерные черты кибервойн позволяют сделать вывод об их уникальности относительно всех других типов военных действий. Эти же свойства делают кибервойны особо опасными, легко развязываемыми и трудно урегулируемыми.

### 1.4. Факторы угрозы

Тенденции технологического развития, темпы и противоречивость мировой динамики являются дополнительными дестабилизирующими факторами. Эти фак-

торы повышают вероятность, расширяют масштабы и увеличивают разрушительную мощь применения кибероружия.

Экспоненциально растет интернет вещей. Уже сегодня он включает в себя не только бытовую технику и даже предметы гардероба, но и «умные» дома, кварталы и города, где практически все сети и предметы имеют встроенные, либо удаленные системы автоматизированного контроля и управления, подключенные к интернету. Сегодня большинство IP адресов принадлежат не пользовательским и корпоративным устройствам и сетям, а также Интернет-ресурсам, а промышленным, инфраструктурным объектам, а также системам управления вещами и сетями, буквально окружающими современного горожанина. Согласно данным компании Cisco, уже в настоящее время на интернет вещей приходится 10 млрд. IP адресов, а в 2020 г. число таких адресов возрастет не менее чем до 50 млрд.

По оценкам ведущей аналитической компании Neilsen, уже сегодня интернет вещей берет на себя более 70% интернет-трафика. По сути, всеобщая интернетизация вещной среды, окружающей человека, как на производстве, так и в быту крайне обостряет проблему информационной безопасности, поскольку многократно увеличивает количество взаимодействующих сетей. В условиях, когда даже крупнейшие государственные сети практически ежемесячно оказываются жертвами хакеров, ожидать, что будет обеспечена должная защита всех компонентов интернета вещей, было бы утопией. По данным компании Symantec, производителя линейки программ Norton, в настоящее время не более 3% вещей, имеющих выход в интернет, имеют хотя бы минимально допустимый уровень информационной безопасности. Для боевых программ интернет вещей является едва ли не самым уязвимым сегментом электронных коммуникаций.

Буквально на наших глазах, вслед за интернетом вещей появился так называемый «бодинет». Он включает в себя миниатюрные электронные устройства, используемые в диагностических, лечебных целях, а также во все ширящихся системах прямого интерфейса компьютер-человек. Первой ласточкой такого рода интеграции являются уже поступившие в продажу так называемые очки Google Glass. По оценкам экспертов, в течение ближайших двух-трех лет успехи нанотехнологий позволят создать массовые продукты на основе контактных линз, имплантированных контрольных чипов для людей с хроническими заболеваниями и т.п. Уже в этом году только в Соединенных Штатах будет продано более 12 млн. индивидуальных медицинских приборов, приспособлений и имплантатов, подключенных к интернету. Как правило, такие системы имеют единые пункты контроля и управления в компаниях-изготовителях. Причем, взаимодействие между микроустройствами на теле, либо в теле человека и управляющим центром опять же осуществляется по интернет-линиям. Это не фантастика. В этом году в Соединенных Штатах уже вынесен приговор, связанный с убийством посредством отключения кардиостимулятора, параметры работы которого контролировались через интернет. Развитие бодинета, несомненно, открывает новые горизонты, прежде всего, для кибертерроризма и специальных операций в ходе кибервойн.

Невиданные ранее чрезвычайно благоприятные для применения кибервооружений, кибертерроризма и кибершпионажа возможности открывает уже совершившийся переход к множественности подключений к общедоступным и внутренним сетям с одного устройства. До взрывного роста мобильного интернета с практически полным охватом населения развитых стран мира такими устройствами, как планшетники, смартфоны и т.п., была возможность решать проблему информационной безопасности за счет размежевания общедоступных

и внутренних сетей аппаратным способом. Грубо говоря, одни компьютеры предназначались для дома или работы в открытых сетях, а другие, не связанные с интернетом компьютеры, функционировали в составе закрытых, высокозащищенных сетей. На сегодняшний день имеются уже не сотни, а тысячи примеров, когда несмотря на все увещевания специалистов по информационной безопасности, работники самого разного ранга, как в государственном (в том числе военном) секторе, так и в частных компаниях используют одни и те же мобильные устройства для работы со множеством сетей, и в первую очередь с общедоступным интернетом.

Свою лепту в создание дополнительных угроз вносит и активное развитие облачных вычислений. Облачные вычисления делают доступными для бизнеса, государственных структур наиболее дорогостоящие и сложные программные продукты, обеспечивают значительную экономию на развертывании аппаратной и программной частей IT инфраструктуры, содержании высококвалифицированных системных администраторов и т.п. Но их экономические достоинства могут обернуться существенными проблемами в сфере информационной безопасности. Облачные технологии априори предусматривают, особенно в корпоративном секторе, наличие множественности пользователей облака и распределение ответственности за информационную безопасность между организацией-собственником облачной платформы, интернет-провайдером и организацией-пользователем. А любая распределенная ответственность означает ее размывание, а значит появление слепых пятен и зон информационной опасности. Кроме того, экономия достигается за счет резкого снижения уровня компьютерной квалификации для персонала организаций-пользователей облачных платформ. Редко в какой из таких организаций имеются специальные

офицеры по информационной безопасности и соответственно системы защиты от разнообразных киберугроз.

Нельзя не выделить как отдельный, сильнодействующий фактор угрозы, кластерный характер происходящей на наших глазах технологической революции. Информационные технологии с коммуницированием как по закрытым, так и по общедоступным сетям, де-факто стали обязательным компонентом таких решающих для мировой экономики направлений, как робототехника, 3D печать, биотехнологии. Со стремительным удешевлением этих технологий, их все расширяющемся распространением, превращением в основу постиндустриальной промышленной революции, интернет становится буквально вездесущим в производственной и экономической жизни.

Особые риски создает теснейшая интеграция информационных и биотехнологий. Удешевление за последние пять лет примерно в семь раз оборудования для сложных биотехнологических процессов, включая генную, иммунную инженерию и т.п., вместе с широко распространившейся практикой коллективного распределенного использования этого оборудования, делает самые сложные биопроизводства и биоконструирование доступным не только для крупных корпораций, но и для самых маленьких компаний, неформальных групп и отдельных лиц. Такая ситуация не только удешевляет и расширяет сферу применения биотехнологий, но и открывает невиданные ранее возможности для создания кибербиооружия и использования его не только государственными структурами, но и различного рода террористическими группами, а также маньяками-одиночками.

### 1.5. Великий уравнитель

Кибервойны впервые за долгий период истории дают весомые шансы более слабым, менее технологически развитым государствам и наднациональным силам

одержать победу в жестком противоборстве с гораздо более могущественными странами, обладающими превосходящим военным, политическим, экономическим и научно-техническим потенциалом.

Произвести или приобрести высокоуровневое кибероружие могут сегодня не только достаточно ограниченные в ресурсах государства, но и отдельные группы, сети и т.п.

Роль кибероружия, как великого уравнителя сопряжена с тремя главными факторами:

• во-первых, кибернетические войны имеют ярко выраженный ассиметричный характер. Страны, обладающие значительным наукоемким сектором экономики, высокотехнологичной производственной сферой и/или характеризующиеся высоким уровнем внедрения интернета в повседневную жизнь социума, гораздо более уязвимы для применения кибероружия. Когда интернет является одной из несущих конструкций всей инфраструктуры, высокий уровень его защиты становится на практике почти невозможным. Например, подсчитано, что для того, чтобы на должном уровне обеспечить информационную безопасность только военных, правительственных и критических корпоративных и общесоциальных электронных сетей и объектов в США, необходимо потратить сумму средств, неподъемную для американской экономики. В эквиваленте она превышает долю фактических расходов на оборону в государственном бюджете, которые был вынужден нести Советский Союз, чтобы выдержать гонку вооружений, и которая в значительной степени подорвала его экономику;

• во-вторых, в современном мире действует принцип коммулятивности рисков. Страны и их военно-политические объединения несут тем большие риски применения против них кибероружия, чем в большем числе военных конфликтов высокой и низкой интенсивности, гражданских войн и острых внутриполитических

противоборств в третьих странах они участвуют. Более того, высокая инерционность социума приводит к тому, что аккумулирование рисков происходит в течение длительного периода времени и активное участие в том или ином конфликте может иметь последствия в виде применения кибероружия через несколько лет, а то и десятилетий после его завершения;

• в-третьих, специалистам по системотехнике и теории сложности, вовлеченным в разработку военной политики хорошо известен такой термин, как «ловушка сложности». Очевидно, что синхронное развитие технологий, формирующих следующий технологический уклад, неизбежно ведет не только к росту могущества во всех его компонентах, но и делает страну гораздо более уязвимой для кибератак. Чем шире применяются во всех сферах жизни информационные технологии, чем сложнее электронная инфраструктура, тем ниже ее совокупная надежность. На практике это проявляется в возрастании риска лавины отказов. Она может иметь началом относительно небольшие технические сбои в периферийных секторах информационной инфраструктуры, которые затем распространяются в сети по каскадному принципу. Этот принцип для наглядности часто называется «эффектом домино».

Представляется, что зачастую высокие руководители различных рангов, в отличие от специалистов по информационной безопасности и кибервойнам не вполне отдают себе отчет в роли кибероружия, как великого уравнителя, и практических последствиях действия трех, указанных выше, факторов. Например, в марте 2013 года Глава АНБ и Киберкомандования США Генерал Кейт Александер, отвечая на вопросы в Конгрессе, подчеркнул: «Мы уверены, что наша кибероборона является лучшей в мире».

Приведем лишь несколько примеров, заставляющих усомниться в эффективности американской кибе-

робороны. Как показывает практика, она не только не позволяет отразить массированные кибератаки, но и не может сдержать проникновение в закрытые сети хакерских групп.

В конце апреля американская пресса сообщила, что в январе 2013 года хакеры сумели получить доступ к Национальному реестру плотин – закрытой базе данных, которую ведет Инженерный корпус армии США. База охватывает данные обо всех 79 тыс. плотин на территории Америки, включая 8,1 тыс. наиболее крупных плотин, регулирующих водопотоки и водоснабжение крупнейших городов, объектов национальной безопасности, центров критической инфраструктуры и т.п. База содержит наряду с прочим результаты обследования по каждой плотине с указанием их слабых, уязвимых мест, а также оценку возможного количества погибших в случае прорыва, повреждения и т.п. Самое поразительное, что проникновение на сервер с информацией произошло в январе, а было обнаружено только в конце апреля.

О высокой уязвимости американских сетей к проникновению говорят сами американцы. Выступая в 2013 году, Глава Комитета по разведке Конгресса США Майкл Роджерс, отметил, что китайским кибершпионам удалось похитить научно-техническую документацию по более чем 20 особо секретным военно-технологическим разработкам. Общие же потери от китайского экономического кибершпионажа, связанные с хищением интеллектуальной собственности, он оценил в сумму порядка 150 млрд. долларов за последнее время.

Другим характерным примером является получение доступа хакерами к суперкомпьютеру в Национальной лаборатории имени Лоуренса в Бёркли, одному из самых мощных суперкомпьютеров в списке Топ-500. Помимо прочего этот суперкомпьютер входит в закрытую суперкомпьютерную сеть Министерства энергетики США. Но и это еще не все. Согласно появившимся в последнее

время публикациям, суперкомпьютеры Агентства Национальной Безопасности и Министерства энергетики увязаны в единую общеамериканскую сеть суперкомпьютеров, которая используются для нужд обоих ведомств. Самым интересным в этой истории является даже не то, что хакерам удалось подключиться к одному из самых мощных компьютеров в мире, а соответственно и сети суперкомпьютеров, а то, что взлом не был обнаружен техническими средствами. Двадцатичетырехлетний американский хакер Э. Миллер был арестован в результате дачи показаний другим хакером, пошедшим на сделку со следствием. Причем, арестован при попытке продать аренду на доступ к суперкомпьютеру.

### 1.6. Неопознанная война: эскалация

Кибервойна, в силу трудностей определения инициаторов и инструментария кибератак, времени развертывания кибервооружений и фактического начала боевых действий в киберпространстве, замаскированности во многих случаях ущерба от кибернападений под технические отказы и человеческие ошибки, а также в силу других факторов, без преувеличения может быть названа «неопознанной» войной.

Отдавая себе отчет в принципиально новом характере кибервойн по сравнению с другими видами вооруженных конфликтов, оценивая возможности и угрозы, связанные с этим видом вооружений, американская элита в условиях несомненного лидерства США в сфере информационных технологий приняла несколько лет назад решение о фактическом начале крупномасштабного превентивного кибершпионажа, как первой фазы неопознанной кибервойны.

В марте 2013 года опубликован очередной сводный доклад о глобальных угрозах национальной безопасности США, подготовленный при участии всех 16 разведывательных и контрразведывательных структур США –

Statement for the Record Worldwide Threat Assessment of the US Intelligence Community.

В докладе впервые киберугрозы четко и безоговорочно поставлены на первое место и особо выделены из спектра прочих угроз национальной безопасности США. Причем, киберугрозы в докладе трактуются весьма расширительно. Они включают наряду с атаками на государственные и военные сети, на критически важные объекты и сети, также кибершпионаж, не только в отношении правительственных учреждений, но и американских корпораций. В их состав включаются также хакерские атаки, например, на банки Wall Street и крупнейшие компании электронной коммерции типа Amazon и eBay и т.п. При этом в числе стран, с которыми связываются указанные угрозы, выделяются в первую очередь Китай и Россия.

Впервые в доклад добавлен раздел про угрозу усиления глобального контроля над интернетом со стороны национальных государств и попытку перекраивания глобальной модели управления Сетью, предпринятую Россией, Китаем и Ираном на Всемирной конференции по международной электросвязи (ВКМЭ), проведенной Международным союзом электросвязи в Дубае в декабре 2012 г.

Бывший на тот момент главой АНБ и Киберкомандования США генерал Кейт Александер в марте 2013 года, отвечая на вопросы конгрессменов, особо подчеркнул, что американская доктрина «кибернаступления требует глубокого, постоянного и повсеместного присутствия в сетях противников, чтобы в нужный момент добиться максимального эффекта... Непревзойденный эффект по поражению систем противника будет достигнут за счет американского технологического и эксплуатационного превосходства» в сфере информационных технологий. Действующая в настоящее время Президентская Директива №20, выданная руководителям национальной безопасности и разведки в октябре 2012 года, включает

ряд процедур для обеспечения законности кибератак. Директива указывает, что правительство считает, что кибератаки, известные как «Наступательные кибероперации» (OCEO от англ. Offensive Cyber Effects Operations), происходят все чаще и кибернетическая война может быть очень близко.

Наступательные кибероперации могут предоставить уникальные и нетривиальные возможности улучшения позиций США во всем мире «без или с малым предупреждением» противника или цели, с потенциальным воздействием от незначительных до серьезных повреждений», – говорится в Директиве №20. «Правительство США должно определить потенциальные цели национального значения, где OCEO-операции могут предоставить лучший по сравнению с другими силовыми инструментами государства баланс эффективности и потенциального риска».

Еще в 2008 г. журнал Вооруженных сил США AFJ опубликовал большую статью полковника Чарльза Уильямсона III «Ковровые бомбардировки в киберпространстве». В этой статье полковник Уильямсон пишет: «Америке необходима сеть боевых программ, которые могут направить такое количество трафика на сервера противника, что они больше не смогут функционировать и превратятся в бесполезные куски металла и пластика. Америка нуждается в создании программ, обеспечивающих эффект ковровых бомбардировок киберпространства. Это позволит получить сдерживающий фактор, которого у нас пока нет». Развивая подход «ковровых бомбардировок в киберпространстве», Президентская директива №20 предусматривает, что новые наступательные кибероперации «обеспечат потенциальные эффекты, начиная от едва заметного до причиняющего серьезный ущерб». К числу наступательных кибероперациий в Директиве отнесены «перехват управления, нарушение функционирования, физическое уничтожение хранимой инфор-

мации, компьютеров и их сетей, систем связи, а также управляемых компьютерами объектов физической или виртуальной инфраструктуры». В Директиве предусматривается, что при проведении кибероперациий возможны «очень значительные последствия и разрушения для противника».

Основополагающей информацией, которая с уверенностью позволяет говорить о развертывании Соединенными Штатами сети глобального кибершпионажа, как первой фазы превентивной неопознанной кибервойны, являются сведения о многофункциональных программных продуктах для этих целей.

В 2013 году «Лаборатория Касперского» провела анализ платформы Flame, разработанной ориентировочно в конце 2010 г. и используемой как одна из базисных платформ для создания кибервооружений. Согласно мнению ведущего эксперта «Лаборатории Касперского» Александра Гостева: «Flame – это троянская программа, бэкдор, имеющая также черты, свойственные червям и позволяющие ей распространяться по локальной сети и через съемные носители при получении соответствующего приказа от ее хозяина. По размеру Flame почти в 20 раз больше Stuxnet и включает в себя много различных функций для проведения атак и кибершпионажа. У Flame нет большого сходства с Stuxnet/Duqu.

Flame – это большой набор инструментов, состоящий более чем из 20 модулей. Назначение большинства связано с тестированием уязвимостей, обеспечением проникновения и его маскировкой, поддержанием долговременного доступа в закрытую сеть через уязвимости, снятием разнообразных типов информации и кражей файлов из сети или аппаратного средства, и, наконец, с разрушением и/или перехватом управления физическими объектами и сетями.

По наблюдениям экспертов в сфере кибербезопасности, хозяева Flame искусственно поддерживают коли-

чество зараженных систем на некоем постоянном уровне. Это можно сравнить с последовательной обработкой полей: они заражают несколько десятков, затем проводят анализ данных, взятых на компьютерах жертв, деинсталируют Flame из систем, которые им неинтересны, и оставляют в наиболее важных, после чего начинают новую серию заражений».

Благодаря опубликованному в газете Washington Post от 30.08.2013 г. очередному материалу, основывающемуся на разоблачениях Э. Сноудена, стало известно о наличии обширной программы под кодовым названием GENIE. В рамках этой программы американские компьютерные специалисты осуществляют проникновение в зарубежные сети с тем, чтобы поставить их под негласный контроль США. В бюджетных документах указано, что 652 млн. долларов было потрачено на разработку и использование «секретных имплантатов» (сложных многофункциональных вредоносных программ), при помощи которых ежегодно инфицируются десятки тысяч компьютеров, серверов, маршрутизаторов и т.п. по всему миру.

К концу 2013 года в рамках программы GENIE по всему миру было заражено как минимум 85 тыс. стратегических серверов. Это практически четырехкратное увеличение по сравнению с соответствующим показателем в 2008 г.

Единственным ограничением для АНБ в количестве взятых под контроль аппаратных средств является необходимость использования на сегодняшний день людей-операторов для извлечения информации и осуществления удаленного контроля над взломанными машинами. Даже со штатом 1870 человек GENIE максимально использует только 8448 из 68975 машин с внедренными имплантатами по состоянию на 2011 г. Сейчас АНБ внедряет автоматизированную систему под кодовым названием TURBINE, которая должна позволить в автоматизированном режиме управлять миллионами имплан-

татов для сбора разведывательной информации и осуществления активных атак, вплоть до разрушения и/или перехвата управления над материальными объектами и сетями по всему миру. На расчетную мощность система TURBINE выйдет с началом полноценной эксплуатации сданного в 2013 г. нового огромного датацентра АНБ в штате Юта.

Согласно опубликованным в составе досье Сноудена документам, программное обеспечение для наступательных операций нацелено, прежде всего, не на отдельные компьютеры, а на сети. Оно решает задачу проникновения в сети противника, используя известные и обнаруживаемые самим Агентством уязвимости, которые содержатся не только в программах и технических средствах, разработанных противником, но и в харде и софте, используемых по всему миру известных брендов, большинство из которых производится в США. В настоящее время по разным оценкам от 65 до 75% коммерчески реализуемого на мировых рынках программного обеспечения, производится компаниями под американской юрисдикцией. На корпорации из Соединенных Штатов и их ближайших союзников приходится более 85% производства своего рода «сердца компьютеров» – от планшетников до серверов – процессоров. Как стало известно, подавляющее большинство этих компаний в рамках сотрудничества с американским разведывательным сообществом намерено оставляют в своей продукции те или иные уязвимости, облегчающие несанкционированное проникновение и закладку логических бомб, выводящих в нужный момент компьютеры из строя.

В бюджетных материалах, обнародованных Эдвардом Сноуденом, говорится о 231 наступательной кибероперации. Однако из сопроводительных документов к бюджету становится ясным, что это лишь верхушка айсберга. Из анализа опубликованных документов становится понятным, что это активные операции Киберкомандо-

вания, санкционированные в соответствии с законодательством высшим руководством Соединенных Штатов. В то же время, в соответствии с законодательством для собственно разведывательных операций в большинстве случаев таких санкций не требуется. Между тем, как видно из анализа компьютерных вооружений, одна и та же программная платформа может использоваться как для кибершпионажа, так и для разрушительных кибероперацій. В отличие от материального мира, чтобы перейти грань между шпионажем и войной в киберпространстве, достаточно только активировать один дополнительный модуль программы, а именно боевую программу на уничтожение или перехват управления материальными объектами и сетями.

Подлинным откровением опубликованных в рамках бюджетного доклада документов из досье Э. Сноудена стала активная вовлеченность ЦРУ в наступательные кибероперации. В чем чрезвычайная важность именно этого факта? Она состоит в том, что в отличие от АНБ, ЦРУ имеет право вербовать агентов, а также использовать в качестве агентов сторонние, никак не связанные контрактными отношениями с правительством США, компании и организации. В сочетании с информацией о том, что АНБ в 2013 г. потратило более чем 25 млн. долларов на «дополнительные тайные покупки программ обнаружения уязвимостей в программном обеспечении» у частных производителей хакерского софта на так называемом «сером» рынке, это означает возможность для американского разведывательного сообщества вести частные, формально не связанные с правительством США, кибервойны против любой страны мира.

Эти войны могут вестись тайными компаниями-агентами ЦРУ с использованием финансируемого правительством США, но формально никак с ним не связанного, боевого софта. Т.е. фактически кибервойны сколь угодно высокой степени интенсивности против любого

противника могут вестись частными кибервоенными компаниями вне всякой формальной привязки к США, но при финансировании и всех видах поддержки со стороны Пентагона и американского разведывательного сообщества. Это означает полную бесконтрольность кибервойн. Особая же опасность состоит в том, что эти квазичастные киберармии могут использовать для своих боевых действий уязвимости, обнаруженные государственным разведывательным софтом в рамках вполне законной деятельности.

Совокупность фактов и сведений позволяет с уверенностью утверждать, что кибервойна США против остального мира, и в первую очередь Китая, России и Ирана уже началась. Пока она находится на первой стадии эскалации, а именно в фазе тотального шпионажа, обнаружения множественных уязвимостей и внедрения в них программ-имплантатов многоцелевого применения. Причем, в любой момент начальная фаза неопознанной войны может по сигналу оператора быть переведена в фазу разрушительных в прямом физическом смысле этого слова военных действий.

Нельзя не отметить, что в первую фазу эскалации кибервойн вступили не одни Соединенные Штаты. Другим крупнейшим актором кибершпионажа, а соответственно и разработки многоцелевых вредоносных разведывательных и боевых программ, является Китай.

По оценкам экспертов в сфере информационной безопасности и кибервойн на сегодняшний день лучшие в мире кибервойска имеются в составе Народно-освободительной армии Китая (НОАК). Китайская армия, технически проигрывая американцам в обычном и ядерном вооружениях, уже долгие годы целенаправленно вкладывает деньги именно в информационные технологии. В итоге ей удалось создать на сегодняшний день наиболее эшелонированную и мощную кибероборону страны, одновременно развивая наступательные кибер-

вооружения. Китай сделал ключевым элементом своей военной стратегии «ассиметричное сдерживание» за счет создания киберподразделений.

Развитие китайских кибервойск осуществляется в соответствии с пятнадцатилетней стратегией (2006-2020 гг.) информатизации Китая, включающей вопросы использования киберсредств в целях национальной безопасности. Согласно специальному докладу ASPI (Австралийского института стратегической политики, связанного с австралийским разведывательным сообществом) «Enter the Cyber Dragon», опубликованном в июне 2013 г., структура кибервойск Китая выглядит следующим образом.

Китайские кибервойска сосредоточены во Втором, Третьем и Четвертом департаментах НОАК. Причем, решающую роль в кибервойнах призваны играть Третий департамент, обеспечивающий кибершпионаж и киберконтрразведку и Четвертый департамент, ответственный за атаки на компьютерные сети.

Помимо государственных кибервойск, соответствующие подразделения НОАК тесно взаимодействуют с Red Hacker Alliance. RHA является своего рода неформальной, но управляемой государством сетью хакеров, включающую десятки тысяч хакеров из Китая и других стран, в основном из китайской диаспоры по всему миру.

Помимо всемирно известных успехов китайцев в кибершпионаже, уже зафиксировано несколько случаев использования ими сложных платформ, типа многофункциональных троянов. В частности, они использовались в сентябре 2010 г. против австралийских правительственных сетей, в январе 2012 г. против европейского военного авиакосмического агентства и известной компании по безопасности ASC. Кроме того, многие эксперты связывают с RHA размещение вредоносных имплантатов в сентябре 2012 г. в сетях аэрокосмических предприятий, принадлежащих правительству Индии, а также в марте 2011 г. в сетях RSA – крупнейшей компании-

производителе электронных ключей безопасности. В результате, предположительно, китайским хакерам удалось проникнуть в корпоративные сети крупнейших подрядчиков Пентагона L-3 Communications Lockheed Martin и Northrop Groumman, и изъять стратегически важную научно-техническую и технологическую документацию, касающуюся военных разработок.

Наряду с Соединенными Штатами и Китаем объявили о создании киберподразделений в составе вооруженных сил Израиль, Великобритания, Иран, Германия и т.п.

### 1.7. На пути к кибермиру

Несмотря на развернувшуюся гонку кибервооружений и фактически начало пассивной фазы кибервойны, в долгосрочной перспективе, новая цифровая война не соответствует интересам ни одной из стран мира и может иметь труднопредсказуемые экономические, политические, а возможно и военные последствия для всех. Поэтому крупномасштабной кибервойны необходимо избежать.

Необходим кибермир, который базируется на цифровом равенстве и равном доступе, правах и ответственности всех суверенных государств в отношении всемирной Сети. Именно эти принципы заложены в «Основах государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 г.» Сходных позиций придерживаются и другие участники таких организаций, как БРИКС, ШОС, ЕврАзЭС.

Предотвратить переход из пассивной в активную фазу кибервойны могут только согласованные усилия мирового сообщества, и в первую очередь тесное сотрудничество и взаимодействие стран-лидеров в сфере информационных технологий в целом и информационной безопасности, в частности.

Первым необходимым шагом на этом пути, предусмотренным «Основами государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 г.» является интернационализация управления интернетом под эгидой ООН, обеспечение цифрового равенства и суверенитета всех стран.

Переход от сегодняшнего и де-факто, и де-юре нерегулируемого в международном масштабе интернета к ясной и понятной схеме единого интернета, состоящего из информационных пространств суверенных стран, позволит четко определить не только права, но и ответственность каждой страны за соблюдение безопасности интернета в целом и отдельных его сегментов. На практике это означает, что страна должна нести ответственность за акты киберагрессий, которые осуществляются из или с использованием информационного пространства страны. Естественно, что мера ответственности должна зависеть от степени вовлеченности страны в провоцирование или участие в кибервойне. При этом в соответствующих международных соглашениях, по мнению экспертов, должны быть четко прописаны возможные санкции и условия их применения к стране-нарушителю. В условиях, когда агрессором могут быть не только государственные или частные структуры, но и неформализованные сетевые образования, признание цифрового суверенитета означает государственную ответственность за пресечение деятельности таких организаций и образований, прежде всего, силовыми структурами самой страны, а при необходимости и с согласия страны – с подключением международной помощи.

Изменение структуры управления Интернетом и разработка соответствующих международных соглашений естественно потребуют определенного времени, но все потенциальные участники этого процесса должны понимать, что распространение кибервооружений про-

исходит не по годам, а буквально по месяцам. Соответственно возрастают риски кибервойны и кибертерроризма. Поэтому в данном случае необходима быстрая и согласованная работа всех заинтересованных государств.

Другой очевидной и возможно непопулярной мерой по пресечению неконтролируемого распространения кибервооружений и их частной разработки является ужесточение контроля не только за интернетом, но и другими альтернативными интернету сетями, включая так называемые мэш- и пиринговые сети. Причем, речь идет не только о деанонимизации интернета и пользователей электронных коммуникаций в широком смысле этого слова, но и о расширении предусмотренного национальными законодательствами возможностей государственного контроля за деятельностью компаний и отдельных лиц, задействованных в разработках в сфере информационной безопасности, а также отработке методик тестирования проникновения. Многие полагают, что одновременно должны быть ужесточены национальные законодательства в части хакерской деятельности, наемничества в сфере информационных технологий и т.п.

В современном мире выбор между ничем не ограниченной личной свободой и ответственным, укладывающимся в социально безопасные рамки поведением, перестают быть темой для дискуссий и предметом для спекуляций. Если национальные правительства и международное сообщество хотят предотвратить кибервойны, то необходимо публично и открыто ввести соответствующие нормы в национальные и международное законодательства. Эти нормы должны позволить усилить суверенный технический контроль над поведением, частной и коммерческой деятельностью в интернете с целью обеспечения национальной и международной безопасности в киберпространстве.

Возможно, заслуживает также обсуждения вопрос о создании на базе потенциала ведущих в сфере информа-

ционных технологий стран, прежде всего, Соединенных Штатов, России, Китая, Великобритании, Японии и др. международных сил по раннему обнаружению и пресечению угрозы кибервойн. Создание таких международных сил позволило бы с одной стороны в ускоренном порядке мобилизовать в значительной степени взаимодополняющий потенциал различных стран для пресечения кибервойн, а с другой стороны волей-неволей сделало бы их разработки более открытыми, а соответственно и менее угрожающими для других участников пула, добровольно взявших на себя повышенную ответственность за соблюдение кибермира.

### 1.8. Борясь за кибермир, готовься к новым кибервойнам

При всем стремлении к миру, как показывает российская история, безопасность страны может быть обеспечена только при наличии мощных оборонительных и наступательных кибервооружений.

Согласно сообщениям российских информационных агентств, в российской армии в текущем году сформированы и приступили к выполнению своих задач специальные подразделения, которые занимаются борьбой с киберугрозами. Эти подразделения способны не только отражать кибератаки на нашу страну, но и при необходимости вести наступательные кибероперации. В их состав по информации заместителя министра обороны РФ Павла Попова входит в том числе структура, осуществляющая глубинный анализ хакерского программного обеспечения и декодирование любых телекоммуникационных протоколов.

Чтобы успешно решить задачу форсированного создания кибервойск, у России есть все необходимые предпосылки. Следует помнить, что в отличие от многих других отраслей, российские компании, занимающиеся информационной безопасностью и тестированием уяз-

вимостей, входят в число мировых лидеров и продают свою продукцию на всех континентах. Русские хакеры стали всемирно известным брендом. Подавляющая часть софта, обслуживающего высокочастотный трейдинг и наиболее сложные финансовые операции на всех основных биржевых площадках мира, созданы российскими программистами и разработчиками. Такие примеры можно множить и множить. И относятся они, прежде всего, к созданию софта, требующего высочайшего уровня математической подготовки и знания наиболее сложных языков программирования.

В отличие от многих других направлений науки и техники в России, научные школы по математике, компьютерным наукам и программированию, за последние 20 лет не только не потерпели урона, но и значительно развились, вышли на лидирующие мировые позиции. Такие российские ВУЗы, как МФТИ (ГУ), МГУ им. Ломоносова, МГТУ им. Баумана, НИЯУ МИФИ, Санкт-Петербургский государственный университет, Ульяновский государственный технический университет, Казанский государственный университет и т.п. являются признанными центрами подготовки алгоритмистов, разработчиков и программистов мирового уровня. Из года в год российские команды программистов выигрывают мировые первенства по программированию среди университетов. Работы отечественных алгоритмистов постоянно цитируются в ведущих мировых журналах. Российские математики постоянно входят в число соискателей премии Филдса.

Кстати, интересно, что в разгар скандала со Сноуденом, одна из ведущих американских организаций по изучению общественного мнения Pew Internet & American Life Project провела опрос, кто в наибольшей степени угрожает конфиденциальности личной и корпоративной информации. Итоги оказались таковы. 4% – силовые структуры, 5% – правительства, 11% – другие бизнес-структуры, 28% – рекламодатели и интернет-гиганты

и 33% – хакеры. При этом, по мнению едва ли не самого популярного издания об интернет-технологиях в Америке, журнала Wired, несомненную пальму первенства среди хакеров держат русские хакеры.

Иными словами, необходимый научный, технологический, программный и кадровый задел для ускоренного формирования грозных кибервойск в России имеется. Вопрос состоит в том, каким образом привлечь в кибервойска, а также компании, которые будут включены в программу национальной кибербезопасности, наиболее квалифицированных, талантливых разработчиков, программистов, тестировщиков систем информационной безопасности и т.п. Здесь важно не повторить ситуацию, которая имеет место сегодня в отраслях военно-промышленного комплекса, где из-за низких зарплат качественные кадры не задерживаются и уходят в различного рода коммерческие разработки, зачастую имеющие иностранных инвесторов.

В мире сложилось три основных направления рекрутирования лучших программистских кадров в государственные программы, связанные с кибервойнами. Наиболее известен опыт Соединенных Штатов. Он базируется на своего рода трех китах. Во-первых, ежегодно DARPA проводит множество конкурсов, мероприятий, круглых столов для программистского сообщества, где идет отбор наиболее талантливых, подходящих для задач Пентагона и разведки, молодых людей. Во-вторых, практически все ведущие IT компании Соединенных Штатов связаны с военно-разведывательным сообществом и программисты соответствующих подразделений частных компаний, многие из которых даже не являются подрядчиками Пентагона в своей повседневной деятельности, заняты разработкой программ в сфере кибервооружения. В-третьих, АНБ непосредственно взаимодействует с ведущими американскими университетами, а также в обязательном порядке присутствует на всех

общенациональных хакерских конференциях и черпает кадры оттуда.

Китайский подход базируется на строгой государственной дисциплине и руководящей роли КПК в решении ключевых кадровых вопросов китайских вооруженных сил. По сути, для китайского программиста или разработчика работа над кибервооружениями является проявлением долга, ключевой характеристики поведенческих паттернов китайской цивилизационной традиции.

Что же касается Европы, то здесь сделан упор на поддержку в большинстве стран ЕС движения так называемых «этичных хакеров», т.е. разработчиков и программистов, которые не занимаются противоправными действиями, а специализируются на сотрудничестве с коммерческим сектором в части обнаружения информационных уязвимостей и силовыми структурами, в части создания кибервооружений.

Представляется, что в России можно в той или иной мере использовать элементы и американского, и европейского, и китайского опыта. При этом вполне очевидно, что главным должно стать понимание со стороны государства, что в сфере цифровых войн именно человеческий фактор является определяющим при разработке и использовании оборонительных и наступательных кибервооружений.

В этой связи всячески следует развивать инициативу создания научных рот, прямую государственную поддержку стартапов, связанных с разработкой программ в сфере информационной безопасности, тестирования проникновений и т.п. Необходимо, конечно же, провести тщательную инвентаризацию имеющихся уже сегодня в России разработок, которые при определенном апгрейде могли бы стать мощными кибервооружениями. Такая инвентаризация необходима потому, что в силу серьезных недостатков и коррупции при проведении

государственных тендеров, подавляющее большинство маленьких компаний и талантливых программистов, по сути, отсечено от этой задачи и не востребовано силовыми структурами.

Понятно, что государству, как это не парадоксально, надо повернуться лицом к хакерам.

Наряду с возможным ужесточением уголовных наказаний за компьютерные преступления, государство должно предоставить возможность хакерам применить свои способности и навыки в общественно-полезной деятельности и, прежде всего, в разработке кибероборонительных и кибернаступательных вооружений, тестировании сетей на предмет злонамеренного проникновения. Возможно, заслуживает обсуждения идея о создании своего рода «хакерских штрафбатов», где разработчики, программисты и тестировщики, имевшие те или иные правонарушения в России или за рубежом, могли бы делом искупить свою вину.

И, конечно же, следует помнить, что едва ли не самые востребованные профессии в мире на сегодняшний день – это разработчики, программисты, специалисты по Большим Данным и т.п. Их зарплаты стремительно растут и в нашей стране и за рубежом. По независимым оценкам американских и российских экспертов, до 20 тыс. российских программистов сейчас трудятся в США. Поэтому, памятуя, что в кибервойсках ключевое звено – это разработчик, программист, патриотичный хакер, на их оплату и социальный пакет не надо жалеть денег, также как не экономили в свое время деньги на зарплату и бытовые условиях ученых и инженеров при разработке советского атомного проекта.

Оборонительные и наступательные кибервооружения являются одной из немногих сфер, где Россия высококонкурентна на мировой арене и может в короткие сроки создать программные средства, способные не только заметно повысить уровень безопасности соб-

ственных критически важных сетей и объектов, но и за счет наступательных возможностей сдержать любого потенциального киберагрессора.

Кибероружие для России – это реальный и серьезный шанс ассиметричного ответа на гонку высокоточных вооружений, развязанную в мире и один из ключевых элементов достаточной национальной безопасности.

### 1.9. Кибероружие сдерживания

На сегодняшнем уровне развития информационных технологий, включая средства киберзащиты и цифрового нападения, такие страны как Россия и Китай могут успешно противодействовать планам развязывания крупномасштабной активной кибервойны со стороны таких потенциальных агрессоров, как США и их союзники, в первую очередь Великобритания, Франция, Израиль.

Правящая элита США отдает отчет в сегодняшней уязвимости своей страны перед угрозой сколько-нибудь масштабной цифровой войны. Пожалуй, это является главным фактором, сдерживающим переход пассивной фазы цифровой войны в активную, связанную с применением наступательных, разрушительных кибервооружений.

В этих условиях часть американской элиты делает ставку на конвертацию сложившегося превосходства Соединенных Штатов в сфере информационных и других технологий седьмого технологического уклада в создание кибервооружений нового поколения.

Эти кибервооружения и решения в сфере информационной безопасности США призваны преодолеть нынешний ассиметричный характер кибервойн и сделать страны – потенциальных противников США беззащитными перед американской кибермощью.

Вопросы новейших разработок в сфере кибервооружений являются, естественно, тайной за семью печатя-

ми американского военно-промышленного комплекса. Однако внимательный анализ тенденций развития информационных технологий и опубликованных в СМИ государственных документов США позволяют сделать ряд выводов о мерах, предпринимаемых по достижению неоспоримого кибердоминирования.

Еще в 70-90-е годы прошлого века в ходе исследований, направленных на создание искусственного интеллекта, проводимых в СССР, США и Японии, была создана математическая база и алгоритмическая основа для так называемых самосовершенствующихся программ, заложены основы генетического и эволюционного программирования. Была создана математико-алгоритмическая база для разработки программ, которые могли бы самообучаться в зависимости от поступающих из внешней среды сигналов и соответственно трансформироваться в сторону все более эффективного выполнения своих функций. Позднее одно из ответвлений этого направления получило название «машинное обучение». В прошлом веке для практической программной реализации этого подхода не было аппаратных возможностей. Что называется, не хватало вычислительных мощностей.

В середине прошлого десятилетия критический порог был перейден, и машинное обучение, как основа для решения широкого круга задач, стало активно развиваться и реализовываться на базе суперкомпьютеров. Наиболее известной демонстрацией возможностей машинного обучения и эволюционного программирования стал знаменитый Watson. В 2011 г. суперкомпьютер IBM победил экспертов, чемпионов американской версии «Своя игра». В настоящее время Watson активно используется для диагностических и прогнозных целей в здравоохранении, страховании и сфере национальной безопасности США.

Некоторые эксперты полагают, что огромные сети имплантатов, выполняющие шпионские функции, буду-

чи подсоединенными к подобной экспертной системе и способные к машинному обучению, могут стать боевыми самообучающимися киберпрограммами. Образно говоря, передавая информацию в экспертную систему, они получают от нее команды, позволяющие этим программам, как бы самим достраиваться, адаптируясь к конкретным параметрам зараженных компьютеров и сетей. По мнению специалистов, скорее всего такие программы будут применяться не столько для разрушения, сколько для незаметного перехвата управления критически важными объектами и сетями потенциального противника.

Чтобы от машинообучаемых перейти к полноценным самоизменяющимся и самоорганизующимся программам, необходимо задействовать даже не сегодняшние суперкомпьютеры, а суперкомпьютеры следующего поколения с еще большей степенью быстродействия. В этом случае однажды разработанная многомодульная программа-имплантат, в зависимости от конкретных условий и стоящих задач, сможет достраивать свои модули, адаптироваться и предупреждать действия по ее обнаружению или уничтожению. Более того, недавно в специальных научных журналах а также в Wall Street Journal была опубликована информация о том, что такие самоорганизующиеся программы-имплантаты смогут выводить из строя объекты никак не подключенные к интернету, а функционирующие в закрытых сетях. Причем, в этих публикациях утверждается, что найден способ проникновения программ-имплантатов этого класса даже в отключенные сложные компьютеризованные объекты, линии, энергосистемы и т.п. При переходе этих объектов в активный режим программы реализуют свои задачи разрушения, либо перехвата управления. Эти программы и имплантаты для проникновения используют акустическую и оптическую среды.

На сегодняшний день самым мощным суперкомпьютером в мире является китайский Тяньэх-2. Большая часть компонентов этой системы была разработана в Китае. Однако надо иметь в виду, что подавляющая часть наиболее мощных суперкомпьютеров принадлежит Соединенным Штатам и в отличие от Китая, соединена в единую распределенную сеть под эгидой АНБ и Министерства энергетики США. Но главное даже не это. Чтобы осуществить следующий скачок в скорости вычислений, необходимо переходить уже на уровень нанотехнологий. Летом этого года ведущие американские производители процессоров для суперкомпьютеров объявили о том, что к 2015 г. они смогут начать производство микропроцессоров, пока еще на основе кремния, но уже со значительным использованием нанотехнологий. Приближаются к подобному решению и японцы.

Китай, наращивая мощность суперкомпьютеров, пока, судя по оценкам экспертов, не имеет необходимой технологической базы для производства процессоров с использованием нанотехнологий. Ключевым вопросом в обеспечении превентивного доминирования в киберпространстве является способность декодировать защищенную специальными шифрами информацию, передаваемую как в интернете, так и в закрытых сетях государств – потенциальных противников. Согласно документу АНБ, обнародованному Сноуденом, «в будущем сверхдержавы будут появляться и приходить в упадок в зависимости от того, насколько сильными будут их криптоаналитические программы. Это цена, которую должны заплатить США, чтобы удержать неограниченный доступ к использованию киберпространства».

Уже давно Агентство на постоянной основе работает с IT-компаниями по встраиванию в их продукты закладок в интересах спецслужб США, а также ведет работу по целенаправленному ослаблению международных алгоритмов защиты данных. Поскольку именно американские

компании являются поставщиками подавляющей части используемых в мире процессоров, маршрутизаторов, серверной инфраструктуры и т.п., становится понятным, что на сегодняшний день в подавляющем большинстве стран, в том числе в России, даже закрытые компьютерные сети весьма уязвимы для проникновения, а используемые системы шифрования в значительной части являются прозрачными для американских спецслужб.

Хотя в опубликованных Э. Сноуденом документах и имеется информация, что службы США и Великобритании могут взломать любой шифр, используемый в интернете, это, по мнению подавляющего большинства специалистов, не является корректным утверждением. Более того, тесные контакты АНБ с производителями харда, в который они стремятся встроить соответствующие закладки, лишний раз подтверждает это мнение.

Проблема состоит в том, что мощностей нынешних суперкомпьютеров, даже в виде распределенной сети не хватает для уверенного взлома наиболее изощренных шифров, используемых в правительственной связи и коммуникациях спецслужб информационно продвинутых стран мира, включая Россию.

Однако, ситуация изменится с появлением на свет квантового компьютера. Собственно, одна из сверхзадач квантовых компьютеров как раз и состоит во взломе любого шифра, созданного на традиционных, доквантовых компьютерах. На сегодняшний день математически доказана справедливость подобной постановки задачи. Против квантового компьютера все доквантовые системы шифрования бессильны.

Хотя самих квантовых компьютеров пока нет, уже созданы многочисленные алгоритмы для них, а буквально в этом году по заданию IARPA разработан язык программирования Quipper. Работы по практическому созданию квантового компьютера ведутся в Соединен-

ных Штатах в рамках проекта Quantum Computer Science (QCS) IARPA.

Немаловажно понимать принципиальное отличие IARPA от DARPA. Помимо прочего оно состоит в том, что проекты DARPA относятся к сфере двойных технологий, предусматривают оповещение о разработчиках тех или иных проектов и их результатах. Вся информация по проектам IARPA, кроме их наименования и условий, является секретной.

В 2013 году совершен прорыв и в аппаратном компоненте квантового компьютера. Компания Google, совместно с NASA запустила в эксплуатацию в рамках сети суперкомпьютеров квантовый модуль D-Wave Two. Это еще не полноценный квантовый компьютер, но при выполнении сложных вычислений с более чем 500 параметрами его мощность в тысячи раз превосходит производительность лучших суперкомпьютеров из списка Топ-500.

По осторожным высказываниям Google в ближайшие два-три года они собираются создать сеть, включающую несколько подобных модулей, работающих вместе с обычными суперкомпьютерами, которые по своим совокупным возможностям вплотную приблизится или будет равна полноценному квантовому компьютеру.

Когда это произойдет, то помимо прочего, любой шифрованный трафик окажется полностью открытым и свободно читаемым, а саморазвивающиеся программы позволят в этих условиях беспрепятственно ставить под контроль любые объекты и сети потенциальных противников. Тем самым будет достигнуто фактически неограниченное доминирование в киберпространстве. Электронные сети противника в любой момент могут быть разрушены или поставлены под полный контроль кибреагрессора, обладающего описанными выше программными и аппаратными средствами. Тем самым кибервойна закончится, не успев начаться.

Но и это еще не все. Летом 2013 года, несмотря на разоблачения АНБ и американского разведывательного сообщества, в Соединенных Штатах состоялся ряд совещаний по повышению уровня кибернетической национальной безопасности. Впервые за всю историю всерьез обсуждался вопрос создания общеамериканской электронной стены – фаервола. В этом случае весь интернет-трафик, входящий из-за рубежа подвергался бы глубокой инспекции пакетов, и любые подозрительные пакеты блокировались так же, как великий китайский фаервол блокирует нежелательные сайты. Участники обсуждения пришли к точке зрения, что это был бы лучший способ, но решили, что подобный подход будет невозможно реализовать на практике из-за американских реалий. Однако приведенные в докладе опросов американского общественного мнения и руководителей американских корпораций, а также подогреваемые СМИ истерия по поводу китайских и русских хакеров, могут создать питательную почву для практических шагов в этом направлении.

Согласно анализу, проведенному по открытым источникам экспертами Центра военно-промышленной политики Института США и Канады, американцы взяли курс на развертывание автономных спутниковых группировок, обеспечивающих защищенные электронные коммуникации и развертывание системы ПРО, нацеленной не столько против террористов, сколько против потенциальных американских конкурентов в космосе.

Спутниковые группировки призваны создать параллельную современному интернету защищенную систему электронных коммуникаций, завязанную на выведенную в космос суперкомпьютерную систему с квантовыми составляющими. Другая часть орбитальных спутниковых группировок призвана вывести из строя телекоммуникационные и электронные сети противников, способные функционировать в случае принудительного отключе-

ния обычного интернета. Наконец, система ПРО должны блокировать запуски ракет противника, нацеленных на орбитальные группировки и космическую платформу с центральным квантовым или квантовоподобным суперкомпьютером.

В этой связи возникает проблема разработки кибероружия сдерживания.

Недавно президент РАН Владимир Фортов сообщил, что «Работы, проведенные под руководством академика Геннадия Месяца, позволили создать генераторы, испускающие очень короткие и мощные импульсы. Их пиковая мощность достигает миллиардов ватт, что сопоставимо с мощностью энергоблока АЭС. Это более чем в 10 раз превышает зарубежные достижения». Указанный генератор может быть размещен на носителе, выведенном в космос на низкую орбиту или в мобильном варианте на земле, либо даже на подводной лодке вблизи берегов потенциального противника. Использование такого генератора позволяет получить направленный мощнейший электромагнитный импульс, способный полностью вывести из строя любую электронику, независимо от ее защиты на весьма значительных площадях. Более того, имеются расчеты, показывающие возможность вывести из строя при помощи системы указанных генераторов энергосистемы, телекоммуникации, электронные сети, включая интернет, в самых разных странах мира, в том числе в США.

Какие выводы можно сделать из вышеприведенного анализа и складывающейся внешнеполитической ситуации?

• Грубейшее вмешательство США и их союзников в украинский кризис, события вокруг Сирии показывают, что у геополитических конкурентов России нет никаких моральных ограничений в реализации любых агрессивных планов и провокаций самого чудовищного типа (с уничтожением мирного населения химоружием для

обоснования начала войны против суверенной страны в обход международного права). Поэтому скорейшее полноценное развертывание российских кибервойск в структуре вооруженных сил и разработка кибероружия сдерживания являются в современный период не менее важной государственной задачей, чем поддержание в боевой готовности ядерного потенциала.

• Информационный взрыв, связанный с опубликованием в открытой печати сверхсекретных материалов Сноудена о ведущейся кибервойне армией и спецслужбами США против России и других стран, и применяемых при этом технологиях, ставит задачу внесения серьезных корректив в государственную политику обеспечения кибербезопасности. Речь идет о пересмотре стратегических документов, увеличении бюджетного финансирования, ускоренной и качественной подготовке кадров, способных вести противоборство в киберпространстве.

• Сдерживание кибервойн XXI века невозможно без развития фундаментальных научных исследований самой различной направленности. По всей видимости, процесс реализации фундаментальных научных разработок как и прежде будет ориентирован в первую очередь на военные цели для достижения превосходства над потенциальным противником. Причем скорость реализации фундаментальных открытий в прикладных военных целях в условиях идущей информационной революции будет неизменно возрастать. Поэтому государственные бюджетные вложения в фундаментальные исследования должны быть качественно увеличены.

# Глава 2
# ИНФОРМАЦИОННЫЕ ВОЙНЫ 3.0

В отечественной военной традиции широко используется известный афоризм классика военной мысли Карла Клаузевица: «Война есть продолжение государственной политики иными средствами». Между тем, для информационных войн гораздо больше подходит другое его высказывание: «Война – это акт насилия, имеющий целью заставить противника выполнить нашу волю».

В этой связи характерно, что в концептуальном документе Пентагона – «Основополагающей концепции ведения объединенных операций – 2020» (сентябрь 2012 года) указано: «Война остается столкновением между враждующими, независимыми и непримиримыми волями, каждая из которых стремится достичь доминирования над другой посредством насилия. Противники будут продолжать свои стремления найти и использовать уязвимости США. Даже если конфликт будет вестись с использованием самых современных технологий, ведение военных операций остается по большому счету делом человека».

Это совершенно не случайно, поскольку агрессивная информационная составляющая стала неотъемлемым элементом военной доктрины Запада, начиная со времен Первой мировой войны.

К настоящему времени можно выделить два поколения информационных вооружений. Первое поколение связано с использованием в ходе военных действий или подготовки к ним пропаганды, как вида информационных вооружений. На этом этапе объектом интенсивного информационного воздействия были массы военнослу-

жащих и населения стран-противников. Начало второго этапа датируется 70-80 годами прошлого века. Если на первом этапе в военном деле использовались методы пропаганды и рекламы, то второй этап связан с использованием в качестве вооружений методов и технологий маркетинга. Для информационных войн 2.0 характерны самые разнообразные каналы воздействия на сознание, способы подачи информации, включая комбинирование текстовых, визуальных и звуковых сообщений, переход к интерактивным методам. Главной же чертой является ориентация не на массы, а на четко выделяемые группы военнослужащих и населения стран противника, обладающих определенными характеристиками.

В настоящее время мы являемся свидетелями формирования третьего поколения информационных вооружений, используемых в информационных войнах 3.0. С предыдущими поколениями их роднит нацеленность на перепрограммирование сознания в нужном для агрессора направлении, парализацию и подчинение воли руководителей, военнослужащих и населения стран-противников. Принципиально новым для информационных войн 3.0 является то, что в решающей степени они направлены на разрушение активных групповых субъектов, противодействующих агрессору, и напротив, конструирование новых групповых субъектов, являющихся проводниками интересов и исполнителями воли нападающей стороны внутри вооруженных сил, элиты и социума государства – жертвы агрессии.

### 2.1. Взлет и падение «мягкой силы»

Дж. Най без сомнения относится к числу наиболее влиятельных представителей американского политического истеблишмента. Его книги издаются и переиздаются на многих языках мира. Его воззрения оказывают прямое и непосредственное влияние на государственную политику США времен президента Б. Обамы.

За рубежом, в том числе и в России Дж. Най относится к числу наиболее известных американских политологов. Соответственно, складывается впечатление, что именно его концепция на сегодняшний день представляет собой последнее слово в американской внешнеполитической мысли. Однако на практике дело обстоит несколько сложнее. Чтобы понять ситуацию, сложившуюся вокруг концепции «мягкой силы», необходимо внимательнее присмотреться к истокам ее формирования.

Дж. Най является не только крупнейшим исследователем и знаменитым профессором, но и был длительные годы практикующим политиком, занимавшим ключевые посты в разведывательном, военном и дипломатическом секторах американского правительства.

Ключевым моментом для формирования подхода Дж. Ная стала его теснейшая связь с Дэвидом Рокфеллером. Перед своей государственной карьерой он был одним из основных функционеров знаменитой в свое время Трехсторонней комиссии. Трехсторонняя комиссия была организована влиятельнейшей финансово-энергетической группой американской элиты – кланом Рокфеллеров. Главной целью комиссии, созданной в начале 70-х годов, была координация усилий американской, европейской и японской элит в деле построения нового мирового порядка и противодействия СССР. В своих мемуарах Дэвид Рокфеллер писал: «Некоторые даже верят в то, что мы (семья Рокфеллеров) являемся частью секретной политической группы, работающей против жизненных интересов Соединённых Штатов, и характеризуют мою семью и меня как «интернационалистов», вступивших в сговор с другими группами по всему миру для построения более интегрированной глобальной политической и экономической структуры – единого мира, если угодно. Если обвинение заключается в этом, то я признаю себя виновным, и я этим горжусь».

Собственно Трехсторонняя комиссия и стала одним из инструментов формирования тех наднациональных

элитных сетей, которые вместе с государствами являются основными акторами сегодняшней мировой политики и экономики.

Трехсторонняя комиссия, по сути, стала рабочим органом глобалистского направления в мировой элите. Работы Дж. Ная в этом смысле представляют собой идеологическое обоснование не национально ориентированной американской внешней политики, а базу для глобальной геополитики, осуществляемой в интересах наднациональных элит высшим государственным аппаратом Соединенных Штатов. Нетрудно заметить, что между национальными интересами государства США и интересами наднациональных элит имеются серьезные различия.

Необходимо отметить, что в американском политическом истеблишменте интересы глобалистов наиболее полно представлены так называемым кланом Клинтонитов. Он помимо собственно семьи Клинтонов включает в себя обширную и разветвленную группу политиков, администраторов, военных, финансистов и т.п., чье выдвижение опять же прямо или косвенно связано все с той же Трехсторонней комиссией. Дж. Най является одним из представителей этого клана.

Впервые концепция «мягкой силы», разработанная в недрах Трехсторонней комиссии была представлена в 1990 году. В книге «Bound to Lead: The Changing Nature of American Power» («Призвание к лидерству: меняющаяся природа американской силы») Дж. Най разделяет мощь государства на две составляющих: так называемую «жесткую силу» (hard power) и «мягкую силу» (soft power). Под «жесткой силой» подразумевается совокупная политическая, экономическая и финансовая мощь, а «мягкая сила» в основном характеризуется культурой, ценностями и политической идеологией.

В книге «Мягкая сила. Средства достижения успеха в мировой политике», вышедшей в свет в 2004 году, понимание «мягкой силы» раскрывается следующим об-

разом: «Если Наполеон, распространявший идеи Французской революции, был обязан полагаться на штыки, то ныне, в случае с Америкой, жители Мюнхена, равно как и москвичи, сами стремятся к результатам, достигаемым лидером прогресса». И далее автор подчеркивает: «Когда ты можешь побудить других возжелать того же, чего хочешь сам, тебе дешевле обходятся кнуты и пряники, необходимые, чтобы двинуть людей в нужном направлении. Соблазн всегда эффективнее принуждения, а такие ценности, как демократия, права человека и индивидуальные возможности, глубоко соблазнительны».

На постах директора национальной разведки и заместителя министра обороны Дж. Най пытался на практике реализовывать свою концепцию. Однако по оценке подавляющего большинства политиков, практиков, а также представителей военной и разведывательной элиты, не слишком преуспел в замене «жесткой силы» на «мягкую».

Главные аргументы критиков сводились к следующим. Методы «мягкой силы» включают в себя в первую очередь культурную политику, активные мероприятия по продвижению ценностей и идеалов так называемого свободного мира. Иными словами, идеологии. Однако, как показала вся предыдущая история и подтвердили годы, когда Дж. Най пытался на практике реализовать свою концепцию, применяя «мягкую силу» никогда нельзя планировать временные рамки достижения результата. Весьма условен, если вообще возможен, учет рисков и вероятности успеха подобных мероприятий. И, наконец, практически затруднен объективный анализ – произошли ли перемены в результате осуществления политики «мягкой силы», либо под воздействием каких-либо других факторов.

В этом плане концепция «мягкой силы» гораздо в большей степени обсуждалась в академических кругах и использовалась для ведения информационного про-

тивоборства, нежели была принята на вооружение, как базисная концепция реальной внешней политики США.

В итоге Дж. Най сменил государственную службу на преподавательскую работу. Казалось бы, концепция «мягкой силы» уйдет в прошлое вместе с ним. Однако жизнь распорядилась по-иному. Если быть более точным, то не жизнь, а Хиллари Клинтон и группа ее советников.

Готовясь в 2006 году к избирательной кампании 2008 года на пост президента, она инициировала создание в Центре стратегических и международных исследований (ЦСМИ) (Center for Strategic and International Studies, CSIS) комиссии по интеллектуальной власти – «Bipartisan Commission on Smart Power», которую возглавили профессор Дж. Най и Р. Эрмитэдж, бывший высокопоставленный сотрудник администрации Б. Клинтона. Итогом работы комиссии стал доклад «Более умная, более безопасная Америка». В докладе впервые был использован термин «умная власть» (власть интеллекта, smart power). Публично его впервые озвучила Хиллари Клинтон в своей речи в Сенате непосредственно перед утверждением ее кандидатуры на должность госсекретаря. В своем выступлении она сказала: «Мы должны использовать так называемую «власть интеллекта», полный набор имеющихся у нас средств – дипломатических, экономических, военных, политических, правовых и культурных, – выбирая нужное средство или сочетание средств в каждой конкретной ситуации».

Возникает вопрос, почему столь опытный и эффективный политик, как Хиллари Клинтон для своего дебюта на посту госсекретаря, который достался ей в результате соглашения с группой, которая смогла продвинуть на пост президента мало кому известного Б. Обаму, использовала, казалось бы, скомпрометировавшую себя концепцию.

Как это ни удивительно, данный вопрос не получил своего освещения не в американских, не тем более в рос-

сийских профессиональных публикациях. В итоге возникает странное впечатление, что возможно наиболее эффективный политик Америки при своем дебюте на посту Госсекретаря говорила совершенно избитые вещи о том, что внешняя политика должна использовать все рычаги воздействия, а культурная политика является одним из важных инструментов внешнеполитической активности. Собственно последний тезис не являлся никакой новинкой и был хорошо известен до «мягкой силы» как минимум с 30-х годов прошлого века. Тем не менее, выбор был далеко не случаен по целому ряду обстоятельств:

• во-первых, еще в книге 1990 года Дж. Най сделал чрезвычайно важный и принципиальный вывод о «мягкой силе». Он определили ее, как «способность добиваться желаемого на основе добровольного участия союзников, а не с помощью принуждения или выплат. Если Соединённые Штаты замедлят мобилизацию своих ресурсов ради международного лидерства, полиархия может возникнуть достаточно быстро и оказать свое негативное воздействие. Управление взаимозависимостью становится главным побудительным мотивом приложения американских ресурсов, и оно должно быть главным элементом новой стратегии». Х. Клинтон уточнила это следующим образом: «Америка должна научиться делать то, что другие хотят, но не могут. И делать это коллективно». Т.е. впервые в американской внешнеполитической практике глобалистские интересы и глобалистский образ действия вышли на первый план по сравнению с национальными интересами Америки;

• во-вторых, «умная власть» предусматривает использование всего арсенала инструментов, имеющихся в распоряжении Америки и ее союзников, обслуживающих интересы наднациональной мировой элиты. Соответственно, эти инструменты могут и должны использоваться не только поодиночке, но и совместно, подкрепляя друг друга;

• наконец, в-третьих, внимательный анализ доклада, подготовленного Центром стратегических и международных исследований, позволяет прийти к выводу о том, что в качестве союзников, участвующих в глобалистских акциях, рассматриваются отнюдь не только государства. В докладе указано, что на смену пирамиде с жесткой иерархической структурой приходит «паутина разновеликих, разнокачественных и разнообразных действующих лиц, находящихся во взаимодействии». При этом становится понятным, что «в число таких акторов могут включаться не только различные государства, или их образования, но и общественные движения, политические группы, активистские группы внутри стран, на которые направлены действия». В марксистской литературе прошлого века, после гражданской войны в Испании, такие группы называли «пятой колонной».

С учетом отмеченных выше обстоятельств, провозглашенная Х. Клинтон стратегия являлась принципиально новой, поскольку фактически представляла собой механизм использования ресурсов США, других стран, а также групп «пятой колонны» в интересах наднациональной элиты.

На время госсекретарства Х. Клинтон приходится явно неудачное окончательное завершение вывода войск из Ирака, трудности с выводом войск из Афганистана, в целом негативные для Соединенных Штатов события «арабской весны», неуклюжее и бессмысленное вмешательство бывшего посла США М. Макфола во внутренние дела России во время парламентских выборов 2011 года и т.п. Сменивший Х. Клинтон на посту Госсекретаря Дж. Керри также является выходцем из недр Трехсторонней комиссии. Более того, в период его предвыборной кампании в 2004 году именно Дж. Най рассматривался как основной кандидат на пост Госсекретаря и был его правой рукой в избирательной кампании. Поэтому, при всем различии стиля руководства с Х. Клинтон, Дж. Керри в ко-

нечном счете пытается реализовывать все ту же концепцию «умной силы» в интересах наднациональных элит.

Возникает вопрос, почему же при очевидных неудачах практической реализации концепции «умной силы», она продолжает использоваться в качестве идейной основы внешней политики США.

Представляется, что ответ заключен в следующем обстоятельстве. Жители любой страны, что Америки, что России, что Китая искренне полагают, что их страна является главным пунктом повестки дня для всех стран мира. Однако в те или иные периоды времени это оказывается не вполне так. Дж. Керри, если судить по основным публикациям «думающих танков», отражающих позиции тех или иных политэкономических элитных групп – это в значительной мере, что называется «технический» госсекретарь. Вместе с Б. Обамой он призван до 2016 года реализовать две главных глобалистских задачи. Речь идет о создании Трансатлантического торгового и инвестиционного партнерства и Транстихоокеанского торгового партнерства. В Трансатлантическое партнерство должны войти США, Мексика, Канада, т.е. страны НАФТА и страны ЕС. А в Транстихоокеанское партнерство, как предполагается, войдут все те же страны НАФТА, ряд стран Латинской Америки, Япония, Южная Корея, Австралия, Новая Зеландия и еще ряд стран Южной и Юго-восточной Азии.

Смысл этих партнерств достаточно прозрачен. Они призваны унифицировать различного рода торговые правила, технические и иные регламенты и другие нормативные документы, связанные с ведением бизнеса, использованием информации и т.п. Вместе с отсутствием каких-либо таможенных и иных экономических барьеров, формирование этих партнерств образует своего рода огромную единую технологическую, производственную, финансово-экономическую и в значительной степени политическую зону.

Для реализации именно этой задачи, в которой максимально заинтересованы все крупнейшие корпорации, доктрина «умной силы» с акцентом на коллективные действия, использование активистских групп и наличие единой неолиберальной идеологии, подходит как никакая другая.

Есть основания полагать, что на все другие международные события последнего периода, включая события на Ближнем Востоке, на Украине, в Южной Азии и т.п., верхушка мировой наднациональной элиты смотрит именно с позиции их использования для снятия препятствий и ускорения процессов подписания соответствующих соглашений, которые намечены на 2015 год. А соответственно американское внешнеполитическое ведомство реализует не столько национальные интересы, сколько обслуживает глобалистскую иерархо-сетевую структуру, в основе которой находится кластер крупнейших финансовых институтов и транснациональных корпораций.

При этом если еще 20-25 лет назад внешняя активность США могла распространяться на целый ряд регионов, где они осуществляли наступательные, по большей части эффективные действия, то в последние 10-15 лет картина коренным образом изменилась. Страна либо пытается ликвидировать последствия внешнеполитических неудач, типа авантюр в Ираке и Афганистане, либо, как уже отмечалось выше, обслуживает интересы наднациональных структур. Такое положение в немалой степени усугубилось принятием на вооружение доктрин «мягкой», а затем «умной» силы Дж. Ная.

Каждая доктрина имеет обязательно ключевой инструмент реализации. А этот инструмент в свою очередь предполагает вполне практическую, понятную форму своего действия.

В последние 10 лет сошлось так, что доктрина «мягкой силы» вызвала к жизни целый ряд инструментов и

форм, которые будучи крайне многообещающими на первый взгляд, оказались совершенно провальными на практике.

Прежде чем детальнее рассмотреть, о чем конкретно идет речь, надо отметить, что такое положение является ярким свидетельством уменьшения калибра ключевых фигур на американской политической сцене. Оно же демонстрирует и снижение уровня проработки важнейших внешнеполитических решений.

Сегодня сложилась достаточно парадоксальная ситуация, когда «фабрики мысли» продолжают повышать уровень своей работы, корпорации и отдельные государственные и надгосударственные структуры, в первую очередь, в разведывательном сообществе используют все более изощренные инструменты, а на высшем государственном уровне делаются удивительные по своей нелепости просчеты.

Инструментом реализации политики «мягкой», а затем «умной» силы стала концепция и инструментарий так называемого «управляемого хаоса», разработанные Стивеном Манном. Стивен Манн собственно не скрывал, что его концепция «управляемого хаоса» есть механизм практической реализации построений Дж. Ная. В одной из своих ключевых работ он прямо писал: «Конфликтная энергия заложена в основы человеческих свойств с того момента, когда индивидуум стал базовым блоком глобальных структур. Конфликтная энергия отражает цели, ощущения и ценности индивидуального актора – в сумме, идеологическое обеспечение каждого из нас запрограммировано. Изменение энергии конфликта людей уменьшит или направит их по пути, желательному для наших целей национальной безопасности, поэтому нам нужно изменить программное обеспечение. Как показывают хакеры, наиболее агрессивный метод подмены программ связан с «вирусом», но не есть ли идеология другим названием для программного человеческого вируса?

С этим идеологическим вирусом в качестве нашего оружия, США смогут вести самую мощную биологическую войну и выбирать, исходя из стратегии национальной безопасности, какие цели-народы нужно заразить идеологиями демократического плюрализма и уважения индивидуальных прав человека».

Стивен Манн искренне полагал, что при помощи подобного программирования можно либо «отложить создание критического состояния, либо поощрить его, и направить развитие системы в нужное русло». При этом, «в действительности, сознаем это или нет, мы уже предпринимаем меры для усиления хаоса, когда содействуем демократии, рыночным реформам, когда развиваем средства массовой информации через частный сектор».

Особо следует подчеркнуть, что Стивен Манн не имел ни математического, ни физического образования, а был специалистом по английской классической литературе, который затем перешел на дипломатическую работу. Стивен Манн был карьерным дипломатом, близким Пентагону. Впервые прикладная концепция Стивена Манна была обнародована спустя два года после опубликования первых работ по «мягкой силе» в 1992 году в журнале Военного колледжа армии США, в томе 22 под названием «Теория хаоса и стратегическая мысль». Кроме своей основной работы несколько позже он опубликовал работу «Теория сложности и политика национальной безопасности» в книге «Сложность, глобальная политика и национальная безопасность», изданной Университетом национальной обороны.

В своих статьях, посвященных прикладным аспектам теории хаоса, он обслуживал новую пентагоновскую стратегию, связанную с крахом Советского Союза. Эта стратегия впервые была опубликована в марте 1992 года и утверждена еще президентом Джорджем Бушем-старшим. Стратегия предусматривала, что «первая и главная цель стратегии состоит в том, чтобы предотвратить повторное появление любой новой сверхдержавы

на территории бывшего Советского Союза или в какомлибо другом месте. Цель состоит в том, чтобы Соединенные Штаты Америки никогда впредь не сталкивались с угрозой, сравнимой с Советским Союзом. Это является главным фактором, лежащим в основе новых глобальных и региональных стратегий. Практически они должны обеспечить условия, которые предотвратят доминирование любой враждебной силы в регионах, ресурсы которых достаточны для создания в перспективе новой глобальной власти. К таким регионам относятся Западная Европа, Восточная Азия, территории бывшего Советского Союза и Юго-восточной Азии». (Выдержки из «Руководства Пентагона по предотвращению повторного появления нового соперника», опубликованные газетой New York Times 08.03.1992 г.)

Прикладная теория управляемого хаоса Стивена Манна как раз и была призвана предоставить инструментарий для деструкции территорий и ресурсных баз потенциальных кандидатов в новые сверхдержавы. В первые годы после своего появления теория в основном не выходила за пределы государственного департамента и учебных учреждений министерства обороны США. Ситуация изменилась с приходом к власти администрации Дж. Буша-младшего. Политические авантюристы и, как впоследствии выяснилось, распильщики военных бюджетов и коррупционеры Р. Чейни и Д. Рамсфелд всерьез восприняли дилетантские построения Стивена Манна. Это тем более удивительно, что именно в Соединенных Штатах расположен Институт сложности в Санта-Фё, который является одним из мировых лидеров в сфере изучения нелинейных, неравновесных процессов. Более того, Стивен Манн выступал несколько раз там со своей концепцией и был жесточайшим образом раскритикован. В результате дилетантизма, воцарившегося в Вашингтоне в последние десятилетия, пропагандистпопуляризатор последовательно направлялся на работу в ряд ключевых горячих точек. Итоги говорят сами за себя.

Подавляющая часть проблем, с которыми сталкиваются в настоящее время Соединенные Штаты в самых разных уголках планеты, от Египта до Пакистана, от Бразилии до Афганистана, является результатом их же собственных неразумных, авантюристических действий, в значительной степени связанных с реализацией стратегии «управляемого хаоса». Т.е. сегодня огромные финансовые ресурсы и усилия тратятся на борьбу с собственными ошибками и просчетами.

Не надо быть работником ведущей «фабрики мысли» или выпускником MIT для того, чтобы понять простую вещь. Теория хаоса – это не что иное, как общеупотребительное название теории динамических, стохастических, нелинейных систем. Отличительной особенностью этой теории является тот факт, что она научилась выделять широкий круг существующих в природе и обществе систем и процессов, которые характеризуются высокой неустойчивостью и неопределенностью. Как правило, эти характеристики присутствуют не всегда, а появляются лишь на определенной стадии существования системы. Эти стадии называют еще «самоорганизованной критичностью», «режимом с обострением», «повышенной турбулентностью» и т.п. Названия разные, но суть одна. Будущее таких систем практически невозможно предсказать. Более того, выбор того или иного варианта дальнейшего существования системы в немалой степени случаен. Еще более важно то обстоятельство, что малые воздействия на систему порождают очень большие последствия. Причем, как говорят математики, зависимость между функцией и аргументом имеет не одно, а много решений. Т.е. оказывая малое воздействие, никогда наперед не знаешь, какой будет результат.

В общем, всё это азы математики, синергетики, теории сложности. Однако в мире, где пропагандисты выступают в роли аналитиков и обслуживают дилетантов-политиков, незнание базовых принципов используемых

методов чревато разрушительными последствиями. Собственно, это мы и можем наблюдать во многих внешнеполитических акциях США последнего времени.

Любой выпускник приличного университета или человек, поварившийся в бизнесе, военном деле, или побывавший в горячих точках, если ему задать вопрос об управляемом хаосе, не колеблясь, ответит, что речь идет об оксюмороне. Хаос можно организовать или вызвать, но управлять им еще никто не научился. Ведь хорошо известно, что управляющая система для того, чтобы осуществлять эффективное управление, по сложности должна превосходить управляемую. А это условие, применительно даже к самым простым обществам, выполнить крайне сложно. Поэтому после каждого вмешательства американцев остаются фейл стейт и зоны перманентных боевых действий, типа Сомали, Йемена, Афганистана, других стран Ближнего Востока, лесных районов Колумбии и т.п. В свою очередь, в последующем эти регионы становятся рассадниками мирового терроризма, наркотрафика, работорговли, торговли оружием и т.п. В общем, концепция управляемого хаоса обернулись вторжением хаоса в сами Соединенные Штаты.

Надо сказать, что американский истеблишмент, несмотря на множество сложностей и недостатков, способен быстро учиться на собственных ошибках и извлекать уроки не только из чужих, но и из своих неудач. Поэтому в начале десятых годов теория Стивена Манна стала подвергаться уничтожающей критике в самих Соединенных Штатах, и была фактически снята с вооружения в качестве одного из основных внешнеполитических методов.

Встречающееся среди многих российских экспертов мнение, что события «арабской весны» и война в Сирии являются порождением стратегии управляемого хаоса, реализованной Соединенными Штатами Америки, не имеет сколько-нибудь солидного документального фактологического подтверждения. Природа этих событий

носит несколько иной характер, рассмотрение которого выходит за пределы настоящей работы.

Еще одним до поры до времени эффективным методом реализации стратегий «мягкой», а затем «умной» силы были «оранжевые» революции, базировавшиеся в первую очередь на комплексе работ Джина Шарпа. Фактически Джин Шарп поставил перед собой задачу классифицировать, кодифицировать и привязать к конкретным ситуациям все наблюдавшиеся в истории методы ненасильственных действий. В итоге, в своей работе «Power and Struggle (Politics of Nonviolent Action, Part 1)» («Власть и борьба (Политика ненасильственных действий, часть I»), изданной еще в 1973 году он выделил 198 методов ненасильственного протеста и убеждения.

Хорошо известны примеры «оранжевых» революций и роль американских и британских внешнеполитических разведывательных ведомств в их подготовке и практическом осуществлении. Гораздо менее известен тот факт, что в настоящее время революционный конструктор Джина Шарпа стал предметом критического рассмотрения.

Летом 2013 года в ведущем учебном центре по подготовке специалистов по «оранжевым» революциям, во Флетчеровской школе Университета Тафтса, США совместно с ведущим центром по разработке методов сопротивления власти – Международным центром по ненасильственным конфликтам (ICNC) была проведена в полузакрытом режиме большая конференция «Ненасильственное сопротивление: вчера, сегодня, завтра».

Работа конференции была выстроена вокруг обсуждения доклада М. Стефан и Э. Ченовез «Why Civil Resistance Works: The Strategic Logic of Nonviolent Conflict». В докладе были изложены результаты статистического исследования всех гражданских конфликтов в мире за 1985–2013 годы. По итогам анализа выяснилось, что движения гражданского сопротивления доби-

лись успеха в 55% зафиксированных случаев, в то время, как военные противостояния власти имели успех только в 28%. В итоге был сделан вывод о том, что «гражданские ненасильственные кампании обеспечивают устойчивый переход к демократии в два раза чаще, чем вооруженное противостояние с властью».

Однако наряду с этим привычным выводом, на конференции выяснилось, что в течение последних 15 лет наибольшую эффективность показали смешанные стратегии, которые имели успех почти в 70% случаев. К смешанным стратегиям относились гражданские ненасильственные кампании, которые сопровождались либо угрозой силового противостояния с властью, либо с точечными конкретными вооруженными акциями. Соответственно был сделан вывод о необходимости разработки теории, а главное детального практического инструментария для гибридного гражданского сопротивления, включающего как ненасильственные методы, так и целевые вооруженные акции или угрозы применения силы против власти. Первым примером практической отработки подобного инструментария и технологий стали украинские события начала 2014 года.

Кроме того, на конференции было рекомендовано повысить эффективность гражданских ненасильственных кампаний за счет широкого использования новых информационных технологий, обеспечивающих улучшение координации, информирования и обеспечения совместных действий «гражданского сопротивления».

Приведенный документальный материал показывает, что к середине 2010-х годов концепция «умной силы», включая методы и формы ее реализации, в значительной степени исчерпала себя, по крайней мере, в своем первоначальном виде.

Помимо отмеченных ограничений в использовании методов и форм реализации стратегии «умной силы», безвозвратно скомпрометирована сама основа этой

стратегии. Дж. Най, давая в свое время формулировку источников «мягкой силы» в интервью журналу Шпигель, отмечал, что «во-первых, это культура страны – так, в Америке культурное поле простирается от Гарварда до Голливуда. Во-вторых, политические идеалы, которые могут быть очень привлекательными для других, – это и демократия, и принцип свободы слова, и равенство возможностей. В-третьих, легитимность внешней политики, под которой понимается такой образ действий правительства, который другие народы могут признать соразмерной защитой наших национальных интересов».

Вряд ли кто сегодня будет спорить о том, что практически все три указанных источника, что называется, полностью пересохли. В условиях перехода к широкополосному дешевому интернету Голливуду нанесен едва ли не смертельный удар. В отличие от восьмидесятых – нулевых годов практически во всех основных странах мира налицо подъем национального телевизионного кинематографа, широкая экспансия компьютерных игр, а также других национальных культурных продуктов. Что касается равенства возможностей, то сегодня это самими американцами воспринимается как издевка. В США сегодня один из самых высоких в мире уровней неравенства. Уже долгие годы все хуже работают социальные лифты. Американская мечта о чистильщике обуви, ставшим миллиардером, осталась лишь в воображении только что подключившихся к интернету жителей африканской саванны или австралийских аборигенов. С такой же, по меньшей мере, иронией воспринимается легитимность внешней политики США, которая в текущем веке прошла достаточно бесславный путь от иракской и афганской авантюр до разоблачений Сноудена.

В сложившейся ситуации американские элиты и наднациональные глобалистские сети в значительной мере господствующие и паразитирующие на Соединенных Штатах, заняты разработкой принципиально новых дей-

ственных инструментов эффективного и по возможности экономичного решения проблем устранения геополитических противников и формирования глобалистского пейзажа мира.

### 2.2. Стратегия и тактика превентивных действий

В условиях острого запроса на новые методы борьбы с государственностью наиболее рекламируемым, популярным и доступным для внешнего наблюдения и анализа направлением остается модернизация инструментария, разработанного Джином Шарпом. Сегодня эта работа ведется в международном масштабе в рамках инициативы Civil Resistance 2.0: A New Database of Methods. Целью инициативы является аккумуляция всего мирового опыта использования информационных технологий при осуществлении антиправительственных ненасильственных действий. Наконец, в рамках инициативы собранные методы дорабатываются профессионалами в области информационных, когнитивных и социальных наук и практик, а затем транслируются так называемым гражданским активистам по всему миру.

Инициатива реализуется на базе Вашингтонского университета в Сиэтле, в рамках Digital Activism Research Project (DARP). Финансируется проект имеющим теснейшие связи с военно-разведывательным сообществом Национальным научным фондом США, подведомственным Госдепартаменту Институтом мира США и Фондом Макартуров, одним из главных спонсоров некоммерческих активистских организаций по всему миру. Ежегодно проект выпускает подробнейшую базу данных по методам и инструментам цифрового сопротивления или цифрового активизма. В последнем отчете, опубликованном в 2013 году, обобщено более 400 компаний цифрового активизма из 100 стран за период 2010-2012 годы. Помимо фактического материала для так называемых циф-

ровых активистов доступны усовершенствованные специалистами своего рода методические рекомендации и инструкции по использованию доработанных наиболее эффективных инструментов цифрового сопротивления. Доклады и материалы обновляются ежегодно.

При всей важности этой работы представляется, что, в конечном счете, она является одновременно своего рода переходной стадией и операцией прикрытия для формируемых в настоящее время принципиально новых, взаимоувязанных стратегии, тактики и оперативных мер, обеспечивающих соответствующим инструментарием для борьбы с властью и дестабилизации общественного порядка в странах-противниках глобалистской наднациональной элиты.

Поскольку данная работа находится в полном разгаре, было бы трудно ожидать появления законченных монографий на этот счет. Более того, есть все основания полагать, что такие монографии вообще не будут написаны. Дело в том, что само по себе очерчивание той или иной стратегии с системой мер по ее реализации, как показывает опыт, снижает эффективность ее применения. В зарубежных источниках содержится множество указаний на то, что последние несколько лет многие исследования в области социальных, военных, когнитивных наук полностью или частично секретятся.

Однако анализ всей совокупности исследовательской активности ведущих научных центров и университетов, повесток дня проводимых конференций, а также финансируемых из государственных источников, прежде всего США, исследований и разработок, позволяет очертить не только общую направленность, но и основные блоки формирующейся политики и инструментария борьбы с государственностью и деструкции геополитических субъектов.

Для формирования методологической основы зарождающейся концепции огромное значение имела недавно изданная книга Барнетта Р. Рубина «Blood on the

Doorstep. The Politics of Preventive Action». Автор является ведущим исследователем Нью-Йоркского университета и одной из ключевых фигур в чрезвычайно влиятельном Совете по международным отношениям.

Книга написана в основном на материале кровопролитных конфликтов последних 20 лет. Цель работы – это проработка теоретического, практического и даже юридического фундамента для превентивных действий в отношении независимых государств. Логика книги состоит в следующем. Многие конфликты, унесшие тысячи человеческих жизней, по мнению автора, произошли потому, что Запад, скованный различного рода международными соглашениями, вовремя не вмешался и не положил конец насилию на раннем этапе конфликта. Отсюда делается вывод о том, что для предотвращения потенциально «большой крови» вполне оправдано и справедливо насильственное вмешательство или прямая поддержка вооружением и инструкторами для боевиков извне на самой ранней стадии конфликта, в сочетании с гражданским ненасильственным сопротивлением изнутри. При этом, поскольку государства обременены множеством соглашений и условий международного права, то такие превентивные действия, по мнению автора, могут выполнять, в том числе, негосударственные, частные или некоммерческие организации. Хотя книга написана практически полностью на материале Азии и Африки, последние два года Б. Рубин на многих конференциях отстаивает точку зрения, что предлагаемый им подход носит универсальный характер. Причем его точка зрения находит все большее и большее понимание в официальных кругах Соединенных Штатов, Великобритании и ряда европейских стран.

Этому в значительной мере способствует недавно появившееся и с каждым годом крепнущее идеологическое течение, которое исходит из превосходства Запада над всеми иными цивилизациями. Если С. Хантингтон в своей знаменитой работе «Столкновение цивилизаций»

исходил из наличия нескольких конфликтующих независимых, но в каком-то смысле равных цивилизаций, то новое течение фактически утверждает, что существует только западная цивилизация и варвары, которые к ней, в конечном счете, должны присоединиться.

Экономическое обоснование этой концепции сделано в наиболее популярном экономическом труде последних пяти лет «Why Nations Fail: The Origins of Power, Prosperity, and Poverty». Его авторы Д. Асемоглу и Д. Робинсон, несмотря на молодой возраст, являются наиболее вероятными кандидатами на получение Нобелевской премии по экономике в ближайшие годы. Книга блестяще написана, базируется на огромном фактическом материале и переведена на основные языки. Главный ее смысл состоит в том, что только западные экономические институты способны обеспечить экономическое развитие и социальный прогресс.

Историческое обоснование концепции исключительности Запада сделано в книге Н. Фергюссона «Civilization: The West and the Rest». На русский язык название книги можно перевести, как «Цивилизация: Запад и все остальные». В книге отстаивается концепция, смысл которой в следующем: только на принципах западной, преимущественно британской цивилизации может быть построено нормальное общество. Запад является, по мнению автора, абсолютно уникальным феноменом в истории человечества. Соответственно для остальных цивилизаций единственный шанс на выживание это – ассимиляция в западную, а точнее англо-американскую цивилизацию. По мнению Н. Фергюссона, в противном случае будет происходить не столкновение цивилизаций, как полагал Хантингтон, а «сокрушение цивилизаций, не ассимилировавшихся с Западом».

Н. Фергюссон в течение последних лет входит в число 100 наиболее авторитетных и известных на Западе мыслителей. Он является профессором Гарвардского

университета, советником руководства республиканской партии США.

По мнению Н. Фергюссона гражданский активизм и протестные действия в странах, не относящихся к западной цивилизации, всегда направлены на то, чтобы перейти от состояния фактического варварства к цивилизованному строю, т.е. приобщению к англо-американской цивилизации. Поскольку зачастую власти стран, где действуют гражданские активисты, препятствуют им в ненасильственных действиях по включению в единую и единственную западную цивилизацию, то это чревато в перспективе кровопролитными конфликтами. Соответственно, Запад, по мнению Н. Фергюссона, вправе, чтобы предупредить эти конфликты, осуществить превентивные действия, включая поддержку извне, как ненасильственных кампаний, так и насильственных акций сил сопротивления.

Указанные выше работы представляют своего рода идеологический базис и обоснование новой стратегии превентивных действий.

Вместе с концепцией управляемого хаоса в последние годы критически переосмыслена и, по сути, утратила влияние концепция «умной толпы», впервые описанная в книге H. Rheingold «Smart Mobs: The Next Social Revolution». Дело в том, что даже хорошо технически оснащенная и информатизированная толпа остается толпой, т.е. крайне малоуправляемым, нестабильным и неорганизованным формированием.

В последние полтора года прошел целый ряд конференций, участники которых пришли к выводу, что концепция «умной толпы» построена на значительных преувеличениях. Дело в том, что данная концепция в значительной степени сформировалась под влиянием уличных бунтов и беспорядков в Великобритании, Франции, Германии и т.п. Было отмечено, что по факту все эти события носили локальный характер, охватывали,

в общем, незначительное число участников и не имели по сути никаких политических последствий. При этом на конференциях эти бунты противопоставлялись событиям «парижской весны» 1968 года, движению против войны во Вьетнаме в конце 60-х и др. подобным акциям, которые затрагивали сотни тысяч и даже миллионы людей.

Однако в современном индивидуализированном мире попытка реанимировать технологии, лежавшие в основе этих движений, обречены на неудачу. Поэтому в качестве стержня концепции превентивных действий предлагается использовать прежде всего политтехнологическое наследие Сола Алинского.

Этому в значительной степени способствовало и то, что учеником Сола Алинского являлся политтехнолог номер один в Соединенных Штатах Касс Санстейн. В системе С. Алинского несколько лет работал Барак Обама. Диплом по работам С. Алинского писала Х. Клинтон, которой в двадцатилетнем возрасте С. Алинский предсказал блестящее политическое будущее.

В России ни одна из книг С. Алинского до сих пор не издана. Поэтому есть смысл более подробно остановиться на сути его концепции. С. Алинский начал свою практическую работу в 30-е годы и вел до самой смерти в начале 70-х. После его смерти продолжают действовать многочисленные организации, построенные на идеях С. Алинского, его разработки активно используются политтехнологами Демократической партии США.

Главным содержанием как книг, так и практической деятельности С. Алинского были методы захвата власти для осуществления преобразований. В своей главной книге «Rules for Radicals» («Правила для радикалов») С. Алинский пишет: «Достоевский считал, что больше всего люди боятся сделать первый шаг. Поэтому любому революционному взрыву должно предшествовать медленное, пассивное изменение сознания людей, в результате чего они должны почувствовать себя настолько

неприкаянными, отвергнутыми, потерянными и бесперспективными в господствующей системе, что сами начнут желать отпустить прошлое и изменить будущее. Для любой революции важно желание масс принять преобразование. Чтобы создать такую ситуацию, организатор должен работать не только со средним классом, но и с «голубыми воротничками», иначе они сдвинутся вправо. Этого нельзя допустить». Но у бедных нет никакой власти, поэтому реальной целью должен быть средний класс: «Сейчас и в последующих десятилетиях организация должна сосредоточить свои действия на среднем классе. Это – то место, где концентрируется власть...»

Следует отметить, что под средним классом С. Алинский понимал не офисных бездельников и представителей новой богемы, а, прежде всего, людей дела – инженеров, конструкторов, линейный персонал в фирмах, банках и других организациях.

С. Алинский понимал, что люди дела, у которых есть определенный достаток с одной стороны, а с другой стороны – навыки практической работы, вряд ли горят желанием вступать в конфронтацию с властью. Поэтому прекрасно зная труды Г. Лебона, Г. Тарда и других, С. Алинский делал ставку не на толпу, а на организацию. Он полагал, для того, чтобы бороться с властью, на первом этапе надо ставить совершенно приземленные, конкретные, бытовые цели. На этом этапе он ставил задачу объединить людей, живущих в одном районе, организовать вокруг общих для них проблем и втолковать, что им нужно сообща финансировать их решение. В свою очередь решение предполагает создание сильной структуры – своего рода кооператива по решению проблем отдельно взятого района – способного к долгосрочной работе.

При этом он отдавал себе отчет, что сам народ организоваться не в состоянии. Для этого ему нужен специально подготовленный, обученный и натренирован-

ный организатор. Организатор должен, во-первых, обладать необходимыми знаниями и недюжинным умом, во-вторых, длинной волей и сильным характером, и, в-третьих, иметь суггестивные способности, и быть обученным методам успешного манипулирования людьми и организационной работе. Т.е. ключевой фигурой в концепции С. Алинского был организатор.

Готовились организаторы в специальных школах, открываемых, как правило, при университетах. Наиболее активно эта работа развернулась в Чикаго, включая Чикагский университет, где с системой С. Алинского познакомились Б. Обама, К. Санстейн и др.

При подготовке организаторов С. Алинский сформулировал правила, которые они должны реализовать в своей работе. Эти правила изложены в его главных книгах «Rules for Radicals» и «Reveille for Radicals». В число важнейших правил входят следующие:

• Медленно проникайте, просачивайтесь в такие существующие организации как церкви, профсоюзы, политические партии и т.п. Скрытно добивайтесь влияния внутри этих организаций и затем начинайте перемены с этой платформы.

• Полностью поддерживайте людей в их недовольстве и разногласиях.

• Используйте провокационные вопросы, чтобы манипулировать и использовать людей для предварительно заданной программы. Раздувайте напряжённость между ними как можно сильнее.

• Организатор должен вызвать на себя атаку, которая затем закрепит доверие к нему людей.

• Врага народа необходимо обозначить и назначить персонально.

• Враг должен быть совершенно поляризован, 100% негативно, как первопричина полного поражения или полной победы.

• Цель оправдывает средства.

• Радикал нацеливается на средний класс, так как он самый большой, и смешивается с ними, говорит на их языке, одевается, как они, использует их нравы, обращается к их моральным принципам.

• Организатор должен быть непредсказуемым и готовым вовлечь всех в хаос и беспорядки ради своих целей.

• Большие и громкие организованные протесты демонстрируют силу, даже если движение является небольшим.

• Добивайтесь того, чтобы люди действовали, а потом уже думали.

• Реагируйте шоком и ужасом, когда враг совершает любую ошибку, оговаривается и т.д.

• Жестоко подначивайте врага, смейтесь над врагом, издевайтесь над врагом. Используйте насмешки.

• У организаторов всегда должно быть несколько «драк в запасе», запас крестовых походов, между которыми они могут переключаться, чтобы сохранять темп.

• Случаи кратковременного тюремного заключения укрепляют движение.

• Власть – это не только то, что у вас есть, но и то, что враг думает, что у вас есть. Власть исходит из двух основных источников – деньги и люди.

• Никогда не выходите за предел знания ваших людей. Это заканчивается неразберихой, страхом и отступлением. Знания добавляют твердости каждому.

• Где только возможно, выходите за пределы ожиданий врагов. Ищите пути, чтобы усилить неуверенность, беспокойство.

• Заставьте вашего врага жить по им же сформулированным правилам. Если правило таково, что на каждое письмо необходим ответ, пошлите 30 тысяч писем. Вы можете уничтожить их этим, поскольку никто не может выполнить свои же собственные правила.

• Осмеяние – самое мощное человеческое орудие. От него нет защиты. Оно иррационально. Оно приводит

в бешенство. Работает как ключевой аргумент давления, заставляя врага пойти на уступки.

• Хорошая тактика – эта та, которая радует ваших людей. Они выполняют ее без понукания и возвращаются, чтобы сделать больше, делать свое дело и даже подсказывать лучшие.

• Тактика, которая тянется слишком долго, становится волокитой. Не превращайтесь в старые новости.

• Не отключай давление, но и не переусердствуй. Если переборщишь в негативе, он станет позитивом, поскольку публика симпатизирует обиженным. Ищи новые тактики, атакуй со всех флангов, не давая врагу шанса передохнуть, перегруппироваться и сменить стратегию. Угроза чаще более действенна, чем реальная акция. Она рождает в коллективном уме атакуемой организации картины ужаса от возможных последствий и деморализует противника.

• Цена успешной атаки – конструктивная альтернатива. Никогда не позволяйте врагу набирать очки оттого, что вас поймали врасплох без решения проблемы.

• Ухвати цель, заморозь ее и поляризуй. Отсеки сети поддержки и изолируй цель от симпатий. Иди по следу людей, а не учреждений, людям быстрее причинить боль, чем учреждениям. Это жестоко, но очень эффективно. Прямая, персонализированная критика и осмеяние дают результат.

Реализуя изложенные выше правила, организатор должен вести свою организацию по ступенькам – начиная с малых бытовых практических дел, постепенно выводя ее на все более высокие уровни, которые в итоге приводят к жестким конфликтам с властью. Одновременно, по мысли С. Алинского, организация будет сплачиваться и разрастаться. К какому-то моменту самой логикой развития организации, ее члены убеждаются в необходимости противодействия и борьбы с властью на самом высоком уровне.

Организационные и политические технологии С. Алинского были опробованы в десятках городов Соединенных Штатов, в самых различных кампаниях и практически везде показали свою высокую эффективность. Затем деятели Демократической партии США обучили методам С. Алинского активистов в ряде стран Латинской Америки, где также эти методы доказали свою высокую действенность.

В последние четыре года прошло около 20 конференций, посвященных технологиям С. Алинского. Причем, эти конференции проводили не только университеты, партийные или общественные организации, но и структуры, напрямую связанные с военно-разведывательным сообществом США.

Ключевым моментом в эффективном использовании методов С. Алинского является обеспечение на самом первом этапе критической массы членов организации, которая затем будет разрастаться и укрепляться. Если сам С. Алинский связывал решение этой задачи исключительно с подготовкой организаторов, то его ученик, бывший «информационный царь» Б. Обамы и один из членов комиссии по реформе АНБ Касс Санстейн предложил использовать разработанную им технологию «Надж», о которой подробно рассказано в разделе «О чем умолчал Эдвард Сноуден» в главе «Большие Данные».

Применение технологии «подталкивания», или «Надж» на основе анализа Больших Данных об участниках конкретного территориального, профессионального или любых других сообществ позволяет уже на первом этапе максимально охватить потенциальных участников и облегчить им принятие решения о вступлении в организацию. Этот же метод помогает и росту организации на всех этапах ее развития.

Естественно, что в современных условиях гражданская организация сопротивления должна обладать всем

необходимым набором коммуникационных, аналитических и иных технологий, повышающих эффективность ее деятельности. Достаточно подробно об этом описано в книге Э. Шмидта и Д. Коэна «Новый цифровой мир».

В частности они указывают: «В долгосрочной перспективе развитие телекоммуникационных технологий способно подорвать положение большинства авторитарных режимов, поскольку, как мы видели, их шансы в противостоянии с людьми, вооруженными персональными устройствами для проверки фактов, снижаются с каждым одиозным случаем, ставшим достоянием гласности. Другими словами, нельзя назвать совпадением то, что авторитарные режимы существуют сегодня в странах с самым низким в мире уровнем проникновения интернета. Однако в краткосрочной перспективе такие режимы смогут извлечь преимущества за счет подключения их граждан к сети, что уже используют в своих интересах законодательство и средства массовой информации. Среди авторитарных правительств уже складывается определенная тенденция: они стараются использовать всю мощь современных высоких технологий вместо того, чтобы бояться и запрещать их, то есть налицо сдвиг от явного тоталитаризма к более тонким формам контроля, который описал в своей отличной книге The Dictator's Learning Curve («Кривая обучаемости диктатора») журналист Уильям Добсон. Вот что он пишет: «Сегодняшние диктаторы и авторитарные правители гораздо умнее и сообразительнее, чем раньше, и чаще руководствуются здравым смыслом. Видя растущее давление, самые умные из них не ужесточают свой режим до полицейского государства и не закрываются от внешнего мира; вместо этого они учатся и адаптируются. Вызовы, с которыми сталкиваются десятки авторитарных режимов в результате развития демократии, заставляют их экспериментировать, придумывать, хитрить». Добсон перечисляет множество средств, при помощи которых

современные диктаторы концентрируют власть в своих руках, создавая при этом видимость демократии: псевдонезависимая судебная система; ручной «всенародно избранный» парламент; широкое толкование и селективное применение законов; медийный ландшафт, допускающий существование оппозиционных СМИ, но только до тех пор, пока оппоненты режима признают существование негласных границ, которые нельзя переходить. По словам Добсона, в отличие от диктатур и государств-изгоев прошлого, современные авторитарные государства – это «сознательно и искусно созданные проекты, их заботливо выстраивают, укрепляют и постоянно совершенствуют».

Для того чтобы противостоять этим тенденциям и информационно вооружить гражданские организации сопротивления практически все ведущие американские интернет-платформы и многочисленные стартапы реализуют разнообразные программы, приложения. Примерами могут быть мессенджеры с самоуничтожающимися сообщениями, легко шифруемая электронная почта, сервис публикации в интернете быстростирающихся фотографий и т.п. При этом интересно, что значительная часть подобных программ координируется и финансируется QCRI (Катарским институтом компьютерных исследований). И конкретно Центром социальных инноваций этого института, возглавляемым доктором Патриком Меером.

В рамках концепции превентивного действия особое внимание уделяется разработке инструментария, который позволил бы осуществлять решительные выступления против государственной власти и организовывать их превентивную поддержку извне лишь в те моменты, когда выступления имеют большие шансы на успех.

В этой связи важнейшим составным элементом системы превентивных действий является создание и оснащение протестных групп компьютерными программами

и сервисами раннего предупреждения кризисных событий и ситуаций. В настоящее время SecDev Foundation и компания Palantir заняты разработкой так называемого четвертого поколения компьютерных систем раннего предупреждения для гражданского сопротивления. Эти системы в отличие от третьего поколения, использующего лишь структурированные данные, в значительной степени опираются на информационные потоки из различного рода социальных СМИ, платформ и сетей, типа Twitter, Facebook и проч., а также активного использования краудсорсинга. Базовой платформой для разработки этой системы является свободное программное обеспечение Ushahidi.

Наконец, ключевым элементом системы превентивных действий является подготовка целевых групп, способных к проведению насильственных, в т.ч. вооруженных акций в рамках общих гражданских акций сопротивления. По имеющейся информации на сегодняшний день преобладает точка зрения о том, что не следует смешивать участников кампаний ненасильственных действий и организаций гражданского сопротивления с членами боевых групп.

Последние должны проходить специализированную подготовку и рекрутироваться в основном из лиц, уже прошедших военную службу, либо активистов спортивных, стрелковых и прочих клубов. Детальное описание этого фрагмента концепции практически отсутствует. В то же время общие принципы подготовки, а также задачи, стоящие перед такими группами, и способы их выполнения можно извлечь из работ едва ли не наиболее известного специалиста по войнам, конфликтам низкой интенсивности и городским восстаниям Дэвида Килкуллена «Out of the Mountains: The Coming Age of the Urban Guerrilla» и «Counterinsurgency». На вторую половину 2014 года анонсирован выход сборника работ «Civil Cyberwars». В сборнике будут впервые рассмотре-

ны практические вопросы гражданской кибервойны, как вида боевого сопротивления авторитарным режимам. При этом по аннотации можно понять, что под кибервойной понимается осуществление операций по выводу из строя объектов критических военных, правительственных или гражданских инфраструктур или перехват управления ими. С учетом того, что книга издается в США, можно предположить, что гражданская кибервойна рассматривается как возможный элемент разрабатываемой в настоящее время доктрины превентивных действий.

Таким образом, есть все основания полагать, что в настоящее время не только сформирована, но и начала проходить практическую апробацию новая комплексная система превентивных действий по деструкции социальных субъектов, борьбы с государственностью и подрывом общественного порядка в странах – геополитических противниках США, их союзников, а главное, наднациональной иерархо-сетевой, финансово-корпоратократической элиты.

### 2.3. Государство и личность в Сети

Спецслужбы всегда стремились контролировать распространение информации. И это правильно. Это их прямая задача. Сегодня ее важность возросла.

Известный американский специалист по безопасности, едва ли не культовая фигура в Сети Стив Рамбам любит повторять: «Если злоумышленник запустил к вам вредоносное программное обеспечение – это уже не ваш компьютер. Если злоумышленник при помощи программ внес изменения в оперативную систему – это уже не ваш компьютер. Если злоумышленник знает ваши пароли на сайтах, где вы их неосторожно оставили или взломал вашу электронную почту, то это уже не ваш компьютер».

Почитаешь С. Рамбама, а потом узнаешь, что согласно данным «Лаборатории Касперского», в этом году каж-

дый второй интернет-пользователь в Санкт-Петербурге и окрестностях подвергся кибератаке. Сёрфишь дальше, и выясняешь – 70% всех смартфонов с Android`ом заражены. Рука сама тянется к Рождественской сказке А. Куприна «Жизнь», откуда хочется выписать бессмертное: «...как страшно жить!».

Однако, в действительности, все не так, как в реальности. Всех стращают киберпреступностью. Недавно известный производитель антивирусов McAfee Secure и Центр стратегических и международных исследований представили совместный отчет под названием «The Economic Impact of Cybercrime and Cyber Espionage», главная тема которого – влияние киберпреступлений на глобальную экономику. Из доклада можно почерпнуть любопытную цифру. Оказывается, глобальный ущерб от киберпреступлений в годовом исчислении находится между $300 миллиардами и $1 триллионом. Примерно с таким же разбросом дают оценки и другие уважаемые международные организации. Это похоже на то, как если бы к больному пришел врач и сказал: «У Вас температура где-то между 36.0 и 43.0, и у Вас возможно насморк, а возможно рак в неоперабельной стадии».

Понятно, что с интернетизацией всего и вся, киберпреступность растет по экспоненте. Соответственно и ущерб глобальной экономике, хозяйству отдельных стран и личным бюджетам граждан возрастает из года в год, возможно, не на проценты, а на десятки процентов, а то и в разы. Однако, оценки, подобные приведенной выше, дискредитируют аналитические методы и дают дополнительные аргументы тем, кто в блогах, социальных СМИ и на мейнстримных ресурсах пишет материалы о злонамеренном АНБ, преступном ФБР, «кровавой гебне», «продажных ментах» и их подручных из БНД и Моссада.

Ситуация и в мировом интернете, и в Рунете относительно вопросов контроля над всемирной сетью лучше

всего описывается строками еще одного великого русского литератора Н. Некрасова:

*Выдь на Волгу: чей стон раздается*
*Над великою русской рекой?*
*Этот стон у нас песней зовется...*

Наряду с рядовыми блоггерами, в процессе участвуют и очень уважаемые люди. Например, Тим Бернерс-Ли, носящий почетный титул создателя сети, решительно осудил государственную цензуру и слежку в интернете, назвав их угрозой демократии. Будучи в России, другой уважаемый человек, в прошлом хакер номер один и социальный инженер от Бога (или черта), а ныне добропорядочный специалист по предотвращению киберпреступлений и информационной безопасности, Кевин Митник сожалел по поводу тех, кто «готов пожертвовать своими свободами ради безопасности. Поскольку, если однажды уступить свои права, то обратно их уже не вернуть».

Пока копья ломаются в пылу сражений за сохранение анонимности в интернете, складывается весьма странная ситуация. Никому не придет в голову отменить паспорта, водительские удостоверения, медицинские карты и другие документы, связанные с идентификацией личности. Мало кто окажется сторонником нового обычая – не представляться при знакомстве, или передвигаться по улице в шелковой маске Зорро или железной маске героя Дюма-отца.

В мире, где окончательно стерлась грань между реальностью и виртуальностью, которые слились в совмещенную действительность, сетевая анонимность становится анахронизмом.

Человеческое взаимодействие должно строиться в этой действительности по единым правилам, законам и обычаям. Кстати, это очевидно и подавляющей части пользователей сети, которые озабочены реальными

жизненными проблемами и не страдают параноидальными страхами относительно того, что за ними следит Большой Брат, использующий PRIZM или COPM. В этой связи показательно, что на широко анонсированный митинг в поддержку Эдварда Сноудена, и против АНБ и других Больших Братьев в Вашингтоне вышло чуть больше двух тысяч человек, а на состоявшемся в тот же день мероприятии против жестокого обращения с домашними животными присутствовало в разы больше людей.

Думаем, деанонимизацией интернета дело не закончится. Процесс неизбежно пойдет гораздо дальше. Прежде чем обосновать такое, можно сказать, экстремистское утверждение, расскажем три коротких истории.

Как уже говорилось выше, не так давно американская пресса сообщила, что в январе 2013 года хакеры сумели получить доступ к Национальному реестру плотин – закрытой базе данных, которую ведет Инженерный корпус армии США. База охватывает данные обо всех 79 тыс. плотин на территории Америки, включая 8,1 тыс. наиболее крупных плотин, регулирующих водопотоки и водоснабжение крупнейших городов, объектов национальной безопасности, центров критической инфраструктуры и т.п.

Через плотину Гувера автомобильным транспортом ежедневно перевозится от 13 до 16 тысяч человек. Ее электростанция обеспечивает электричеством ряд крупных городов США. Получив контроль над ней можно натворить немало интересного.

Другим характерным примером, о котором уже шла речь, является получение доступа хакерами к суперкомпьютеру в Национальной лаборатории имени Лоуренса в Бёркли, одного из самых мощных суперкомпьютеров в списке Топ-500. Помимо прочего этот суперкомпьютер входит в закрытую суперкомпьютерную сеть Министерства энергетики США. Но и это еще не все. Согласно появившимся в последнее время публикациям, супер-

компьютеры Агентства Национальной Безопасности и Министерства энергетики увязаны в единую общеамериканскую сеть суперкомпьютеров, которая используются для нужд обоих ведомств.

Самым интересным в этой истории является даже не то, что хакерам удалось подключиться к одному из самых мощных компьютеров в мире, а соответственно и сети суперкомпьютеров, а то, что взлом не был обнаружен техническими средствами. Двадцатичетырехлетний американский хакер Э.Миллер был арестован в результате дачи показаний другим хакером, пошедшим на сделку со следствием. Причем, арестован при попытке продать аренду на доступ к суперкомпьютеру.

И, наконец, третий пример. Не так давно хакеры из движения Anonymous взломали серверы Пентагона, Министерств энергетики и здравоохранения, и ряда других служб. Самым пикантным в этой истории был тот факт, что взлом правительственных серверов произошел еще в декабре 2013 года, долгие месяцы оставался незамеченным, и хакеры гуляли по правительственным компьютерным сетям, как по лужайке перед своим домом.

От себя заметим, что практически все ведущие компании, специализирующиеся на обеспечении программных решений по информационной безопасности для крупных сетей имеют американскую юрисдикцию. Иными словами, говорить о том, что в Америке царит полный бардак и безответственность, было бы несколько наивным.

А теперь давайте на минуту задумаемся, что, если в приведенных выше словах С. Рамбама заменить слово «компьютер» на слова «плотина», «атомный реактор», «биолаборатория» и т.п. Всем будут понятны последствия такой замены. И желающих посмотреть, как это будет выглядеть на практике, окажется очень мало.

То, что по состоянию на сегодняшний день не произошло ни одного крупного кибертеррористического акта

в отношении не просто критически важных, а смертельно опасных объектов военной, промышленной, энергетической и иных инфраструктур, абсолютно не гарантирует того, что этого не произойдет буквально завтра. Пока можно сказать, человечеству в целом, и отдельным странам просто хронически везет. Но, как известно, жизнь похожа на зебру, и белые полосы имеют тенденцию сменяться черными.

При этом к кибертеррористическим акциям, которые могут повлечь за собой не просто многочисленные, а гигантские человеческие жертвы, нельзя подходить с теми же мерками, что и к обычным, даже крупным преступлениям. Понятно, что когда взлетят ракеты с атомными боеголовками, уже поздно будет разбираться, кто конкретно в этом виновен и вести расследование в поисках причин. В отношении подобного рода смертельного оружия давно действует принцип презумпции виновности. А он предполагает не последующие расследования, а превентивные меры по тотальному предупреждению подобных рисков.

Информационные технологии вплотную подошли, а возможно уже и перешли тот рубеж, когда кибероружие по своим разрушительным последствиям становится сопоставимым с атомным, химическим и биологическим. Кстати, что касается последнего, то они имеют тенденцию сращиваться.

Отсюда, с неизбежностью, следует что, спецслужбы и правоохранительные органы всех технологически развитых государств гласно или негласно перейдут к превентивному контролю за всеми лицами, обладающими уникальными хакерскими компетенциями, соответствующими профессиональными навыками и знаниями, а также имеющими знакомства, указывающими на возможность возникновения неоправданных рисков, связанных с кибероружием.

# Глава 3
# БОЛЬШИЕ ДАННЫЕ

## 3.1. Большие данные как стратегический ресурс

В последние годы Большие Данные являются общепризнанным трендом экономического и технологического развития. Им посвящены тысячи публикаций. Они относятся к числу наиболее популярных тем, как в специализированных изданиях, так и в различного рода СМИ, рассчитанных на самую широкую аудиторию. В результате возникло впечатление, что Большие Данные – это нечто само собой разумеющееся, ясное, понятное. Широко распространена иллюзия о повсеместном применении Больших Данных в России.

Между тем, дело обстоит совсем не так. Беспристрастный анализ фактических данных показывает, что наша страна существенно отстает в сфере Больших Данных. Значительная часть компаний только используют термин «Большие Данные» в маркетинговых целях, а по сути, применяют старую, хорошо известную бизнес-аналитику, которая заметно отличается от Больших Данных. В стране практически нет спроса на специалистов по Большим Данным. Достаточно посмотреть наиболее популярные порталы работ, чтобы убедиться, что спрос на специалистов по Большим Данным у нас на порядки меньше, чем в США, Европе, Японии, Китае. В то время как во всем мире издаются сотни профессиональных и общедоступных книг по отдельным аспектам Больших Данных, в России только в этом году вышла первая книга по Большим Данным – работа В. Майер-Шенбергера и К. Кукьера «Большие данные. Революция, которая из-

менит то, как мы живем, работаем и мыслим». Да и эта книга носит не профессиональный характер, а написана в жанре нон-фикшн.

Происходящее вызывает особую тревогу в условиях, когда ведущие наднациональные мировые структуры и транснациональные корпорации, правительства ведущих стран мира, бизнес самых различных масштабов, системы управления производственной и социальной инфраструктурой и, конечно же, военно-разведывательный комплекс всех основных стран мира уже используют Большие Данные как важнейший стратегический ресурс.

Достаточно парадоксально, что до сих пор при широком использовании технологий Больших Данных нет общеупотребительного их определения. Наиболее часто используется популярное определение Майкла Франклина из Университета в Беркли: «Большие Данные – это любые данные, работа с которыми требует значительных затрат и из которых трудно извлечь информацию». Данное определение кочует из книги в книгу, из работы в работу. Между тем, оно является лучшим подтверждением тезиса о том, что наука о Больших Данные и практические технологии Больших Данных живут в параллельных реальностях. Соответственно, наука о Больших Данных не столько выступает надежным базисом для инженерии данных, сколько намерено или ненамеренно скрывает революционную суть технологий Больших Данных.

В самом деле, определение через большие затраты и трудность обработки может указывать не только на специфические характеристики данных, но и на неэффективность применяемых технологий. По сути, это определение ничего не говорит о том, чем Большие Данные отличаются от просто данных. Казалось бы, штука эта безобидная и носит исключительно академический характер. Однако, на практике это не так. Когда лица, принимающие решения, возможно и не обладающие

глубокими профессиональными познаниями, но в подавляющем числе наделенные недюжинным здравым смыслом, встречаются с подобными определениями, у них возникает подозрение, что они имеют дело с очередной маркетинговой уловкой. Суть этой уловки в том, чтобы просто извлечь из организации деньги, заставив ее заплатить за старые решения под новым названием. Несомненно, что непонятность Больших Данных для лиц, принимающих решения, в том числе и у нас, принципиальное отличие технологий Больших Данных от того, что было раньше, стали одними из важных причин, почему Россия и целый ряд других стран, располагающих всеми необходимыми предпосылками для использования этих технологий, на сегодняшний день отстают в гонке цифровых вооружений.

Чтобы разобраться с тем, что такое Большие Данные и в чем принципиальная новизна их технологий, надо для начала отследить время возникновения термина. Сам по себе термин «Большие Данные» появился пять лет назад после публикации специального выпуска ведущего американского научного журнала Nature, целиком посвященного этой теме. Затем тема, как по команде, была растиражирована сначала специализированными IT-изданиями, а затем подхвачена элитными СМИ, типа Foreign Affairs, Wall Street Journal и т.п.

Что же произошло пять лет назад? Есть ли какие-то документальные доказательства, что мы имеем дело с чем-то принципиально новым, а не с хорошо продуманной маркетинговой кампанией по принуждению правительств и корпораций к покупке нового, дорогостоящего софта? Ведь таких примеров в истории IT-индустрии было немало. В данном случае твердые документальные доказательства перехода некоего Рубикона имеют место быть.

Во-первых, он связан с достижением интернетом уровня контентной зрелости и переходом в фазу ярко

выраженного экспоненциального развития. Эта фаза получила название «информационный взрыв». Примерно, с 2008 года объем информации, вновь генерируемой в сети, стал удваиваться в течение примерно полутора-двух лет. На сегодняшний день можно привести следующие ключевые характеристики информационного взрыва.

По данным компании Cisco, объем сгенерированных данных в 2012 году составил 2,8 зеттабайт и увеличится до 40 зеттабайт к 2020 г. Примерно треть передаваемых данных составляют автоматически сгенерированные данные, т.е. управляющие сигналы и информация, характеризующие работу машин, оборудования, устройств, присоединенных к интернету, или к интернету вещей. Причем с каждым годом доля интернета вещей или как его сегодня еще называют «интернета всего» растет в общем объеме мировых информационных потоков. На 40% ежегодно увеличивается объем корпоративной информации, передаваемой и хранящейся в сети интернет.

Число пользователей интернета в мире к концу 2013 года составило 2,7 млрд. человек, или 39% населения земли, а к 2016 году эта доля составит 65-75% населения по данным Центра новостей ООН. Как ожидается, количество корпоративных пользователей интернета во всем мире увеличится с 1,6 миллиарда в 2011 году до 2,3 миллиарда в 2016 году.

Во-вторых, примерно в этот период времени появились и стали доступны для корпоративных пользователей принципиально новые IT-решения, позволяющие в режиме реального времени обрабатывать практически безразмерные массивы данных самого различного формата. Причем эти решения сразу же стали реализовываться не только как программные платформы, устанавливаемые на серверы, но и как облачные вычисления, где от организации не требовалось наличия дорогостоящей инфраструктуры компьютерного железа.

В-третьих, к концу нулевых годов западные, прежде всего, американские поведенческие и когнитивные науки, с одной стороны получили широкое признание бизнес-сообщества и государств, а с другой – из фазы исследований и разработок перешли в стадию производства эффективных технологий. Косвенным показателем этого процесса стал тот факт, что в течение нулевых годов три виднейших представителя поведенческих наук: Д. Канеман, Дж. Акерлоф и Р. Шиллер получили Нобелевские премии по экономике. Экономика была выбрана лишь потому, что Нобелевских премий в сфере наук о человеке просто не существует.

Теперь давайте вдумаемся, чем же, по сути, является интернет. Причем без разницы, о каком интернете мы говорим – об интернете людей или об интернете вещей. Не надо обладать глубокими техническими знаниями, чтобы понять, что фактически интернет является хранилищем, своеобразным архивом следов человеческой деятельности. Причем, не только той деятельности, которая реализована в конкретных поступках, действиях, событиях, но и архивом намерений, мнений, мыслей и отношений. Не зря автор знаменитых бестселлеров Маршалл Смит уподобил интернет толще земли, в которой можно обнаружить след доисторического животного, умершего миллионы лет назад. По сути, в интернете ничего не исчезает. Даже популярные в постсноуденовскую эпоху различного рода сервисы удаления аккаунтов и других следов пребывания в сети, удаляют лишь те следы, которые доступны для наблюдения простыми пользователями, не вооруженными специальными программами, доступными для корпораций и государств.

Соответственно формирование огромного, постоянно пополняющегося архива поведенческой активности самых различных субъектов, от отдельных государств и огромных компаний до небольших групп и отдельных индивидуумов собственно и послужило базисом появ-

ления Больших Данных. С тех пор направление Больших Данных стало ведущим в сфере информационных технологий.

Анализ накопленного за последние годы опыта применения технологий Больших Данных позволяет выделить несколько ключевых черт, отличающих Большие Данные от всех других информационных технологий. К ним относятся:

• во-первых, огромные массивы разнородной информации о процессах, явлениях, событиях, объектах, субъектах и т.п., пополняемые непрерывно в режиме он-лайн. Согласно имеющейся статистике 60% этой информации носит неструктурированный, в основном текстовой характер и 40% составляет структурированная, или табличная информация. В последние годы в общем объеме Больших Данных постоянно нарастает доля информации структурированного характера, поступающей от вещей, соединенных с интернетом – от холодильника до городской системы регулирования светофоров и т.п.;

• во-вторых, специально спроектированные программные платформы, где Большие Данные любого объема могут храниться в удобном для вычислений виде. Особо надо подчеркнуть, что эти архивы отличаются от привычных баз данных, которые приспособлены только для структурированной или табличной информации. Отличительной чертой этих хранилищ является то, что структурированная и неструктурированная информация могут обрабатываться совместно, как единое целое;

• в-третьих, наличие различного рода математического, прежде всего, статистического инструментария для обработки Больших Данных и получение результатов в виде, понятном для человека. Причем, при анализе Больших Данных используются не только традиционные методы математической статистики, но и алгоритмы распознавания образов, нейронные сети, построенные на основе аналогии с нервной системой и т.п.

По данным различных исследований, не более 0,6% всей имеющейся сейчас информации подпадает под категорию Больших Данных, т.е. накапливается, хранится и перерабатывается. В этих же исследованиях указывается, что потенциально в качестве Больших Данных может использоваться 23% всей хранимой в настоящее время информации. Т.е. фактически сейчас из всей этой информации используется как Большие Данные, т.е. обрабатывается, анализируется чуть больше 3%. Между тем, последние достижения в области создания платформ накопления, хранения и обработки объемов данных всех форматов позволяют увеличить потенциальные Большие Данные с 23% до примерно 40% всей передаваемой в сетях информации.

Еще в 2011 году McKinsey Global Institute объявил Большие Данные «следующим рубежом для инноваций, конкуренции и производительности». По данным целого ряда ведущих международных деловых изданий, уже сегодня Большие Данные дают заметный эффект в бизнесе. Например, выяснилось, что в транснациональных компаниях, входящих в список Fortune 500, где, казалось бы, до мелочей отлажены все процедуры и процессы, внедрение технологий Больших Данных на 5-7% увеличило эффективность использования ресурсов – труда, основных производственных фондов, энергии и т.п. и на 7-9% обеспечило рост объемов продаж. Для среднего бизнеса показатели оказались в полтора-два раза выше. Причем, следует отметить, что данные получены в условиях, когда мировая экономика испытывает на себе последствия глубочайшего финансово-экономического кризиса и экономический рост измеряется в лучшем случае 1-2%.

На чем же базируется эффективность Больших Данных? Технологии Больших Данных и прежде всего, методы статистического анализа, компьютерного распознавания образов и т.п., применяемые на огромных, постоянно пополняемых массивах данных позволяют:

• проводить самые различные и сколь угодно подробные классификации той или иной совокупности людей, компаний, иных объектов по самым разнообразным признакам. Такие классификации обеспечивают точное понимание взаимосвязи тех или иных характеристик любого объекта – от человека до компании или организации, с теми или иными его действиями;

• осуществлять многомерный статистический и иной математический анализ. Этот анализ позволяет находить корреляции между самыми различными параметрами, характеристиками, событиями и т.п. Корреляции не отвечают на вопрос – почему. Они показывают вероятность, с которой при изменении одного фактора изменяется и другой. В каком-то смысле Большие Данные представляют собой альтернативный традиционной науке метод. Наука на основе теоретических моделей отвечает на вопрос – почему, а затем, получив ответ, делает рекомендации, как действовать. В случае корреляции стадия поиска причины ликвидируется, а действие происходит в тех случаях, когда факторы тесно взаимосвязаны и на один из факторов легко или возможно осуществить целенаправленное воздействие;

• прогнозировать. На основе классификаций и аналитических выкладок осуществляется прогнозирование. Суть прогнозирования состоит в том, чтобы на основе корреляции определить наиболее легкий способ воздействия для того, чтобы один набор факторов, характеризующих тот или иной объект, лицо, компанию, событие и т.п. был преобразован в другой.

Как любой новый технологический пакет, Большие Данные тут же обросли мифами и заблуждениями. Многие из них постоянно усиливаются как самими производителями программных продуктов в сфере Больших Данных, так и средствами массовой информации, вынужденными адаптировать сложные вопросы информационных технологий для читателей, не обремененных излишними знаниями.

Из всей совокупности мифов стоит выделить три главных. Именно они наносят наибольший вред технологиям Больших Данных и тормозят их практическое применение, в том числе в нашей стране.

Прежде всего, в маркетинговых целях прикладываются немалые усилия, чтобы представить технологии Больших Данных неким новым Святым Граалем. На них необоснованно возлагается роль панацеи от всех бед. Между тем, очевидно, что любой технологический пакет имеет строго определенные условия для своего применения. Касательно Больших Данных таким ограничением является сопоставимость текущей ситуации с ранее наблюдавшимися ситуациями, процессами, периодами времени и т.п. В качестве примера можно привести прогнозирование потребительского поведения. Каждый человек на собственном опыте знает, что в ситуации умеренной инфляции он будет делать одни покупки, а при гиперинфляции его потребительское поведение коренным образом изменится. Если уже имеются Большие Данные как по периоду с низким уровнем инфляции, так и ситуации гиперинфляционного шока, то технологии Больших Данных будут полезны. Они позволят распознать, к какому классу относится текущая ситуация, обратиться к соответствующим поведенческим паттернам, характеризуемым теми или иными параметрами, и позволят дать достаточно достоверный прогноз. А вот если Больших Данных по периоду гиперинфляции нет, а она наступила, то в такой ситуации технологии Больших Данных будут бесполезны. Более того, их применение чревато непоправимыми ошибками. Этот пример показывает: технологический пакет Больших Данных, также как и другие технологические пакеты имеют строгие условия, где его применение эффективно, а где – нет.

Бытует мнение, что Большие Данные могут применяться только государственными структурами и транснациональными корпорациями, и недоступны для других

субъектов. Связано это с дороговизной как серверной части, так и программных продуктов, требуемых для работы с Большими Данными. И, наконец, с высокой зарплатой специалистов по Большим Данным. На практике в последние пару лет пользу из Больших Данных извлекают не только гигантские, но и небольшие структуры. Это стало доступным благодаря облачным вычислениям. В этом случае небольшие структуры выступают конечными пользователями технологического пакета, который получают как услугу. Использование этой технологии, как показывает опыт небольшого и среднего бизнеса в США, Западной Европе и Японии дает компаниям неоспоримые конкурентные преимущества по сравнению с бизнесами, которые подобными возможностями не располагают.

Наконец, очень серьезным заблуждением является рассмотрение технологического пакета Больших Данных как чисто машинной технологии. Многие государственные и корпоративные структуры впустую затратили огромные суммы средств только потому, что все ресурсы были направлены на закупку компьютерного железа и программных продуктов. При этом, затраты на кадры формировались по остаточному принципу. Между тем технологии Больших Данных требуют специалистов высочайшего уровня квалификации, как правило, обладающих образованием и профессиональными навыками не только в области информационных, но и гуманитарных наук. Сегодня, например, в США по оценкам экспертов не хватает от 50 до 70 тыс. специалистов по данным (data scientists). Большие Данные представляют собой не машинную, а человеко-машинную технологию.

Это наглядно показал пример любимого детища АНБ, компании П. Тиля Palantir. Одна из версий программы ориентирована на борьбу с мошенничествами в крупных финансовых структурах. Пока действовал чисто машинный вариант, система давала множество ложных

срабатываний. При этом полностью выявлялись и реальные случаи хищений, но они были смешаны с неточными выводами. В результате за программу посадили ветеранов служб экономической безопасности в качестве операторов. За короткий срок они обучились работе с программой и, используя человеческий опыт, выбирали из всей совокупности сигналов лишь те, которые указывали на реальные хищения.

По этому поводу руководитель одной из самых перспективных компаний в области прогнозирования Quid, также принадлежащей П. Тилю, Ш. Горли сказал: «Наибольший эффект Большие Данные дают тогда, когда возможности компьютеров в обработке гигантских массивов информации и выявлении нетривиальных связей соединены с человеческим опытом и профессиональной интуицией. А все, что вам рассказывает Р. Курцвейл про искусственный интеллект, это как минимум на ближайшее будущее просто красивые истории и PR-ходы».

Подытоживая суть технологий Больших Данных, можно согласиться с краткой формулировкой консалтинговой компании Forrester: «Большие Данные объединяют техники и технологии, которые извлекают смысл из данных на экстремальном пределе практичности».

Большие Данные в первую очередь были использованы в маркетинге, инвестиционном бизнесе, в продажах и т.п. Т.е. фактически там, где речь идет о косвенном, незаметном управлении поведением. Другой сферой применения Больших Данных стали процессы, описываемые множеством параметров, где за счет изменения режима можно получить экономию того или иного ресурса. В этой связи за пределами маркетинга и продаж самыми активными пользователями Больших Данных стали государственные учреждения и энергетический сектор экономики.

Но это лишь надводная часть айсберга. А подводная часть, как известно, всегда намного больше и, если мож-

но так сказать, серьезнее. Подводной частью айсберга стало использование технологий Больших Данных в таких сферах как разведка и контрразведка, военное дело, геостратегия и то, что традиционно называлось информационными войнами, а фактически представляет собой форму жесткого когнитивного противоборства.

Большие Данные были быстро осознаны такими странами, как Соединенные Штаты, Великобритания и Япония, в качестве важнейшего ресурса стратегического значения. 29 марта 2012 года администрация Б. Обамы выступила с инициативой «Big Data Research and Development Initiative». Инициативой предусматриваются вложение значительных объемов ресурсов и проведение комплексных мероприятий в целях активного использования технологий Больших Данных на ключевых направлениях государственной политики США. В рамках инициативы ежегодно в Вашингтоне проводятся большие конференции «Big Data for government & defense».

В сентябре 2013 года правительство Японии опубликовало информацию о разработке национальной программы по Большим Данным. Летом того же года правительство Австралии заявило, что рассматривает Большие Данные как важнейший национальный стратегический ресурс и выдвинуло задачу стать головной страной в сфере использования технологий Больших Данных как на правительственном уровне, так и на всех других уровнях государственного аппарата в масштабах Британского Содружества Наций.

### 3.2. Большие Данные в сетевом измерении

Долгие десятилетия в основе политтехнологий, методов жесткого информационного противоборства, конструкторов для проведения государственных переворотов и революций лежала так называемая «теория толпы». Она была разработана усилиями Лебона, Тарда, Конетти, Московичи и проч. Эта теория базировалась на

внешнем описании процессов. Как любая описательная теория она исходила частично из наблюдений, частично из картины мира самих исследователей. Тем не менее, теория, так или иначе, работала и построенные на ее основе методы давали определенный эффект. Едва ли не последним представителем школы «теории толпы» был Дж. Шарп с его книгами, включая работу «От диктатуры к демократии». Однако сегодня с уверенностью можно сказать, что «теория толпы» описывает лишь небольшой фрагмент реальности.

В последние годы создана, по сути, новая наука – социодинамика, которая обобщает эмпирические закономерности, полученные в результате применения технологий Больших Данных к огромным массивам информации, содержащейся в архивах крупнейших социальных платформ web 1 и web 2, таких как Google, Facebook, Twitter и т.п.

Эти эмпирические закономерности сегодня используются для отработки практического инструментария внешнего воздействия, управления и манипулирования социальными группами любых масштабов и любого уровня структурированности, а также для сборки и деструкции социальных субъектов. Именно применение Больших Данных к информации, полученной из социальных сетей, позволило осуществить прорыв в отработке инструментария внешнего социального управления поведением.

Как правило, зарубежные работы о Больших Данных можно поделить на две основных группы. Одни заполнены техническими подробностями архитектурных решений и интересны лишь профессионалам-айтишникам. Другие представляют собой набор красивых поучительных историй об эффективности применения Больших Данных для решения тех или иных задач, прежде всего, в бизнесе. Читать такие истории весьма занимательно, но с практической точки зрения абсолютно бесполезно.

Поэтому мы постарались пойти третьим путем. Он заключается в изложении результатов наиболее интересных исследований социодинамики и соответственно описании тех самых, только что выявленных эмпирических закономерностей, которые используются для разработки нового инструментария социального конструирования и разрушения.

Научная группа Facebook с привлечением специалистов из американских университетов, научных центров Европы и Азии провела исследование не только на материалах Facebook, но и ряда других крупнейших сетей. Было установлено, что внутри глобальной сети существуют более-менее устойчивые субсети, или как их называют на английском – паттерны.

Оказалось, что при всем многообразии этих паттернов, в конечном счете, они образуют восемь базовых структур. В основу типологии структур положена внутренняя конфигурация паттерна, плотность связей и структура внешнего взаимодействия паттерна с глобальной сетью или другими паттернами. Под внутренней конфигурацией понимают взаимоотношения внутри паттернов между людьми с различными социальными ролями. Оказалось, и возможно это самое главное, что в каждом из восьми базисных паттернов информация распространяется различным образом и с неодинаковой скоростью. Различаются также по этим паттернам взаимоотношения между онлайн и офлайн поведением. Фактически – это ключевое открытие. Оно позволяет заметно увеличить эффективность внешнего управления групповым и массовым сознанием и поведением.

К. Марлоу, руководитель научной команды Facebook отметил, что им, вместе с исследователями Северо-Западного университета в Чикаго удалось обнаружить, что все сложные сетевые системы, например, такие как интернет, социальные сети, электросети и даже колонии термитов имеют множество сходных черт, характери-

зующих как динамику, так и статику этих систем. Более того, выяснилось, что во всех этих системах есть своего рода несущие узлы и элементы, которые образуют своего рода «скелет» сети, либо ее устойчивого паттерна. Собственно эти «скелеты» и определяют само существование сетей, паттернов. В значительной степени от них зависит жизненный цикл сети и ее устойчивость к внешним воздействиям.

Решающую роль в этой работе сыграл коллектив профессора А.Э. Барабаши. Еще в 2010 году А. Барабаши подключился к работам созданного на деньги Пентагона центра по исследованию социально-когнитивных сетей (Social Cognitive Network Academic Research Center – SCNARC). Там перед ним была поставлена задача практической проверки разработанных ранее теоретических моделей безмасштабных сетей на больших объемах реальных данных. Результатом работы А. Барабаши стала статья «Достижение социального консенсуса в результате влияния убежденного меньшинства». В работе говорилось, что при достижении в социуме пороговой границы примерно в 10% убежденных сторонников какой-либо идеи, возникает лавинообразный процесс завоевания этой идеей умов большинства членов социума. Начиная с 30% процесс становится необратимым. Но всего этого недостаточно. Нужно контролировать от 15 до 25 % драйверов сети. Отличие драйверов в том, что они не просто собирают информацию от разных людей и не просто являются источником информации для других участников сети. Их особенность в том, что они делают и то, и другое, выступая в роли коммуникаторов между группами людей и, как бы являясь информационными мостами, соединяющими изолированные островки микрообществ, из которых обычно состоит любая соцсеть. Поэтому настоящие драйверы – это не чемпионы Facebook по количеству друзей, и не чемпионы Twitter по количеству фолловеров. Это коммуникаторы, полу-

чающие информацию от одних групп людей и передающие ее другим группам. Принцип действует и в реале, и в виртуале.

Структура связей между драйверами сети в реале или в виртуале собственно и создает тот самый «скелет» сети, который выявили команды Facebook и Чикагского университета. Соответственно разрушение любой сети или сложного социального субъекта наступает не тогда, когда удается разрушить наиболее плотные связи внутри сети, а когда удается разрушить контакты между драйверами, или «скелет» сети.

Исследователи из Северо-Западного университета в Чикаго в сотрудничестве с группой из Массачусетского технологического института, установили, что для того, чтобы взять сеть или ее устойчивые паттерны под контроль и осуществлять внешнее управление ими достаточно контролировать определенный процент участников сети или паттернов. Этот процент, в зависимости от типа сетей и паттернов, колеблется в интервале от 10 до 80%. Проценты прямо определяются двумя параметрами – плотностью связей внутри сети или паттернов и степенью однородности элементов, входящих в сеть или паттерн.

Жан Жак Слотин, профессор Массачусетского технологического института отметил в этой связи, что для сетей, где элементами являются люди, т.е. социальных сетей в онлайне и офлайне, показатель контроля составляет от 9 до 15%. Практически это означает, что если контролируется информационный поток или поведение от 9 до 15% участников сети, то в значительной степени контролируется и вся сеть или паттерн. Это относится и к небольшим группам, и к социальным сетям максимального размера.

К. Марлоу в своих работах отмечает, что плотность социальных сетей гораздо выше, чем принято думать. Все хорошо знают правило шести рукопожатий. Оно гла-

сит, что любые два человека в мире увязаны через цепочку из шести человек. Это правило растиражировано и в научной, и в популярной литературе, вошло в обиход. А между тем, базируется оно всего на нескольких экспериментах, проведенных в одном городе, а именно в Бостоне во второй половине 70-х годов. Команда Facebook, используя имеющиеся данные, проанализировала сведения на совокупности, составляющей 300 млн. пользователей сети в самых различных странах мира. Выяснилось, что для 98% пользователей Facebook действует правило не шести рукопожатий, а чуть больше четырех.

К неожиданным результатам привело недавнее исследование под руководством члена научной группы Facebook Э. Бакши. Его осуществляли коллеги из университета штата Мичиган. Эксперимент назывался «Эхокамера». Суть его состояла в том, что исследовались пути распространения мемов и факторы, влияющие на отношение пользователей Facebook к тем или иным лицам, событиям, процессам. Эксперимент проводился на совокупности 80 млн. аккаунтов. С одной стороны был получен весьма ожидаемый результат, что распространение мемов зависит от конфигурации паттернов, а между паттернами решающую роль играет массовость охвата мемом участников сети в целом. Гораздо более неожиданным оказался другой вывод. До эксперимента все были уверены, что на отношения участников паттерна решающее влияние оказывает позиция по этому вопросу других его членов, или как еще их называют «близких друзей». Выяснилось, что это не так. Слабые связи, т.е. позиция сети в целом или большого его фрагмента, куда входят несколько паттернов, оказывает большее влияние, чем позиция «близких друзей». Результат был настолько неожиданный, что эксперимент был трижды повторен и дал те же результаты. Не менее удивительным оказался тот факт, что мнение в виртуале может существенно расходиться с поведением в реале. Кроме того, оказалось,

что в реале зачастую действуют несколько иные законы, чем в виртуале.

Присцилла Чан, жена Марка Цукерберга попросила его использовать возможности Facebook для увеличения добровольных бесплатных доноров крови в США. Цукерберг попросил научную группу предложить стратегию и практические инструменты реализации этой программы. При анализе результатов программы выяснилось, что при переходе из онлайна в офлайн ситуация меняется. Если на виртуальное мнение более сильное влияние оказывают слабые связи, то на реальное поведение больше воздействуют сильные связи. Фактически технология научной группы была построена на том, чтобы с одной стороны обеспечить максимально быстрое распространение мема «донор – это круто» по сети и создать этому мему климат максимального благоприятствования, а с другой стороны побудить наиболее влиятельных членов паттернов показать пример реальным поступком. Достигнуто это было путем отправления им персональных посланий за подписью Цукерберга, содержащим помимо просьбы не очень значащую, но приятную бесплатную «плюшку».

Недавно вышла публикация центра Беркмана по изучению информации и общества при Гарвардском университете. Исследование проводилось на материале мониторинга веба и непосредственно полевых работ в Тунисе, Египте, Ливии, Йемене. Было выделено три аспекта влияния социальных сетей на политические процессы, прежде всего, в арабском мире, а именно – коммуникационный, мобилизационный и информационный. Исследователи из Гарварда сделали однозначный вывод о том, что мобилизационная роль социальных сетей в событиях в противовес мнению СМИ и блоггеров была весьма невелика. Различного рода виртуальные сообщества не придали сколько-нибудь массового характера выступлениям. Решающей технологией мобилизации

стали пятничные молитвы и обращения мулл.

Коммуникационный фактор социальных сетей, безусловно, присутствовал. Более того, как было выявлено и по результатам мониторинга, и по результатам полевых исследований, он нарастал по мере развития событий. Т.е. на первом этапе коммуникация шла в основном вживую и через банальные телефоны, но дальше все чаще стали использоваться платформа Twitter и социальные сети.

Наиболее заметную роль социальные сети сыграли в части информационного освещения событий в арабском мире и во всемирном медийном пространстве. Результаты исследования убедительно показали, что сообщения в Twitter и социальных сетях оставляла ничтожно малая часть участников событий. В их число входили, прежде всего, агитаторы, или ангажированные блоггеры. Кроме того, среди них было немало и тех, кто писал то, что думал, или выкладывал видео, которые реально снимал. При этом именно сообщения ангажированных блоггеров в значительной степени использовались мировыми онлайн СМИ всех форматов и формировали информационные потоки. Частично здесь имел место фактор целенаправленного использования фрагментарной информации в целях манипулирования общественным мнением. Но главным, по мнению исследователей из Гарварда, было то, что именно такая технология формирования новостей встроена в производственные процессы мировых интернет- и офлайн-СМИ. Т.е. так произошло не только потому, что кто-то целенаправленно занимался манипуляциями, но и потому, что это соответствовало отработанным технологиям подачи новостей в режиме нон-стоп.

Широко обсуждаются результаты промежуточных исследований Института анализа социальных и политических конфликтов Джорджтаунского университета. Этот университет является одной из ведущих «фабрик мыс-

ли», обслуживающих, прежде всего, Госдепартамент и Совет национальной безопасности. Институт вот уже девять лет ведет тему «Квазитолпа в политических событиях».

Еще в прошлом веке Г. Лебон написал свою знаменитую работу о толпе. В ней сформулировано и классическое понимание толпы, как большого, в каком-то смысле даже избыточного количества людей, оказавшегося в определенное время в конкретном месте. Квазитолпа отличается от толпы тем, что представляет собой толпу, которая собралась не случайно из-за стечения тех или иных обстоятельств, либо объективных процессов, а была собрана сознательно, либо собралась в результате каких-то общественных процессов.

Уникальность этого исследования состоит в том, что феномен квазитолпы изучался не только на материале арабского мира, но и Западной Европы, конкретно, событий в Лондоне, Париже, Берлине в последние годы, США («Оккупай Уолл-стрит»). В результате исследований, которые велись с привлечением специалистов из МТИ и Северо-Западного института, выяснились очень интересные вещи. Для каждой из стран имеется свой критический порог численного состава квазитолпы, когда она начинает играть активную роль в политических, социальных и экономических процессах, прежде всего, на региональном, городском и территориальном уровнях. Этот порог зависит от численности населения в ключевых городах, культурных особенностей, национального темперамента и компьютерной вооруженности населения.

В исследовании установлено, что квазитолпа превращается в своего рода устойчивый субъект действия, способный собираться с определенной периодичностью при выполнении условий, связанных с ее структурным составом. Конкретно речь идет о следующем. Ранее считалось, что в квазитолпе четко выделяются три группы участников. Это «заводилы», выступающие организаторами квазитолпы и первыми выходящие на площади и

улицы. Вторая – «регулярные бойцы». Это – участники квазитолпы, склонные к жесткому противодействию с властью и органами правопорядка, как правило, берущие на себя основной удар при попытках сдержать или рассеять квазитолпу. Третья – «примкнувшие». Это те, кто откликается на призыв заводил, и является массовкой для бойцов. Впервые структура квазитолпы была раскрыта исследователями из Лондонской школы экономики на примере анализа движения британских футбольных болельщиков – ультрас в 70-е годы прошлого века.

Проведенные в последние годы исследования заставили посмотреть на квазитолпу несколько по-иному. Квазитолпа понимается не как простое объединение большого числа людей, а как единое целое, состоящее из людей и групп, объединенных сильными, слабыми и очень слабыми связями. Выяснилось, если в квазитолпе не менее 7-15% людей принадлежат к группам, внутри которых имеются сильные связи, то это необходимый но недостаточный фактор превращения квазитолпы в реальный фактор действия. Что это за группы? Это не организаторы квазитолпы, а люди, которые влились в нее не поодиночке, а группами, которые тесно взаимодействуют в реале и общаются в виртуале. Эти группы становятся центрами притяжения и стабилизации квазитолпы. Они же в значительной степени втягивают в себя понемногу остальных членов квазитолпы. Про эти группы было известно и раньше.

А вот третий компонент квазитолпы четко выделен впервые. Выяснилось, что в квазитолпе, которой удалось стать субъектом действия, обязательно присутствовали микрогруппы, выполняющие роль катализаторов. Их численность должна составлять от 2 до 5% от общего числа участников квазитолпы. Это люди, которые наиболее активно ведут себя в квазитолпе, а также оказываются первыми при любых конфликтах и столкновениях. Было бы упрощением, как показали результаты исследований,

всех их без исключения относить к провокаторам. Конечно, провокаторы в ряде случаев составляют большинство этой группы, но немалая часть людей, попавших в указанную категорию – это участники квазитолпы, которые по своим личностным и социально-психологическим характеристикам, культурным стереотипам и возрастным особенностям склонны к импульсивным действиям, имеют низкий порог сдерживания страхом и т.п. Исследованиям этой категории в России длительное время с успехом занимается д.ф.н. И. Сундиев. Очень интересно, что согласно анализу института, эта группа в значительной степени формируется и рекрутируется в социальных сетях. По численности они ничтожны, но последствия их деятельности очень велики. И это не удивительно, поскольку динамика квазитолпы – это чисто синергетический процесс. При таких процессах даже малые изменения могут привести к очень большим последствиям.

Имеется много свидетельств, что для того, чтобы квазитолпа превратилась в субъект действия, одних процессов самоорганизации недостаточно. Должно присутствовать внешнее управление со стороны тех, кто сам ни в коем случае не участвует в квазитолпе, а обеспечивает своего рода логистику, финансирование и т.п. Проще говоря, каждому кукольному театру нужен свой Карабас-Барабас. Хотя в реальности обычно действует не индивидуальный, а коллективный Карабас.

Значительный интерес вызвала недавняя работа Парижского центра изучения социальных, этнических и межконфессиональных конфликтов о взаимоотношениях виртуальных и реальных социальных сетей и групп в конфликтных ситуациях. Исследование имело целью выяснить вопрос, какие именно виртуальные группы быстрее всего самоорганизуются в конфликтных ситуациях и способны к согласованным действиям. В качестве материалов были использованы данные по беспорядкам в Париже, событиям прошлого года в Тунисе, футбольным

беспорядкам в центральной Германии. Было выделено три типа групп: полностью виртуальные группы, которые до событий не имели между собой никаких контактов в реале, смешанные группы, где часть людей взаимодействовала в реале и все взаимодействовали в социальных сетях и, наконец, реальные группы, все члены которых многократно пересекались и взаимодействовали в реальном мире.

К некоторому удивлению исследователей выяснилось, что наибольшей способностью к самоорганизации обладают не реальные, как это предполагалось до сих пор, а смешанные группы. Под самоорганизацией имелась в виду способность людей на месте события быстро идентифицировать себя как единое целое и, кроме того, увеличивать численность группы за счет включения в нее других участников конфликтов или беспорядков. Оказалось, что реальные группы быстрее всех переходят к действиям, но с трудом коммуницируют с толпой на месте конфликтов или беспорядков. В то же время смешанные группы немногим уступали реальным группам в скорости перехода к тем или иным активным действиям, намного превосходят их по способности вбирать в себя неорганизованных участников конфликтов и беспорядков и просто людей, оказавшихся в это время в соответствующем месте.

Далее исследователи выяснили, что во всех странах наблюдения в смешанных группах наиболее авторитетные их члены связаны между собой не только виртуальными, но и реальными взаимодействиями. При этом число участников смешанной группы, имеющих устойчивые реальные взаимодействия, колеблется, как правило, в интервале от 10 до 25% от общей численности группы.

Международный центр практик краудсорсинга при стихийных бедствиях опубликовал данные аналитики, которую они провели по отражению в социальных сетях и Twitter наводнения в Новом Орлеане, землетрясения

на Гаити, катастрофы вокруг Фукусимы и наводнений в результате разливов Красной реки.

Аналитику для центра вели специалисты Университета И. Лойолы, который, кстати, является поставщиком кадров для разведсообщества, при поддержке лаборатории аналитических методов обработки неструктурированный информации Стэндфордского университета. Было выявлено два новых неожиданных и технологически очень интересных обстоятельства.

Во-первых, оказалось, что социальные сети имеют различную пропускную способность в зависимости от оценочной окрашенности информации. Давно и хорошо известно, что наиболее рейтинговыми передачами на телевидении оказываются различного рода шоу, соревнования и т.п., имеющие, несомненно, положительную окрашенность, несущие позитивные эмоции. В социальных сетях, напротив, скорость распространения и широта охвата негативной информации в 2-2,6 раза превышает аналогичные показатели для позитивных новостей и сообщений. Данные цифры получены впервые и естественно в ближайшее время будут осмыслены и с военных, и с политических, и с коммерческих позиций.

Во-вторых, выяснилось, что люди, оказавшиеся в зоне стихийных бедствий, как это не удивительно, используют социальные платформы и социальные сети достаточно неожиданным образом. До проведения исследований и эксперты, и практики были убеждены, что социальные платформы и сети в зонах бедствия и экстраординарных событий используются, прежде всего, для того, чтобы подать призывы о помощи, просигнализировать властям или добровольческим организациям о необходимости предпринять усилия для спасения тех, кто выходит с соответствующими сообщениями. Оказалось, что такие сообщения составляют по различным регионам от 27 до 38% от общего числа осмысленных сообщений. При этом наибольший удельный вес призывов

о помощи имел место на Гаити и при разливах Красной реки. Наименьший – в Японии.

Самыми распространенными сообщениями, на которые приходилось от 40 до 52% от общего количества осмысленных сообщений составили твиты и записи в социальных сетях, которые имели своей целью сообщить родным и близким о своем местоположении и самочувствии и наладить с ними эффективное взаимодействие. Фактически речь идет о том, что эти сообщения имели своей целью запустить процессы самоорганизации групп, находящихся в зонах стихийных бедствий. Причем, состав этих групп входили люди, как правило, имеющие тесные связи в реале, либо устойчивое взаимодействие в виртуале. В общем, оказалось, что старая и вечно молодая фраза из еще советского фильма: «Спасение утопающих – дело рук самих утопающих» как нельзя лучше отображает реалии вне зависимости от географической локализации. Наконец, третью группу сообщений составила информация о состоянии инфраструктуры в зонах стихийных бедствий. Как показал дальнейший анализ, эта информация по всем проанализированным районам оказалась на порядки более точной, чем передаваемая в то же время в онлайн режиме информация со стороны государственных и других официальных структур.

Недавно известный американский социолог и психолог П. Голвиттцер опубликовал переиздание книги «Символическая самореализация». В ней впервые на суд экспертов и практиков были представлены результаты более чем семилетних экспериментов, характеризующих взаимоотношения между высказанными намерениями и практически реализованными действиями. Исследования охватили почти 50 тыс. человек в Америке, Европе и Азии. Вне зависимости от региона, культурной принадлежности и возраста, выяснилось, что те, кто хранил свои намерения при себе, были более склонны

их достигать, чем те, кто оглашал их и при этом получал высокую оценку от других.

Профессор психологии Нью-Йоркского университета П. Голвиттцер выяснил, что намерение, будучи высказанным и оцененным, формирует самооценку человека и снижает побудительные мотивы к практическим последующим действиям. Поскольку профессор начал свои эксперименты еще в 1982 г., в доинтернетную эру, ему удалось посмотреть на динамику расхождений между намерениями и действиями во времени. Он выяснил, что это расхождение стремительно нарастает и строго коррелируется с повышением доступности интернета и распространением социальных сетей. Отсюда П. Голвиттцер сделал вывод, что социальные сети имеют еще один неожиданный аспект. Для значительной части населения они выступают как своеобразная машина «забалтывания», блокирования действий за счет коммуникации и одобрения со стороны сообщества высказанной точки зрения. Получив одобрение, люди в некоторой степени теряют побудительные мотивы для осуществления практических, подчас связанных с риском или неприятностями действий.

Как явствует из материалов проведенных в последнее время конференций с участием ведущих американских и британских исследователей, политиков, военных, представителей разведывательного сообщества, бизнеса сложилась четкая точка зрения, что любыми социальными сетями, сообществами и группами можно эффективно управлять, если знать закономерности формирования и динамики, а также характеристики групп любых масштабов и структур. На страницах ведущих американских СМИ мелькает применительно к синтезу технологий Больших Данных и сетевых исследований эпитет «новая ракетная наука». На американском политическом сленге «новая ракетная наука» – это сфера науки и технологий, способная обеспечить максимальные разрушительные

и созидательные эффекты, а также имеющая двойное применение, и в военной, и в гражданской областях.

В этой связи хотели бы отметить следующее. Вряд ли стоит ожидать в ближайшие годы появления обобщенного труда, типа известных работ Д. Шарпа и Д. Ная. По сути, речь идет о полусекретных разработках. Однако, в силу особенностей финансирования американской науки, практически все значимые результаты исследований публикуются в открытой печати, как правило, в платных научных журналах, размещенных в так называемом «невидимом» интернете. В этой связи важнейшей практической задачей является каждодневный мониторинг таких публикаций, их своевременная оценка, классификация, включение новых методов в общесистемный арсенал цифровых социумных вооружений и опережающая разработка средств борьбы с новыми угрозами.

### 3.3. Прогностические вооружения и Большие Данные

Прогнозирование в сфере высшей политики, экономики и военного дела всегда имело амбивалентную, а по-русски говоря, двойственную природу. С одной стороны прогнозирование являлось важнейшей стадией разработки ключевых стратегических, тактических и оперативных решений тех или иных проблем и задач, разработки и реализации крупных проектов и военных компаний. С другой стороны, прогнозирование, подкрепленное мощным информационно-пропагандистским аппаратом, само по себе выступало как своеобразный вид вооружения, способ формирования будущего.

После знаменитых экспериментов американского социолога У. Томаса, прогнозы, подкрепленные соответствующим информационным воздействием, сами по себе формируют реальность. Как гласит теорема Томаса: «Если человек определяет ситуацию как реальную, она – реальна по своим последствиям». Другой американский

социолог, а по совместительству советник администраций нескольких президентов Р. Мертон на основе теоремы Томаса опубликовал статью «Самоисполняющиеся пророчества». Самоисполняющееся пророчество – это ложное определение ситуации, вызывающее новое поведение, которое превращает первоначально ложное представление в реальность. Таким образом, теорема Томаса вкупе с технологией Мертона позволяют использовать прогнозирование как мощное оружие в социодинамике, психоинжиниринге, военном деле и бизнесе.

Поэтому вполне очевидно, что с развитием интернета и появлением Больших Данных, представляющих собой, в том числе и огромный поведенческий архив, возникло желание максимально использовать открывающиеся возможности для разработки прогностических вооружений.

При этом к началу нулевых годов профессионалам, работающим в этой сфере, были ясны, по меньшей мере, три фундаментальных положения:

• во-первых, используя самые изощренные и эффективные методы, можно прогнозировать процессы, но не события;

• во-вторых, прогнозы с высокой степенью вероятности можно делать в отношении групп различной размерности, но не отдельных индивидуумов;

• в-третьих, знания о действиях групп и индивидуумов в одной ситуации не позволяет давать точные прогнозы о подобных действиях, осуществляемых в другой ситуации.

Соответственно, оказалось, что различного рода прогнозы, базирующиеся на традиционных выборках, построении сценариев, экстраполяции попросту не работают.

Развитие интернета дало возможность оперировать Большими Данными относительно человеческого поведения, намерений, желаний и т.п. В этой связи специа-

лист номер один в мире по интеллектуальному анализу данных Г. Пятецкий-Шапиро писал: «Прогнозирование на основе Больших Данных состоит в извлечении нетривиальных выводов из заранее известных характеристик, признаков и сведений об объектах».

Использование интернета, как огромного, пополняемого в режиме он-лайн поведенческого архива для прогнозирования развивается по трем ключевым направлениям:

• первое – это прямой интеллектуальный анализ общедоступных данных, предоставляемых поисковыми системами и различного рода социальными сетями и платформами;

• второе – это создание рекомендательных систем, которые прогнозируют различного рода выбор субъектов и групп, и на этой основе рекомендуют им что угодно – от книг до кандидатов в президенты;

• третье – это сложные прогностические системы, использующие разнородные данные, получаемые из открытой и закрытой части всемирной сети, обрабатываемые с помощью всего арсенала интеллектуального анализа данных.

Исторически главный упор был сделан на работу с общедоступными интернет-данными из социальных сетей и поисковых машин. Еще два-три года назад никто не мог помыслить о том, что инструменты веб-прогнозирования будут в благожелательном ключе обсуждаться на сайте головного банка ФРС. Но это произошло. Первым делом, как всегда бывает, за дело взялись академические исследователи, которые в Америке очень даже прагматически настроены и заинтересованы в максимально быстром внедрении их научных разработок в практику. В октябре 2010 г. в кругах инвестиционных аналитиков прогремел доклад Johan Bollen, Huina Mao (Indiana Unviersity), Xiao-Jun Zeng (The University of Manchester) «Twitter mood predicts the stock market».

Ими была сделана программа, которая позволяла использовать сообщения Twitter для прогнозирования движения индекса Dow Jones. Алгоритм работал следующим образом – отбирал из всех Twitter сообщений в режиме реального времени сообщения, маркированные определенными словами, затем удалял эмоционально окрашенные сообщения и на основе обработки нейтральных, эмоционально не окрашенных сообщений выдавал прогноз. Выяснилось, что он позволил предсказывать движение индекса на срок от двух до шести дней с точностью почти до 88%.

Большое признание в последнее время в Америке получили разработки Р. Петерссона, исследователя из Стэндфордского университета. В качестве неструктурированных данных для прогнозирования он использовал не Twitter, а контент социальных СМИ, т.е. платформ, где контент создают сами пользователи. Таких платформ с качественным контентом в англоязычном интернете насчитывается сотни.

Его исследования были восприняты компанией MarketPsych. Был создан прогностический модуль. Он уверенно дает при достаточно консервативной стратегии 30% прибыли в год. В настоящее время эта компания приобретена крупнейшим информационным провайдером, всемирно известным Thompson Reuters. Соответственно прогнозы получают подписчики Thompson Reuters, интересующиеся инвестиционной и политической тематикой.

Совсем недавно за разработку системы, аккумулирующей информацию Twitter для трейдинга, взялась компания Titan Trading Analytics. В своей системе они используют 1500 ключевых слов и более 600 факторов. Как видим, создание и практическое использование программ прогнозирования, базирующихся на неструктурированных данных web 2 и прежде всего Twitter, стало

сегодня повсеместной практикой инвестиционных, макроэкономических и политических аналитиков.

Огромную роль в современном геополитическом, военном и инвестиционном прогнозировании играют общедоступные данные, связанные с частотой поисковых запросов, которые постоянно публикуют главные поисковики мира, прежде всего, Google и Bing. В нынешней реальности любой поисковый запрос представляет собой фиксацию процесса мышления о чем-то. Он показывает нам объект этого мышления, его последовательность и многое другое. Когда интернет с одной стороны стал доступен для подавляющего большинства жителей в развитых странах в режиме онлайн нон-стоп, а с другой, пользователи приучились к интернету, как к источнику мгновенного получения любой интересующей информации, использование поисковиков для прогнозирования стало возможным.

К настоящему времени независимыми группами исследователей, использующих различные методы и алгоритмы обработки поисковых запросов в целях прогнозирования установлено, что особым образом обработанная статистика поисковых запросов может выполнять роль опережающих индикаторов для целого ряда рынков и экономических параметров. В частности, это относится к динамике безработицы в США, Германии, Франции; динамике потребительских расходов на рынках электроники США, странах ЕЭС, Канаде; ценам на недвижимость США и Великобритании; биржевым индексам на «голубые фишки» на Нью-Йоркской и Лондонской биржах и фьючерсам на биржевой индекс китайских акций на Гонконгской бирже.

Уже полгода Министерство здравоохранения США успешно использует систему, построенную на анализе поисковых запросов для опережающего мониторинга и прогнозирования различного рода эпидемий в стране. На сегодняшний день обнаружено более 50 показателей,

относительно которых поисковая статистика Google может быть использована как опережающий индикатор.

Вторым, бурно развивающимся направлением прогнозных вооружений, являются так называемые рекомендательные системы. Эти системы базируются на тщательном анализе поведения человека в сети. При этом анализируются не только его желания, высказанные в виде различного рода поисковых запросах, но и поведение на сайтах крупных интернет-магазинов – например, что человек ищет, как долго рассматривает что-либо и т.п. Используется здесь так называемый неявный сбор данных, когда все действия человека в сети протоколируются. Затем, на основе сложных алгоритмов выдаются рекомендации, которые подталкивают человека к тому или иному выбору. Наиболее известные рекомендательные системы созданы Amazon для книг и других товаров, продаваемых на этой универсальной платформе, eBay, Cinemax.com (рекомендации в отношении фильмов, демонстрируемых в кинотеатрах), Videoguide (для потокового видео) и т.п.

Во время последней избирательной кампании команда Б. Обамы, договорившись с крупнейшими рекомендательными платформами, успешно использовала их опыт для рекомендации Б. Обамы в качестве лучшего выбора для выявленных опять же по специальным алгоритмам колеблющихся избирателей и людей, которые вообще не собирались идти на выборы. По оценкам американских экспертов использование этой системы сыграло едва ли не решающую роль в победе Б. Обамы в кампании 2012 года.

Сегодня крупнейшие банки являются клиентами рекомендательной германской компании Kreditech. Гамбургский стартап Kreditech использует во время принятия решений информацию, почерпнутую из Facebook. Людей, претендующих на получение кредита, просят на время предоставить доступ к их учётной записи в

Facebook или других социальных сетях. По словам Александра Граубнера-Мюллера, одного из основателей фирмы, список ваших друзей выдаёт немало. Претендент, приятели которого прилично зарабатывают и живут в хороших районах, имеет больше шансов на кредит. Претендент, знакомый которого отказался возвращать деньги, занятые у Kreditech, ничего не получит.

В качестве одного из наиболее ярких примеров сложных прогнозных систем можно привести проект Recorded Future. В январе 2010 года проект Recorded Future был запущен за счет инвестиций Google, инвестиционного фонда американского разведывательного сообщества In-Q-Tel и собственных вложений К. Альберга – основателя проекта, в прошлом шведского разведчика и известного программиста.

Recorded Future базируется на трех основных блоках:

• Встроенном поисковике третьего поколения. В первом поколении были системы типа Yahoo и HotBot. Они искали просто те или иные слова в документах и выдавали документы в произвольном порядке. Поэтому такого рода поисковики сопровождались каталогами, формировавшимися в основном экспертами на основе поисковой выдачи. Нечто подобное можно до сих пор увидеть на первой странице Rambler. Вторым поколением стал Google. Революция Брина-Пейджа состояла в том, что поисковик стал искать не только по документам, но и в значительной степени по связям между документами или сайтами. Третье поколение ищет не только объекты, соответствующие поисковым запросам, не только связи между документами, но и взаимосвязи между объектами, их характеристиками и отношениями, содержащимися в различных документах. Сегодня это главное направление развития поиска. Оно в полной мере реализовано в Recorded Future.

• Разделении информационного поля на составляющие. В Recorded Future выделено три класса сообщений.

Первый – это сообщения о событиях. События – это длящиеся определенный, достаточно небольшой период времени устойчивые конфигурации, которые характеризуются единством времени, места, участников и т.п. К событиям Recorded Future относит то, что может быть интерпретировано как факты, то, что реально произошло или происходит в данный момент. Второй – это мнения. К мнениям относятся любые сообщения относительно прошлых, настоящих или будущих событий, высказанные в авторитетных источниках, либо авторитетными людьми. В системе есть специальные алгоритмы, которые позволяют для каждой области выделить большую выборку таких источников и персон. Наконец, третий – это реакции. Здесь принимаются во внимание любые спонтанные реакции людей на те или иные ожидаемые события, зафиксированные в различного рода текстовых сообщениях. Не обязательно, чтобы эти сообщения были из авторитетных источников. Главное, чтобы они имели отношение к событиям и мнениям, так или иначе рассматриваемым и высказываемым в авторитетных источниках. Такое разделение на три сегмента информационного поля, как выяснилось, позволяет достаточно хорошо улавливать как господствующие тенденции и опережающим образом реагировать на их изменения, так и выявлять слабые сигналы.

• Рассмотрении интернета, как огромной распределенной сетевой базы неструктурированных данных. Еще у древних греков были знаменитые Мойры, которые пряли нити судьбы, образующие ткань реальности. Сестер было три. Первая олицетворяла, как мы теперь говорим, тренды. Вторая – случайности. Третья – неотвратимость последствий поступков и решений. Собственно Recorded Future использует поисковик, работающий в сегментированном информационном пространстве в масштабе огромной сетевой базы данных. В сетевой базе данных разные объекты и их характеристики связаны друг с дру-

гом прямыми, обратными и опосредованными связями. Соответственно, такой подход позволяет выявлять не только явные и очевидные связи, но и вести так называемый латентный анализ, т.е. получать неочевидные, а иногда даже и абсолютно не предполагаемые связи и отношения. К тому же обрабатывать огромное количество информации в алгоритмическом режиме. Т.е. оперировать информационными массивами, непосильными для непосредственной обработки человеком.

В настоящее время Recorded Future используется в трех сферах: государственной разведке и безопасности, в бизнесе, и в финансах для разработки инвестиционных стратегий.

Другим ярким примером прогностических систем нового поколения является платформа Quid. Эта система создана известным американским программистом и разработчиков Ш. Горли на деньги знаменитого Питера Тиля, чья разведывательная программа Palantir является любимым инструментом американского разведывательного сообщества.

Quid занимается прежде всего научно-техническим прогнозированием, поиском тех ниш, которые могут дать максимальный эффект с точки зрения развития технологий в любых сферах, включая сферу вооружения. Одновременно система может быть использована как своего рода организационное оружие, поскольку выявляет, образно говоря, технологические дыры в потенциале любой страны мира. В качестве материала для прогнозирования программа использует Большие патентные Данные, т.е. миллионы файлов, входящих в патентные базы по всем странам мира, а также информацию, почерпнутую из научно-технических, технологических журналов и средств массовой информации.

В основе системы лежит простая, но очень эффективная мысль. Впервые она была высказана более 50 лет назад знаменитым польским мыслителем и фантастом

С. Лемом. Идея состоит в том, что техника развивается примерно по тем же законам, что и живая природа. Как известно, в живой природе существует такая ключевая единица, как биоценоз, в который входят различного рода живые виды, составляющие пищевые цепочки, системы взаимодействия и в совокупности полностью заполняющими природный ландшафт. С. Лем предположил, что то же самое происходит в технике. И назвал это техноценозом. Система Ш. Горли обнаруживает такие техноценозы, ищет в них пустые, незаполненные места. Именно эти пустые места оказываются точками роста, где появляются наиболее эффективные и одновременно наиболее прибыльные технические и технологические решения. С другой стороны, если это пятно не будет заполнено, то система техноценоза будет уязвимой, неустойчивой и плохо приспособленной к дальнейшему развитию. За 2,5 года работы компании Ш. Горли ее клиентами стали ведущие американские корпорации, разведывательные и военные структуры.

Таким образом, Большие Данные обеспечили появление новых, на порядки более эффективных, чем раньше, методов прогнозирования научно-технических, инженерно-технологических, инвестиционных, политических, социальных и военных процессов. Эти методы в совокупности с методиками глубокого анализа на основе все тех же Больших Данных позволяют говорить о создании принципиально нового вида вооружений, а именно – прогностических вооружений. Они могут быть использованы как обеспечивающий механизм для разработки и применения традиционных вооружений, так и при определенных условиях, о которых расскажем в следующих статьях, как отдельный, принципиально новый вид вооружений. Более того, они становятся своего рода основой Shadow Power или невидимой силы, которая идет на смену мягкой силе.

### 3.4. Большие Данные, фруктовые салаты и Большой Брат

Американская психология в отличие от направленности этой науки в других странах мира, прежде всего, в континентальной Западной Европе, России, Великобритании, отличалась подчеркнуто практическим характером. Фактически с первых дней существования на американском континенте, психология сразу же была взята на вооружение рекламистами, политическими пропагандистами и маркетологами. Они рассматривали ее как поставщика инструментов для решения каждодневных, практических задач. Инструментальная направленность американской психологии в значительной мере привела к тому, что ведущие университеты старались заполучить к себе уже известных, прежде всего в Европе, исследователей. Цель была не в том, чтобы создавать научные школы, а использовать уже имеющиеся наработки.

Собственно, таким образом родилось едва ли не господствующее направление в американской психологии, так называемый бихевиоризм. В переводе на русский оно означает науку о поведении. Наиболее яркие фигуры бихевиоризма Дж. Уотсон и Б. Скиннер, не скрывали, что их разработки имеют в основе труды российской психофизиологической школы и, прежде всего, И.П. Павлова, И.М. Сеченова и В.М. Бехтерева.

Бихевиористы считали, что с практической точки зрения бессмысленно использовать различного рода тесты, наблюдения за внутренним миром человека и т.п. Они исходили из того, что базироваться можно только на объективных, т.е. наблюдаемых данных, которые к тому же должны иметь количественное выражение. Бихевиористы полагали, что каждому стимулу соответствует строго определенная реакция человека.

На практике дело оказалось, естественно, более сложным. В своем дальнейшем развитии бихевиористская школа стала учитывать не только реакции челове-

ка на те или иные стимулы, но и ситуации, в которых он действует. Наряду с этим, благодаря Курту Левину, бихевиоризм обогатился таким важным элементом, как открытие канального, или тоннельного эффекта. Смысл этого эффекта достаточно прост. Оказалось, что для каждой группы людей существуют внешне незначительные факторы, стимулы или другие характеристики, воздействуя на которые можно добиться заметного изменения в поведении, в том числе в отношении значимых его параметров. Этот вывод был проверен на тысячах добровольцев в сотнях экспериментов.

Наконец, с широким развитием так называемых когнитивных исследований в бихевиоризм пришло понимание того, что люди совершенно по-разному думают в зависимости от уровня сложности и непривычности ситуаций, в которых они оказываются. Одновременно выяснилось, что реальный человек не похож на классического рыночного человека, который все выборы осуществляет рационально, на основе соизмерения плюсов и минусов, доходов и затрат. Человек, особенно в простых, привычных ситуациях, действует в соответствии со стереотипами и сложившимися поведенческими моделями, а, отнюдь, не исходя из детальных экономических расчетов. Что же касается сложных ситуаций, то там в основе выбора лежат опять же не расчеты, а прошлый жизненный опыт, ценности и другие трудно считаемые факторы.

В 70-90-е годы поведенческая психология начала активно использоваться в экономических исследованиях. Появилась так называемая поведенческая экономика. Сегодня это одно из главных направлений не только теоретической мысли, но и политике на государственном уровне, принимаемых решений в частном секторе. Одним из первопроходцев применения поведенческой экономики к финансам стал Джордж Сорос. В теоретическом плане за достижения в области поведенческой

экономики Нобелевские премии получили Д. Канеман, Дж. Акерлоф и в 2013 году – Р. Шиллер.

Было бы удивительным, если бы поведенческая экономика, ставшая мейнстримом в маркетинге, рекламе, в финансовом и инвестиционном анализе и т.п. не пришла бы в политику. Решающий шаг в создании поведенческой политики был сделан двумя американскими профессорами, Кассом Санстейном и Ричардом Талером. В 2009 году они опубликовали книгу «Подталкивание: как улучшить решения, касающиеся здоровья, достатка и счастья» (Thaler, Sunstein. Nudge: Improving Decisions About Health, Wealth and Happiness).

Ключевое понятие книги, вынесенное в ее заголовок, – «подталкивание» («Надж») – практически мгновенно вошло в лексикон политиков, юристов, психологов, бизнесменов и т.п. Его стали использовать как для обозначения поведенческой политики, так и сформировавшегося на его основе нормативного подхода к государственному регулированию. Смысл нормативного подхода, сформулированного в книге-манифесте, достаточно прост: «Мы знаем, как сделать вашу жизнь счастливее».

Крайне примечательным является то обстоятельство, что авторами книги были не рядовые американские профессора, а ключевые люди из окружений Барака Обамы и Дэвида Камерона. После опубликования книги К. Санстейн весь первый президентский срок Б. Обамы являлся ключевым лицом в его администрации, а в ходе второго срока был назначен в комиссию по реформе АНБ, состоящую всего из пяти человек. Что же касается Р. Талера, то с 2010 года он является советником премьер-министра Великобритании Д. Камерона.

Что же за магическая технология, этот «Надж»? Он является своего рода квинтэссенцией поведенческой политики, или как ее называют в Америке «нового патернализма». В ее основе лежит тривиальная мысль, что человек – не робот и решения принимает не на основе

соизмерения затрат и результатов, а под воздействием многих факторов, включая эмоции, настроения, привычки и т.п. Однако К. Санстейн и Р. Талер не остановились на азах поведенческой экономики, а интегрировали их с другими научными и технологическими достижениями.

Прежде всего, они обратились к достижениям нейропсихологии. Нейропсихологам хорошо известно, что масса мозга составляет примерно 2% от массы тела. Однако он потребляет в спокойном состоянии до 10% всей энергии организма. Это происходит, когда человек бездумно серфит в интернете, пьет кофе или болтает с друзьями.

Когда человеку необходимо решить задачу, которая требует размышлений, мозг потребляет до 25% энергии. А если стоит не обычная задача, а сложная проблема, то расход энергии увеличивается до 35%. Строго говоря, думать – это очень энергозатратное, и с точки зрения биологического функционирования, зачастую неоправданное занятие.

Поэтому подчас желаемым состоянием человека является лень. И лишь при необходимости он вынужден действовать, а уж тем более, напряженно думать. Однако жизнь устроена так, что думать человеку приходится практически всегда. Чтобы разрешить противоречие между энергетически выгодной ленью и необходимостью мыслить для того, чтобы существовать, а иногда и выживать, человек вооружается привычками, стереотипами, шаблонами действий, поведенческими паттернами и прочими автопилотами. Как говорится, живет «на автомате».

Но, живя «на автомате», человек стремится к удовлетворению своих главных потребностей и получению удовольствий. Поэтому поведенческие стереотипы каждого человека формируются так, чтобы как можно чаще получать удовольствия, и как можно реже сталкиваться с неприятностями и опасностями, а также необходимостью решать сложные проблемы.

К. Санстейн и Р. Талер не ограничились при построении своего метода исключительно достижениями психологии и нейронаук. Как раз к моменту написания их книги начался бум Больших Данных. При этом быстро стало понятно, что Большие Данные тем Больше, чем больше характеристик того или иного объекта, субъекта и т.п. они охватывают, чем больше параметров, характеристик содержится в Данных, и чем чаще эти Данные собираются.

Сегодня в Америке имеется несколько провайдеров данных о людях, социальных группах и компаниях. Крупнейший из них, Acxiom имеет полный набор данных более чем на 500 млн. человек, включая большинство взрослых американцев и жителей других стран. Общее число параметров цифровой личности каждого человека, включенного в базу компании, в среднем составляет в США около 50.

Однако, самый большой провайдер данных – это американское правительство. Официально это – финансовые, налоговые службы, системы медицинского страхования и т.п. В имеющихся у государства и крупнейших частных провайдеров данных содержится практически все. От номеров социального страхования и водительского удостоверения до историй болезни и взаимоотношений с кредитными учреждениями. От девичьей фамилии матери до перечня мелких административных правонарушений. Третьей составляющей технологии К. Санстейна и Р. Талера стало использование Больших Данных в виде поведенческого архива, т.е. интернета. Как сказал уже упоминавшийся автор триллеров Майкл Маршалл Смит: «Цифровые следы, в отличие от следов на земле, остаются навечно».

Фактически интернет, помимо многого другого, является еще и всеобъемлющим цифровым поведенческим архивом, в котором зафиксирована активность людей в Сети за многие годы. При этом в архиве содер-

жатся данные как о практических действиях, включая различного рода поездки, покупки, обращения к врачам и т.п., так и мысли в виде текстов и, наконец, даже намерения и эмоции, материализованные в коротких записях в социальных сетях, в текстах электронных писем и т.п. Этот архив имеет распределенную архитектуру. Его составные блоки имеются у поисковиков, у владельцев социальных сетей, в крупнейших интернет-магазинах, интернет-сервисах и, конечно же, у структур американского правительства, прежде всего, в АНБ.

Наличие огромного всеобъемлющего поведенческого архива позволило компаниям – владельцам Больших Данных использовать их для предсказания поведения. Проиллюстрируем это широко известной в Америке историей. Однажды в магазин крупнейшей торговой сети Target зашел мужчина и потребовал вызвать менеджера. В своих руках он сжимал огромную кипу купонов магазина, полученных его дочерью.

«Моя дочь получила это по почте! – прокричал он. – Она еще в школу ходит, а вы посылаете ей купоны на детскую одежду и памперсы? Да как вы смеете! Вы хотите таким способом побудить школьниц рожать?»

Менеджер посмотрел на пачку купонов на материнскую одежду, детскую мебель – действительно, они были адресованы дочери рассерженного мужчины. Менеджер принес свои извинения.

Через несколько дней он позвонил мужчине, чтобы еще раз извиниться. По телефону голос отца звучал растерянно. «Знаете, я серьезно поговорил с дочерью, и выяснилось, что в моем доме происходило то, о чем я совершенно не догадывался. Она рожает в августе. Примите мои извинения».

Поэтому Target поставил перед отделом прогнозной аналитики задачу: определить, какая из покупательниц ждет ребенка до того, как это станет очевидно. Проанализировав покупательские привычки беременных жен-

щин, аналитиками была разработана система прогнозирования беременности.

Представим себе ситуацию: молодая женщина заходит в магазин и покупает лосьон с кокосовым маслом, сумку для прогулок и ярко-голубой плед. Программное обеспечение в Target выдаст свой вердикт: вероятность беременности этой покупательницы – 87%. Данные поступают маркетологам, и теперь Target начнет формировать ее привычки и управлять ими: пришлет ей купон со скидкой на детскую кроватку, присыпку, детские бутылочки и т.д. Причем это будет выглядеть ненавязчиво, чтобы не вызвать волну негодования за «шпионаж»: скидки на товары для детей помещаются среди скидок на другие товары.

«Подталкивание» («Надж») представляет собой использование поведенческих стереотипов, психофизиологических реакций и Больших Данных для целенаправленной коррекции поведения тех или иных конкретных социальных, имущественных, возрастных и т.п. групп. Для коррекции поведения используется открытый Куртом Левиным канальный, или тоннельный эффект. Выбор тех или иных факторов воздействия, которые обеспечивают реализацию этого эффекта, осуществляется на основе предсказательной аналитики и Больших Данных. В бизнесе это используется для увеличения продаж. А в политике, например, для прямого воздействия на электоральное поведение, как во время последних президентских выборов в США.

Прежде чем применить свою технологию на государственном уровне, К. Санстейн и Р. Талер опробовали ее в экспериментальном порядке. Известно, что чипсы, булочки и шоколадки вредны для растущего детского организма. Также не секрет, что, в общем и целом, школьники скорее возьмут на обед пакет вредных чипсов, чем полезный овощной салат. И любые прямые запреты окажутся недейственными, и будут обойдены. Между тем,

известно, что выбор потребителей зависит от того, как расположены продукты на полках магазина. Попробуйте заставить школьников есть фрукты вместо чипсов. Невозможно? Можно. Главное, правильно использовать лень и поведенческие стереотипы.

Так, почему бы не воспользоваться этим обстоятельством, и не разложить в школьных кафетериях фрукты и салаты на уровне глаз школьников, а чипсы и булочки – в самых дальних углах, на нижних и верхних полках прилавков, куда надо нагибаться и подтягиваться. Когда К. Санстейн и Р. Талер провели массовые эксперименты в школах Вашингтона, Нового Орлеана, Сиэтла и Коламбуса, оказалось, что в поединке между ленью и вожделением в значительном числе случаев победила лень. В течение трех месяцев более половины школьников отказались от чипсов, и перешли на салаты, фрукты и другое полезное питание.

Затем работа была перенесена в онлайн. Р. Талер стал консультантом британского правительства и при помощи «подталкивания» вывел из тупика застопорившуюся пенсионную реформу в стране. Великобритания, подобно другим странам, столкнулась с растущим дефицитом в пенсионной системе и была вынуждена перейти к накопительной системе начисления пенсий. Однако, получив свободу выбора, значительная часть граждан не стала откладывать на старость, и проблема еще больше обострилась. Тогда по предложению созданной правительством поведенческой команды во главе с Р. Талером, после анализа Больших Данных была сформулирована рекомендация. Суть ее состояла в том, что компании должны автоматически включать работников в накопительную пенсионную схему, предоставив им право при желании отказаться от нее. Англичане решали, какой пенсионный план выбрать, при помощи портала пенсионной реформы.

До рекомендаций Р. Талера человек должен был сначала прочитать длинные рекомендации, написанные не всегда понятным для простого человека языком, а затем самостоятельно поставить галочку против выбранного варианта. Р. Талер предложил изменить ситуацию. Место рекомендаций заняли короткие, изложенные ясным слогом разъяснения плюсов и минусов каждого варианта, а галочку человек доложен был ставить, если он отказывался от накопительного варианта и выбирал другой из нескольких предложенных. Накопительный вариант стал выбором по умолчанию. Казалось бы, и в первом, и во втором случае за гражданами оставалась свобода выбора. Но с практической реализацией рекомендаций Р. Талера число граждан, перешедших на накопительную схему, значительно возросло. Лишний раз подтвердилось, что поведение человека зависит не только от самой по себе дилеммы выбора, а и оттого, как она формулируется и в каких условиях реализуется.

Летом 2013 года объявлено, что команды по использованию «Надж» создаются в большинстве министерств США, связанных с социальными вопросами. На них возложена задача «подталкивания» американцев к правильным с точки зрения правительства решениям не на основе объяснений, а путем использования поведенческих стереотипов, привычек и психофизиологических реакций. При этом американские СМИ высказали подозрение, что команды «Надж» создаются и в других, в том числе, разведывательных ведомствах. Однако их финансирование реализуется через секретные статьи бюджета, и поэтому их существование не афишируется.

Профессионалы «Надж», развивая поведенческую политику, исходят из нескольких основных принципов:

1. Для решения своих поведенческих проблем люди нуждаются во вмешательстве третьих лиц. Наилучшим кандидатом на эту роль является государство.

2. Эксперты, изучая то влияние, которое в реальной жизни оказывают на благосостояние те или иные акты выбора, принимают от имени индивидов решения лучше тех, на которые индивиды способны сами.

3. Любые стимулирующие схемы, которые возлагают на людей ответственность за последствия их прошлых действий, неэффективны. Вместо них необходимы схемы, которые немедленно вознаграждают или наказывают людей за будущие последствия их текущих действий – последствия, которые сами они неспособны осознать и учесть.

4. С точки зрения политики то, как люди ощущают себя в обществе, важнее того, что они желают, или того, что они делают.

Фактически, сегодня в Великобритании и США реализуется концепция подлинного Большого Брата. На уровне государственной политики реализуется принцип: правительство лучше знает, что хорошо, а что плохо для людей, и поэтому вправе незаметно подталкивать их к тем решениям, которые оно считает правильными. Ключевую роль в этой технологии играют Большие Данные. Именно Большие Данные позволяют как угодно, в зависимости от поставленной задачи проводить классификацию групп и ситуаций, осуществлять анализ и прогноз, а главное, искать тоннельные или канальные факторы, обеспечивающие нужное поведение целевых групп в конкретных ситуациях. И, наконец, в режиме онлайн отслеживать эффективность подталкивания.

В отличие от многих других технологий, «Надж» не слишком широко рекламируется. Можно говорить о том, что правительства стараются сохранить полную монополию на эту технологию, не допустить ее широкого распространения в коммерческом секторе. Б. Обама как-то даже назвал группу специалистов по «Надж», подготовленную К. Санстейном, бихевиористской командой мечты, способной решать важнейшие государственные

задачи. Кстати, эта команда сыграла заметную роль во второй президентской кампании Б. Обамы на выборах 2012 года.

Следует подчеркнуть, что в ходе практического применения технологии «подталкивания», как в Великобритании, так и в США осуществлялась не выборочное, а практически поголовное наблюдение при помощи самого изощренного интернет-инструментария, насколько применение «Надж» осознается населением. Выяснилось, что действие этой технологии практически не осознается.

Стоит отметить, что при наличии соответствующих Больших Данных нет никаких ограничений для использования технологии «Надж» не только в отношении граждан собственной страны, но и населения любых государств мира. При наличии соответствующих Больших Данных «Надж» может рассматриваться как сверхэффективное информационно-психологическое оружие следующего поколения. Хотя, с учетом принципов и технологий, на которых построена система «Надж», более точным является не привычное наименование информационно-психологического оружия, а скорее отнесение технологии «подталкивания» к поведенческому оружию, базирующемуся на Больших Данных, достижениях объективной психологии и нейронауках.

### 3.5. О чем умолчал Э. Сноуден

В любой спецоперации все прямо и косвенно причастные акторы стремятся реализовать собственные цели. Не является исключением и эпопея Э. Сноудена. Вполне очевидно, что Э. Сноуден хотел раскрыть глаза американскому и мировому общественному мнению на незаконные методы деятельности АНБ, тотальную слежку и прослушку. В то же время нельзя не отметить, что большая часть разоблачений Э. Сноудена, при всей их сенсационности, не открыла чего-то нового для экспер-

тов и специалистов в сфере разведки. Практически все, о чем поведал Э. Сноуден, было известно до него. Хотя и без деталей, подробностей, названий конкретных программ, размеров ассигнованных сумм и т.п. Конечно же, эти детали перевели предположения экспертов из разряда гипотез в сферу конкретных фактов и документированных мнений.

Однако интересно посмотреть, каких разделов коснулись разоблачения Э. Сноудена. В основном речь шла о нарушении приватности не только иностранцев, но и граждан США, прослушивании телефонных разговоров не только рядовых американцев, но и глав стран – союзников США, контроле со стороны АНБ за финансовыми транзакциями, осуществляемым по самым разнообразным потокам, программам развития кибервооружений и т.п. Все это произвело чрезвычайно большое впечатление и имеет до сих пор серьезные последствия как для престижа США, так и для межгосударственных отношений. Несомненно, это сказалось и на доходах компаний, упомянутых в разоблачениях Э. Сноудена.

Тем не менее, есть устойчивое впечатление, что АНБ использовало эпопею Э. Сноудена, уж коль скоро она произошла, как стандартную операцию прикрытия в отношении действительно главной, до сих пор тщательно скрываемой задачи, решаемой Агентством Национальной Безопасности и другими государственными структурами США при его содействии. Речь идет о разработке и практическом использовании технологий управления групповым и массовым поведением в других странах мира, как в странах-союзниках, так и противниках Соединенных Штатов Америки.

Нетрудно заметить, что в материалах Э. Сноудена вообще не содержится информация на эту тему и соответственно может возникнуть предположение, что тезис об управлении групповым поведением сколь угодно большой размерности имеет отношение не к фактическому

положению дел, а к конспирологии. Причем, конспирологии, понимаемой не в смысле научного, фактологического расследования, а в традиционной трактовке, как измышления незрелого ума и порождения неустойчивой психики.

На сегодняшний день существует достаточно большое количество имеющихся в открытой печати, а также в специализированных публикациях данных и фактов, подтверждающих высказанный выше тезис о переходе США к скрытому управлению поведением.

Первое. Начать, несомненно, надо с наиболее наглядного, что называется материализованного свидетельства практической постановки задачи управления поведением. Речь идет о только что отстроенном, оснащенном и выводимом на расчетную мощность циклопическом центре АНБ в штате Юта. Понятно, что для целей шпионажа, радиоэлектронной разведки, криптографии и проч. требуется гигантский объем хранилищ данных. Однако, для них не нужно хранилище объемом в один йоттабайт, которое расположено в новом Дата-центре в штате Юта. Чтобы наглядно понять, о чем идет речь, отметим, что весь ежегодный интернет-трафик, включая собственно интернет, интернет вещей и проч. приближается в настоящее время к одному зеттабайту. Тем самым в Юте имеется хранилище для 100-летнего мирового интернет-трафика. Однако размерность сразу уменьшается в том случае, если не просто хранить трафик, т.е. данные всех типов, а обрабатывать их различными способами, для чего представлять данные в виде самых различных классификаций. Иными словами, не для чего иного, как для интеллектуального анализа сверхбольших объемов данных такое хранилище просто не нужно.

Второе. В США, в отличие от других стран, еще в 1994 г. была создана специальная широкополосная сеть для совместного межведомственного использования ресурсов (аппаратных и программных) суперкомпьютеров.

Фактически в Соединенных Штатах в отличие от других стран суперкомпьютерная сеть не разделена ведомственными и корпоративными барьерами, а функционирует как единое целое. Более того, в начале нулевых годов американцы договорились с Великобританией, что к этой сети подключаются и британские суперкомпьютеры. Это весьма важно, поскольку согласно международным оценкам, лидером по эффективности использования суперкомпьютеров в секретных проектах выступает именно Великобритания. Данных по этой сети нигде нет, но различного рода косвенные расчеты позволяют утверждать, что мощность этой сети составит от половины, до двух третей суммарной мощности всех 500 суперкомпьютеров, входящих в настоящее время в мировой рейтинг. Наиболее мощные суперкомпьютеры, входящие в сеть, принадлежат АНБ, Министерству энергетики США, британской разведке и американским университетам, тесно работающим с военно-разведывательным комплексом. С 2014 года общее руководство сети осуществляет Киберкомандование США.

Третье. За последние четыре года Соединенные Штаты истратили несколько сот миллионов долларов на разработку программ интеллектуального анализа не просто Больших, а сверхбольших массивов данных. Примечательно следующее обстоятельство. В коммерческом секторе для анализа Больших Данных в основном используются методы математической статистики. В то же время, анализируя гранты таких агентств, как DARPA и IARPA, можно увидеть, что средства затрачивались на разработку программ по анализу и прогнозированию на основе Больших Данных, базирующихся на принципиально новых разделах математики, типа теории категорий и функторов, на системах распознавания образов, нейронных вычислениях и так называемом глубоком машинном обучении. Все эти методы на порядки превосходят с точки зрения выявления нетривиальных за-

висимостей и связей, мощности и точности прогнозирования, методы стандартной математической статистики, которые описываются как основной инструмент во всей специализированной литературе по Большим Данным.

Четвертое. Последние годы в США предпринимаются организационные и законодательные меры по обеспечению потребностей разведсообщества Большими Данными. Прежде всего, следует иметь в виду, что само по себе Агентство Национальной Безопасности является обладателем крупнейших массивов Больших Данных, которые оно получает в результате своей шпионской деятельности, о которой мир сегодня неплохо осведомлен благодаря разоблачениям Э. Сноудена.

Гораздо менее известна организация FSD. В переводе на русский она может быть названа Службой Федеральных Данных. Главным ее назначением является концентрация данных об американцах, которые собирают практически все федеральные ведомства, министерства, агентства и т.п. Без преувеличения можно сказать, что не в одной стране мира нет такой подробной базы данных на своих граждан, как в Соединенных Штатах, и содержится эта база не в АНБ, а в неприметной организации с указанным выше названием. При этом надо иметь в виду, что в данную организацию дополнительно стекаются все данные из страховых компаний, банков, пенсионных фондов, авиакомпаний и т.п. под американской юрисдикцией. Соответственно, если те или иные люди застрахованы в американской компании, обслуживаются американскими банками или банками, имеющими корреспондентские счета в американских банках, летали американскими авиалиниями или используют американские кредитные карты, типа Visa, American Express и т.д., то все их данных также попадают в эту организацию, а оттуда – в Центр Больших Данных АНБ.

Э. Сноуден не просто рассказал, а даже показал на слайдах связь с АНБ крупнейших интернет-компаний

и телекоммуникационных гигантов. В результате произошел большой скандал. Компании сначала протестовали, затем сообщили, что вносят соответствующие требования в Конгресс США о том, чтобы прекратить практику использования их данных в интересах АНБ. Однако от публики, и даже большинства экспертов укрылось крайне важное обстоятельство. Речь в протестах идет о персональных данных, т.е. данных, по которым можно идентифицировать пользователя как Ивана Ивановича Иванова, либо Джона Смита Третьего и т.п.

Большие же Данные – это не персональные данные. В принципе, персональные данные могут быть Большими Данными, а могут и не быть. Более того, для технологий Больших Данных сама по себе идентификация конкретного человека не важна и не интересна, потому что связи и закономерности, выявляемые при помощи Больших Данных, имеют статистический характер, а не касаются судьбы конкретного индивидуума. Про Большие Данные речь в разоблачениях Э. Сноудена вообще не шла.

Практически все крупнейшие провайдеры Больших Данных, а ими являются Google, Facebook, Twitter, Amazon, eBay и т.п., имеют американскую юрисдикцию. Между тем, в антитеррористическом законе США, именуемом как «Акт 2001 года, сплачивающий и укрепляющий Америку обеспечением надлежащими орудиями, требуемыми для пресечения терроризма и воспрепятствования ему» и Указе №13603 от 16 марта 2012 г. подписанном Президентом Б. Обамой, озаглавленном «О готовности ресурсов национальной обороны» четко прописаны обязанности американских компаний с точки зрения национальной обороны.

В число этих обязанностей входит предоставление данных, потребных для выполнения задач национальной обороны. Известно, что Большие Данные подпадают под юрисдикцию этих указов. Причем, если в отношении

персональных данных вообще и американцев в частности предусмотрены некоторые ограничения, связанные с необходимостью решений Секретного Суда для получения таких данных, то Большие обезличенные Данные должны предоставляться что называется в рабочем порядке по требованию.

Важно, что такие данные должны предоставлять не только американские компании – провайдеры Больших Данных, либо брокеры данных, но и компании, которые котируются на американском биржевом рынке. Последние два обстоятельства нуждаются в некотором пояснении. В Соединенных Штатах существует целый ряд крупнейших компаний, которые покупают данные по всему миру у других, как правило, у торговых компаний и перепродают их транснациональным корпорациям для целевого, или как его еще называют таргетированного маркетинга, и т.п. В их числе Acxiom, Experian, Epsilon и т.п.

Кроме того, практически все крупные международные интернет-компании котируются на NYSE, либо на Nasdaq. Соответственно, и эти компании при получении запроса под угрозой лишения листинга также должны передавать обезличенные Большие Данные американскому правительству, а иными словами АНБ. При этом то, что они могут иметь иную юрисдикцию и действовать в далеких от Америки регионах, не является препятствием для этих обязательств.

Подытоживая можно сказать, что АНБ сегодня имеет доступ к подавляющему большинству Больших Данных, имеющихся в мире. Некоторые высказывают точку зрения, что исключением является Китай. Однако другая часть специалистов не без основания полагает, что и китайские Большие Данные в немалой степени оказываются в США через американских и британских брокеров данных.

Пятое. В течение последних полутора лет в Соединенных Штатах прошел целый ряд научных конферен-

ций, круглых столов и заседаний, инициированных теми или иными «думающими танками», среди которых выделяется Институт сложности в Санта-Фе. В этих мероприятиях участвовали ведущие исследователи и разработчики в сфере Больших Данных, руководители департаментов поведенческого маркетинга и таргетированной рекламы, специалисты в сфере прогнозирования на основе Больших Данных – с одной стороны, и высокопоставленные правительственные чиновники, представители разведывательного сообщества и члены британской и американской правительственных программ «Надж» – с другой. Например, на одной из такого рода конференций с основным докладом Strategic potential of big data for National Security выступила исполнительный директор IARPA Катарина Марш.

Как правило, в большинстве такого рода мероприятий принимали участие один из ближайших советников Б. Обамы, участник группы по реформе АНБ Касс Санстейн, Ричард Талер, его соавтор по книге «Надж» и Алекс Пентланд. Алекс Пентланд недавно включен журналом «Форбс» в число семи самых влиятельных исследователей в области информационных технологий. Он руководит несколькими лабораториями в знаменитом МТИ, входит в число советников нескольких компаний из списка Форчун-500, консультирует правительство США.

Чтобы понять, о чем шла речь на этих мероприятиях, достаточно процитировать одну из статей Алекса Пентланда. «Я уверен, что значение Больших Данных состоит в том, что они дают информацию о поведении людей, а не об их убеждениях... Понятие Больших Данных и наука о сетях находятся за гранью обычных подходов к проектированию социальных структур... Адам Смит и Карл Маркс ошибались, или, по меньшей мере, предлагали только половинчатые решения. Почему? Потому что они строили свои теории на основе усредненных понятий рынка и классов. И хотя, безусловно, рассуждение в таких

терминах тоже может быть полезным, однако очевидно, что социальные феномены на деле состоят из миллионов мелких транзакций между индивидами. Существуют отдельные примеры межличностных взаимодействий, которые не просто не укладываются в усредненные параметры, а являются причиной социальных вспышек и потрясений, таких как Арабская весна. Придется снизойти до этих мельчайших примеров, этих микропримеров, потому что они позволяют понять социальное устройство вне усредненных показателей. Мы вступаем в новую эру социальной физики, где решающий исход будет зависеть от самых мелких деталей, от таких мелочей, как ты да я... Сам факт того, что мы теперь сможем отслеживать динамику социальных взаимодействий и их происхождение, что мы больше не будем ограничены усредненными показателями, такими как рыночные индексы, вызывает во мне трепет. Мы будем способны предсказывать и управлять поведением рынков и возникновением революций».

На этих конференциях родился пока еще не получивший широкого признания термин *hidden power*, или «невидимая сила».

Вполне очевидно, что представленные факты носят комплиментарный, т.е. дополняющий друг друга характер и показывают целостную картину завершающего этапа создания технологической системы управления групповым и массовым поведением любой размерности в иностранных государствах для реализации интересов США или наднациональной финансово-корпоратократической элиты.

Итогом такого управления должно стать превращение субъектов мировой политики, экономики и т.п. в объекты, находящиеся под внешним, невоспринимаемым руководящим воздействием. Для того, чтобы этого не случилось, необходимо в крайне сжатые сроки осуществить комплекс весьма интеллектуалоемких, вы-

сокотехнологичных мер, подкрепленных целым рядом обеспечивающих мероприятий, требующих затрат ресурсов и принятия новых юридических актов на государственном уровне.

### 3.6. Большие Данные в России: императивы ситуации

В течение последнего года практически ежемесячно, а то и чаще в стране проводятся различного рода конференции по Большим Данным. О чем же идет речь на подобных конференциях? Так на Global Entrepreneurship Congress 2014 «Большие возможности Больших Данных», как сообщают электронные СМИ «участники дискуссии привели многочисленные примеры использования технологий Big Data и связанной с этим серьезной экономии средств компаний. Среди таких примеров – система анализа поведения оборудования самолетов, предсказание сбоев и поломок и упредительная замена изношенных частей в аэропорту, в который направляется конкретное воздушное судно; анализ открытых спутниковых данных для оптимального планирования парковок; управление показами рекламных баннеров на сайте в зависимости от того, какую именно покупку совершает пользователь с помощью своей кредитной карты; сервис, информирующий автовладельцев о планах городских властей произвести ремонт или уборку улицы в том месте, где они оставили припаркованный автомобиль; прогнозирование спроса на отдельные наименования товаров и управление складами онлайн-магазинов; использование беспилотных аппаратов для сбора информации о состоянии линий электропередач в отдаленных районах, которое приводит к исключению ненужных дальних поездок сервисных бригад; наконец, использование сенсоров на лопастях ветряных мельниц, данные с которых помогают спрогнозировать, откуда именно поступит электроэнергия в следующую минуту (поскольку цены на

электроэнергию на глобальном рынке меняются ежеминутно, экономия измеряется миллионами долларов».

Конечно обсуждение «ветряных мельниц» и рекламных баннеров на сайтах впечатляет, но куда важнее следующие обстоятельства:

во-первых, на всех подобных конференциях речь идет о Больших Данных в их вчерашнем, а то и позавчерашнем понимании. Большие Данные, как правило, связываются исключительно с бизнес-аналитикой и с возрастанием объемов, многообразия и скорости передачи данных. Так понимали Большие Данные в США, Европе, Японии три-пять лет назад, когда собственно и появился этот термин;

во-вторых, на конференциях рассуждают, как правило, о будущем времени. По мнению большинства участников, например, одного из руководителей компании Форс – Центра внедрения Oracle О. Горчинской, «Практически нет проблем с наличием и доступностью технологий Больших Данных, готовностью поставщиков и интеграторов к их внедрению. Но в большинстве своем российские организации пока еще только присматриваются к таким решениям»;

в-третьих, ключевыми докладчиками, а то и организаторами таких конференций выступают, прежде всего, зарубежные компании, в первую очередь IBM, Oracle, SAP и т.п. Безусловно, взаимовыгодное, многостороннее сотрудничество с транснациональными гигантами IT-индустрии весьма полезно и выгодно как для российской экономики, так и для российских разработчиков. Углубление такого сотрудничества соответствует интересам бизнеса, способствует оптимальному углублению разделения труда в IT-сфере в глобальном масштабе.

Однако, в нынешней непростой геополитической обстановке нельзя закрывать глаза на одно неочевидное обстоятельство. Сегодня все зарубежные СМИ полны аналитическими статьями об использовании Росси-

ей энергетических ресурсов в качестве своеобразного геополитического оружия и средства достижения национальных целей. В этой связи вполне закономерно и логично предположить, что США, являющиеся бесспорными лидерами в сфере информационных технологий, также рассматривают их как своего рода технологическое оружие и средство научно-технического, экономического и геополитического давления.

Зарубежные специалисты полагают, что рынок в сфере Больших Данных в России достаточно ограничен с точки зрения готовности российских потребителей к использованию кластера этих технологий. Однако представляется, что подобная ограниченность не является единственной причиной повестки дня конференций. Другая, непроговариваемая причина состоит в том, что, по сути, зарубежные производители программных продуктов, связанных с Большими Данными, навязывают российскому рынку своего рода «консервирующую динамику». Эта динамика закрепляет отставание российской экономики вообще, и IT-отрасли в частности от зарубежных конкурентов и поддерживает господство зарубежных производителей на этом стратегическом сегменте IT-рынка.

Любой профессионал в сфере Больших Данных на вопрос, какие темы сегодня обсуждаются на конференциях по Большим Данным за рубежом, ответит, что там речь идет, в первую очередь, о так называемой «предсказательной» аналитике, поведенческом маркетинге на основе Больших Данных, экспертных системах, базирующихся на когнитивных вычислениях Больших Данных и т.п. Ни о чем подобном в практическом плане на российских конференциях, организованных транснациональными IT-компаниями, речи не ведется.

Как же быть в сложившейся ситуации?

Представляется, что начинать сегодня наверстывать упущенное и повторять уже пройденный путь вряд ли це-

лесообразно. В подобном случае российский IT-сегмент Больших Данных, обслуживающий, в том числе, не только интересы бизнеса, но и государственного управления, включая вопросы национальной безопасности, окажется вечно отстающем. Видимо, есть смысл сразу задуматься о реализации решений завтрашнего дня. Тем более, предпосылки в виде отечественной математической и программистской школ, кадрового потенциала, финансовых ресурсов и т.п. в нашей стране имеется.

Что же будет выступать завтрашним днем Больших Данных? Чтобы ответить на этот вопрос, необходимо внимательно присмотреться к наиболее динамично развивающимся направлениям сегодняшнего дня. Среди них выделяются:

• Третья производственная революция с массовой роботизацией, автоматизацией производства, внедрением 3D-печати, базирующаяся на информационных технологиях и Больших Данных, как на несущей конструкции;

• повсеместное распространение «интернета вещей» и ускоренный переход от «интернета вещей» к «интернету всего». «Интернет всего» предполагает, что к всемирной сети будут подключены практически все устройства, предметы и инфраструктуры во всех сферах жизнедеятельности социума и отдельного человека;

• широкое распространение автоматизированных систем поддержки и принятия решений на основе Больших Данных. Наиболее значительным прорывом в этой сфере на сегодняшний день стали системы высокочастотного, полностью роботизированного трейдинга. Ежедневно эти системы при минимальном участии человека или без оного, осуществляют торговые сделки, измеряемые сотнями миллиардов долларов. Ширится мнение, что на высокочастотном трейдинге отрабатываются человеко-машинные и автоматизированные системы принятия решений для сложных и сверхсложных систем.

Все три магистральных направления развития информационных технологий ведут к появлению в ближайшем будущем распределенных самообучающихся систем когнитивных вычислений. Поясним, о чем идет речь на самом простом примере. Всем хорошо известно, что Google активнейшим образом развивает программу полностью автоматизированных автомобилей, способных к нормальной эксплуатации в напряженной городской среде. В рамках этой программы реализуется следующий важнейший принцип. Каждый автомобиль снабжен как автономным бортовым компьютером со встроенной программой машинного обучения, так и подключением к общей базе сверхбольших Данных для всех эксплуатируемых автомобилей. Т.е. на каждой дорожной ситуации, на каждом ЧП, в которое попадает машина, программа учится, находит имеющиеся в ней ошибки, устраняет их с тем, чтобы в последующем не попадать в подобные ситуации. В этом смысле машина, пускай грубо, но имитирует принцип жизнедеятельности человека, который, как известно, учится на собственных ошибках. Одновременно программа сообщает о найденной ошибке, ее решении в общую распределенную базу сверхбольших Данных, к которой подключены все автомобили. Тем самым, каждая машина учится не только на собственных ошибках, но и на ошибках, которые совершаются другими автомобилями. Более того, найденное программой одного автомобиля удачное программное решение становится достоянием всех. Фактически мы имеем дело со своего рода стаей, соединенной тесными связями взаимного обучения. Применительно к производственным роботам подобная программа сейчас реализуется в Германии. К роботам, занимающимся уборкой домов – в Японии.

О чем это все говорит? Мы видим, что повсеместно Большие Данные используются для коллективного обучения и выработки все более эффективных решений.

Фактически это, по сути, является имитацией памяти и логического мышления. Ведь память тоже аккумулирует знания о прошлом, о том, что удалось и не удалось, закрепляет удачные образцы, которые в дальнейшем и используются в поведении и, как открыл П. Анохин, в опережающем реагировании на изменения внешней среды.

Сначала человек использовал только возможности своего физического тела и соответственно своей психофизиологической памяти. Всем хорошо известно, что помнит человек практически все, но вот использовать все, что находится в памяти, не может по многим причинам.

В дальнейшем, с появлением развитых языков и письменности, человек, по сути, выстроил вторую, коллективную память, где фиксировались индивидуальные и групповые успехи и неудачи, к которым мог иметь доступ любой участник социума. В этом смысле тексты, фильмы, аудиозаписи и т.п. представляют собой память «второго рода».

Несложно заметить, что Большие Данные есть не что иное, как память «третьего рода», ориентированная на эксплуатацию человеко-машинными системами. Эта память имеет распределенный характер, в ней ничего не забывается, к ней постоянно открыт доступ, она используется в режиме 24/7 и построена так, чтобы быть удобной для применения мощнейших средств интеллектуального, прежде всего, математического анализа. Наконец, мощность этой памяти и возможность обработки хранящейся в ней информации при помощи самых различных методов значительно превышает мощность любого индивидуального интеллекта.

В этом смысле создание действующих систем хранения, обработки и восприятия Больших Данных, как памяти «третьего рода» является прорывом, сравнимым с появлением самих по себе компьютеров, а также дру-

гих эпохальных технических решений. При этом в данном случае речь идет не только о чисто техническом, но о социотехническом решении, которое затрагивает все стороны практической жизни людей. Также понятно, что создание и эксплуатация памяти «третьего рода» становится одним из решающих преимуществ, обеспечивающих ее обладателям доминирование в любых сферах жизнедеятельности.

В этой связи с особой остротой встает тема, которую в течение последнего года активнейшим образом разрабатывает один из самых известных людей в российской IT-индустрии Игорь Ашманов. Это тема информационного суверенитета.

Информационный суверенитет – это «возможность государства управлять информацией». Информационный, или цифровой суверенитет, как справедливо отмечает И. Ашманов, включает несколько компонентов. Это и техническая инфраструктура, и программные продукты, и собственные поисковые системы, и социальные сети и т.п.

В ближайшем будущем несущей конструкцией и ключевым ресурсом, определяющим цифровой суверенитет, становятся Большие Данные, как «третий вид памяти». Именно Большие Данные аккумулируют в себе архивы поисковых систем, социальных сетей, торговых платформ, бизнес- и государственные базы самого различного рода и т.п.

Особо проблема цифрового суверенитета обостряется в современном мире. Не секрет, что сегодня происходит не только слом однополярной мировой системы, но и де-факто мир прощается с Потсдамской системой мироустройства. Реальностью становится тот факт, что все бо́льшую роль в международных отношениях начинает играть не право, а сила.

Собственно, процесс этот начался давно. Наиболее ярко он проявил себя в конце 90-х г. в связи с распадом

бывшей Югославии и событиями в Косово. Сегодня же мы являемся свидетелями конца монополии на односторонний демонтаж прежнего миропорядка. Прекрасно отдавая себе отчет в возрастании значения силового компонента, Соединенные Штаты и их союзники одновременно не испытывают иллюзий относительно возможностей применения наиболее разрушительных видов вооружения. По мнению большинства экспертов ни Соединенные Штаты, ни Западная Европа не технически, не организационно, не, главное, ментально, не готовы к серьезной «горячей» войне.

В этой связи последние 30 лет, прежде всего, в США и Великобритании ведется неустанный поиск новых видов вооружений, которые позволяют реализовать Оруэллианскую концепцию: «мир – это война, свобода – это рабство». Первыми в ряду этих вооружений были кажущиеся сегодня простыми информационно-психологические вооружения, базирующиеся на традиционной пропаганде и достижениях классической психологии. Затем стали использоваться более изощренные технологии программирования деструктивных действий в виде «цветных» революций и т.п.

Не секрет, что до сих пор наиболее обсуждаемыми темами среди российского экспертного сообщества остаются темы «цветных» революций, так называемого «управляемого хаоса» и т.п. Между тем, эти темы всерьез уже перестали рассматриваться западным военно-разведывательным сообществом как последние, и наиболее совершенные военные технологии. При этом в США, Великобритании и т.п. продолжают активно издаваться книги по «цветным» революциям, управляемому хаосу, деструктивным восстаниям и т.п. Проводятся соответствующие конференции. Однако ничего принципиально нового на них не появляется. Детальный анализ участников конференций и авторов книг, а также конструктивное рассмотрение их содержания показывает,

что последние полтора-два года подобные мероприятия выполняют скорее отвлекающую роль. Фактически есть основания полагать, что эта работа в немалой степени стала элементом большой операции прикрытия и дезинформации, направленной на отвлечение интеллектуальных усилий цивилизационного противника.

На практике же главные усилия сосредоточены на разработке принципиально нового поколения вооружений, так называемых «поведенческих» вооружений. Поведенческие вооружения базируются на трех китах: во-первых, Больших Данных, как памяти «третьего рода», во-вторых, когнитивных вычислениях, объединяющих мощь математических методов с пусть грубой, но уже имитацией работы человеческого мозга и, в-третьих, аккумуляции и использовании достижений поведенческой психологии.

Как показывает анализ видимого и невидимого сегментов интернета, подавляющая часть публикаций на эту тему засекречена. Можно найти лишь отдельные фрагменты, куски работ или исследований, касающихся этих тем, но прямо не связанных с военно-разведывательной тематикой. Тем не менее, недавно появились прямые доказательства разработки, по крайней мере, в США и Великобритании, поведенческих вооружений, ориентированных на скрытое управление групповым поведением коллективов различной размерности. Так, в конце прошлого года Институт оборонного анализа, финансируемый Пентагоном, разведывательным сообществом и Государственным Департаментом опубликовал документ «Pathways to Cooperation between the Intelligence Community and the Social and Behavioral Science Communities». В нем упоминается, что в 2013 году было проведено большое совещание по программе «Minerva Research Initiative». Это закрытая программа IARPA в области управления групповым поведением на основе Больших Данных, которая получила статус

стратегической важности с точки зрения национальной безопасности США.

В подготовленном в прошлом году министерством обороны Великобритании докладе «Global Strategic Trends out to 2040» в качестве одной из целей ближнего прицела также выделено скрытое управление групповым поведением на основе Больших Данных. Этот доклад в определенной степени стал осмыслением британского военного бестселлера последнего года, книги бывшего командующего британскими подразделениями в Северной Ирландии, Косово, Ираке, Ливане и Афганистане генерал-майора Э. Маккея и коммандера С. Тотама «Поведенческий конфликт» (Behavioural Conflict: Why Understanding People and Their Motives Will Prove Decisive in Future Conflict). Выводом книги стали следующие слова: «Наша способность понять и незаметно изменять поведение групп людей станет определяющей характеристикой вооруженных конфликтов нового типа».

Нет сомнений, что в современной сложной геополитической ситуации Большие Данные являются стратегическим ресурсом и приоритетом не только развития экономики и социума, но и важнейшим вопросом обеспечения национальной безопасности. В этой связи представляется целесообразным:

во-первых, сориентировать Фонд развития интернет-инициатив, Фонд Сколково и Фонд перспективных исследований на государственное и негосударственное финансирование стартапов и отечественных разработок в сфере Больших Данных, нацеленных в первую очередь на межотраслевое использование, а также решение задач в области охраны правопорядка и решения задач национальной безопасности;

во-вторых, организовать в ведущих университетах страны с мощными математическими школами и кафедрами по программированию, системному анализу, лингвистике и т.п. кафедры Data science (наука о дан-

ных). В оперативном режиме открыть при кафедрах магистратуры и группы ускоренного обучения Data science и когнитивным вычислениям. Организовать перевод на русский язык имеющихся онлайн видеокурсов по Большим Данным, когнитивным вычислениям и поведенческому анализу;

в-третьих, провести научно-практическое совещание по использованию Больших Данных, когнитивных вычислений и поведенческих наук для прогнозирования и противодействию скрытому управлению поведением. В рамах подготовки к совещанию осуществить инвентаризацию отечественных разработок и имеющихся кадров по указанному направлению;

в-четвертых, организовать с привлечением лучших вне зависимости от академических званий и занимаемых должностей специалистов межотраслевые и вневедомственные коллективы по разработке методологии, математического аппарата и программных решений по прогнозированию сложных социальных систем и противодействию скрытому управлению групповым поведением;

в-пятых, инициировать разработку пакета нормативных документов, связанных с вопросами государственного регулирования Больших Данных, включая их сбор, накопление, использование и возможность трансграничной передачи. При необходимости проработать вопрос о подготовке государственной концепции в сфере Больших Данных.

# Глава 4
# ПРЕСТУПНОСТЬ ЦИФРОВОГО МИРА

Раздвоение действительности на реальность и виртуальность, связанное с появлением интернета на рубеже 90-х гг. прошлого века, в ближайшие два-три года в развитых странах будет окончательно преодолено и опять сложится единая действительность. Фактически это означает, что информационные технологии будут присутствовать повсеместно и постоянно использоваться во всех сферах быта, социальной, политической и экономической жизни. Применительно к задачам правоохранительной деятельности это предполагает, что информационные технологии, так или иначе будут использоваться при совершении практически всех преступлений, и будут востребованы правоохранителями либо как средство борьбы или профилактики преступлений, либо как средство обнаружения улик, создания доказательной базы.

В настоящее время в России де-факто под киберпреступностью понимаются незаконные действия, которые осуществляются людьми, использующими информационные технологии для преступных целей. Среди основных видов киберпреступности выделяют распространение вредоносных программ, взлом паролей, кражу номеров кредитных карт и других банковских реквизитов, а также распространение противоправной информации (клеветы, порнографических материалов) через интернет. Киберпреступлениями также считаются интернет-аукционы, в которых сами продавцы делают ставки для того, чтобы поднять цену выставленного на аукцион товара.

К компьютерным преступлением Уголовный Кодекс РФ относит преступления, подпадающие под следующие статьи:

статья 272 – неправомерный доступ к компьютерной информации;

статья 273 – создание, использование и распространение вредоносных компьютерных программ;

статья 274 – нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

Следует отметить, что пока в России понятие «киберпреступности» не легализовано ни в нормативном, ни в правовом пространстве. В отличие от подавляющей части остального мира в России вместо киберпреступности используется терминология – преступность в сфере компьютерной информации, информационных технологий, информационной безопасности и т.п.

В ситуации, когда информация и информационные технологии пронизывают абсолютно все стороны жизни, оперирование этими терминами для спецификации и выделения видов преступности, а соответственно и подразделений, занимающихся борьбой с ними, является совершенно бессмысленным. Это давно поняли за рубежом. Именно поэтому там изначально речь шла именно о киберпреступности, а не об информационных технологиях вообще.

Существует несколько подходов к определению киберпреступности и соответственно к задачам, которые должна решать киберполиция.

Наиболее общий подход характерен для США. В трактовке Верховного суда США, киберпространство – это «уникальная среда, не расположенная в географическом пространстве, но доступная каждому в любой точке мира посредством доступа в Интернет». Опираясь на это определение, Департамент Юстиции США тракту-

ет компьютерные преступления, как «любое нарушение уголовного права, связанное со знанием компьютерных технологий для совершения преступления, его расследования или судебного преследования». Такой столь широкий подход к определению киберпространства и киберпреступности связан с особенностями американского законодательства, которое в решающем плане образовалось под воздействием прецедентного английского права. И соответственно судебные решения носят максимально широкий характер, а прецеденты по конкретным процессам детализируют их и создают необходимую базу для правоохранительной деятельности. Поскольку российское законодательство построено не на прецедентном, а на романском праве, то имеет смысл обратиться к опыту Европы.

Конвенция Совета Европы о киберпреступности определяет четыре вида компьютерных преступлений «в чистом виде»:

- незаконный доступ – ст. 2;
- незаконный перехват – ст. 3;
- вмешательство в данные – ст. 4;
- вмешательство в систему – ст. 5.

Именно эти четыре вида киберпреступлений являются «компьютерными», остальные – это либо связанные с компьютером (computer-related), либо совершаемые с помощью компьютера (computer-facilitated) преступления.

К ним относятся:

- преступления, в которых компьютер является орудием (электронные хищения, мошенничества и т.п.);
- деяния, при совершении которых компьютер является средством (например, размещение на сайтах детской порнографии, информации, разжигающей национальную, расовую, религиозную вражду и т.д.).

Такой подход, видимо, станет господствующим, поскольку в ходе проходящих в настоящее время перегово-

ров между Соединенными Штатами и Европейским Союзом по вопросам создания Трансатлантического торгового и инвестиционного партнерства наряду с вопросами тарифного и надтарифного регулирования, а также унификации регламентов и нормативов, рассматриваются и вопросы сближения законодательной базы, по борьбе с преступностью, прежде всего, в сфере экономических и цифровых преступлений. В частности, на состоявшемся в июле этого года совещании экспертов США и ЕС в рамках подготовки TTIP по проблемам преступлений, связанных с компьютерами и компьютерными сетями, специалистами было дано два определения киберпреступления – киберпреступление в широком и в узком смысле.

• Киберпреступление в узком смысле (компьютерное преступление) – любое противоправное деяние, совершенное посредством электронных операций, целью которого является безопасность компьютерных систем и обрабатываемых ими данных.

• Киберпреступление в широком смысле (как преступление, связанное с компьютерами) – любое противоправное деяние, совершенное посредством компьютера или связанное с компьютерами, компьютерными системами или сетями, включая незаконное владение и предложение или распространение информации в компьютерных и телекоммуникационных сетях.

Анализ итогов совещания показывает, что стороны склоняются к европейской позиции трактовки кибепреступности. Тем более что под нее «заточен» и классификатор видов преступлений, разработанный Интерполом еще в 1991 г. и используемый в настоящее время более чем в 170 странах.

Борьба с киберпреступностью предполагает, прежде всего, анализ основных направлений и масштабов киберпреступности в РФ.

Согласно мнению начальника Бюро специальных технических мероприятий МВД России, генерал-майора

полиции А.Н. Машкова, высказанному весной 2014 года: «Если мы говорим об угрозах информационной безопасности, то не можем обойти стороной тематику киберпреступности, ведь она остается одной из самых динамично развивающихся и прибыльных отраслей преступного бизнеса. Согласно оценкам экспертов компании Symantec, каждую секунду в мире жертвами киберпреступников становятся 12 человек, и их количество растет с каждым годом. Россия не отстает от мировых показателей по темпам роста киберпреступности, что неудивительно, ведь наша страна входит в десятку государств мира с самым высоким числом интернет-пользователей. В 2013 году количество зарегистрированных преступлений в сфере телекоммуникаций и компьютерной информации увеличилось на 8,6%. При этом можно выделить ряд устойчивых тенденций. Основным мотивом киберпреступников стало желание извлечения материальной выгоды. Практически все случаи неправомерного доступа к компьютерной информации, составляющие на сегодняшний день 19% от общего числа зарегистрированных компьютерных преступлений, или изготовления вредоносного программного обеспечения (8%) направлены на хищение денежных средств. Количество преступлений, совершаемых из хулиганских или иных побуждений, крайне незначительно.

Еще одна тенденция современной киберпреступности заключается в том, что преступники-одиночки постепенно вытесняются с криминального рынка законспирированными, хорошо организованными и разветвленными преступными группами, объединяющими людей из разных регионов России или стран мира. Участники подобных криминальных сообществ имеют свою преступную специализацию, и эффективность их деятельности довольно высока. В целях противодействия таким преступным группам Управление «К» БСТМ МВД России внедряет передовые технологии сбора и анализа дока-

зательственной базы и совершенствует профессиональную подготовку сотрудников, что позволяет повысить качество работы подразделения и сконцентрироваться на расследовании наиболее сложных преступлений».

Рассматривая структуру киберпреступности в нашей стране, начнем с наиболее быстроразвивающегося сегмента киберпреступности, а именно, киберпреступлений в сфере финансов. Здесь существует несколько основных направлений:

Во-первых, преступность, связанная с интернет-эквайрингом, т.е. обслуживанием кредитных карт. Борьба с кардерами началась практически сразу с появления в России кредитных карт и задолго до образования специализированных подразделений в системе МВД России. Строго говоря, значительная доля преступлений, связанных с кредитными картами осуществляется организованными группами, которые действуют как в реале, так и в виртуале. В реале – это работники дорогих ресторанов, бутиков и т.п., а также иногда работники банков. В виртуале – это хакеры, а также программисты, умеющие создавать и обслуживающие сайты в так называемом «dark net», в основном относящиеся к сети Tor. Именно там расположены площадки, которые являются основными торговыми точками по сверхоперативной реализации краденных карт, а также данных и т.п. К российской специфике относится перехват трафика, когда данные по кредитной карте перехватываются в процессе передачи данных от компьютера пользователя к платежной системе, интегрированные в тот или иной торговый сайт. На сегодняшний день рынок интернет-эквайринга в России составляет примерно 6 млрд. долларов. Размеры преступно присваиваемых доходов на этом рынке по данным зарубежных экспертов применительно к нашей стране составляют 300 млн. долларов. Кроме того, еще порядка 500–800 млн. долларов приходится на российских хакеров, действующих на мировом рынке интернет-

эквайринга. Этот вид преступности растет в геометрической прогрессии – с одной стороны по мере увеличения с каждым годом расчетов по платежным картам (в настоящее время они составляют уже порядка 15% от суммы всех расчетов), а с другой – вследствие взрывных темпов роста интернет-торговли, которые составляют 25-30% в год.

Например, в этом году группа российских хакеров в составе четырех человек, во главе с Владимиром Дринкманом украла 950 тыс. платежных карт, что привело к потере сотен миллионов долларов. В ходе этого нападения группа была опознана, а ее руководитель арестован и в настоящее время находится под стражей в Нидерландах. В ходе следствия выяснилось, что группа успешно действовала в течение семи лет. За этот период четырем хакерам удалось взломать финансовые порталы десятка крупных американских и международных финансовых корпораций и украсть номера и коды 160 млн. кредитных и дебетовых карт, нанеся предположительный ущерб, исчисляемый миллиардами долларов.

Во-вторых, в России одной из ведущих сфер киберпреступности является рынок Forex. В настоящее время этим рынком в стране охвачено примерно 400-450 тыс. человек. Общий объем операций на рынке составляет 1,5 трлн. долларов. При кредитном плече 1:100 это означает, что на рынке «крутится» примерно полтора млрд. долларов реальных денег.

Российский розничный рынок Forex не регулируется вообще, хотя существует уже более 15 лет. Даже те компании, которые не являются мошенническими, работают в большинстве случаев с серьезными нарушениями российского законодательства, поскольку все их головные конторы находятся в оффшорных юрисдикциях. Однако, строго говоря, собственно к киберпреступности относится та часть брокерских контор на рынке Forex, которая носит чисто мошеннический характер. Это конторы, ко-

торые проводят операции без перечисления средств реальным валютным дилерам для проведения операций по купле-продаже валюты. Такие конторы всю сумму средств, поступающую от клиентов, оставляют себе и из этих средств выплачивают выигрыши. Согласно статистике, подтвержденной всеми ведущими зарубежными банками, для мелких розничных клиентов соотношение между суммой выигрышей и проигрышей составляет 1:9 – 2:8. Согласно мнению владельцев крупнейших относительно легальных форексовских контор, примерно 40% форексовских брокеров являются мошенниками в полном смысле этого слова и могут быть квалифицированы как киберпреступники. Вся их деятельность осуществляется в киберпространстве при помощи информационных технологий. Несложные расчеты показывают, что объемы ежегодных хищений на рынке составляют 500-700 млн. долларов.

Активно растет киберпреступность в сфере интернет-торговли. По сравнению с США и Западной Европой, где на интернет-торговлю приходится 7% совокупного розничного оборота, в России эта доля невелика, и составляет всего 1,5%. Однако, по темпам прироста российская интернет-торговля оставляет далеко позади и США, и Европу и растет темпами порядка 20-30% в год. В настоящее время объем рынка e-commerce в России составляет 13 млрд. долларов. Ожидается, что в этом году через интернет различные товары и услуги приобретут более 15 млн. человек. Главными категориями покупок являются бытовая и компьютерная техника, спортивные товары, одежда и контент, включая книги и т.п.

Преступления в этой сфере осуществляются по нескольким направлениям. Главным из них является использование серых схем продажи контрафактной продукции, продукции произведенной с нарушением регламентов и технических норм, под поддельными товарными знаками или ввезенных в Россию без уплаты

соответствующих таможенных пошлин, а также торговля за неучтенную наличность. Последнее обстоятельство является специфической особенностью России и других стран постсоветского пространства. Если за рубежом практически все покупки в интернет-магазине осуществляются за безналичный расчет, то в России в настоящее время на долю оплаты товаров по кредитным картам или электронными деньгами приходится чуть более 25% платежей, 75% – это оплата наличными курьеру при доставке товара. Соединение серых схем поставки товаров в интернет-магазины с неучтенными расчетами наличными позволяет специалистам оценивать общий объем преступно присвоенных доходов на рынке электронной коммерции на уровне полутора-двух млрд. долларов с тенденцией к быстрому росту. Указанные цифры приведены без учета налоговых преступлений, а также потерь государства от серых и черных таможенных схем.

Попробуем примерно оценить размах киберпреступности в сфере интеллектуальной собственности. Нельзя не отметить, что с вступлением России в ВТО и подписанием целого ряда других международных соглашений, к этой сфере приковано самое пристальное внимание не только в России, но и за рубежом. В этой связи вполне очевидно, что одной из ключевых задач киберполиции должна стать борьба с пиратством в отношении цифрового контента и программного обеспечения.

По состоянию на 2014 год реалистичная сумма потерь на рынке видео- и аудиоконтента вследствие пиратства колеблется в районе от шести до восьми млрд. долларов ежегодно. Согласно оценкам международной консалтинговой группы IDC, потери российского рынка ПО от пиратов составляют четыре млрд. долларов, плюс еще около полутора млрд. долларов составляет контрафактный софт, установленный в основном на предприятиях малого бизнеса. Весьма ощутимую, но смешную на фоне указанных выше цифр, составляет сумма по-

терь книгоиздателей от пиратов, которая колеблется на уровне 120 млн. долларов в год. В целом Россия входит в число наиболее пиратских стран. В текущем году уровень пиратски скачанного контента и ПО составил 67% от общего их объема (для сравнения в США – 12%, в Японии – 5%, в Зимбабве – 90%, в Монголии – 76%).

Начиная с 2005 г. в основном в интернет перешла значительная часть технологической цепочки, связанная с проституцией. В первую очередь это касается, с одной стороны, отбора контингента, а с другой – площадок для информирования потенциальных потребителей и осуществления коммуникаций с ними. Т.о. можно с уверенностью сказать, что, даже не касаясь вопроса цифровой порнографии и педофилии, бизнес, связанный с проституцией все более смыкается с компьютерной преступностью. По имеющимся оценкам оборот этого бизнеса в крупных городах, а именно здесь он завязан на интернет, составляет ежегодно порядка пяти-семи млрд. долларов. Без интернета этот бизнес существовать сегодня просто не смог бы.

В заключение хотелось бы остановиться на принципиально новом виде бизнеса, связанном с кибернаемничеством. В условиях, когда войны распространились на киберпространство и когда в высокотехнологических странах все большая часть преступлений осуществляется опять же в киберпространстве, спрос на квалифицированных и высококвалифицированных хакеров растет в геометрической прогрессии. По свидетельству эксперта ЕЭС по вопросам информационной безопасности и главы Комиссии по этичному хакерству Пьерлуиджи Паганини российские хакеры на мировом рынке котируются как наиболее изощренные, талантливые и безбашенные, способные выполнять самые сложные задачи. Спрос на их услуги предъявляют как иностранные государства, так и зарубежные корпорации, а также организованные преступные группировки из различных стран мира, дей-

ствующие в первую очередь на территории высокотехнологичных стран. По оценкам ряда американских экспертов в области финансовой киберпреступности совокупные потери американских финансовых учреждений и граждан от кибергруппировок, в состав которых входили российские хакеры, превысили в последние годы 25 млрд. долларов. Из них 15 млрд. пришлось на операции с кредитными картами и банковскими мошенничествами, а остальные – на высокотехнологичные операции, связанные с манипулированием биржевых рынков на основе преступного перехвата управления торговыми роботами.

Таким образом, уже сегодня можно говорить о том, что сформировалась подпольная масштабная экономика киберпреступности, действующая как на территории России, так и в трансграничном масштабе. На последнее следует обратить особое внимание в связи с тем, что законодательства различных стран в сфере киберпреступности значительно разнятся. Поскольку преступные синдикаты обслуживают первоклассные, едва ли не лучшие юридические фирмы и отдельные юристы, то все большее распространение получают так называемые распределенные схемы сетевой киберпреступности. Во все большем числе случаев удается строить такие юридические цепочки, когда явно в целом преступные кибердеяния не являются таковыми, поскольку оказываются разбиты на цепь операций, каждая из которых осуществляется в отдельной стране, где именно эта операция не является преступной.

Пока речь шла только об уже существующих основных видах киберпреступности и денежных оценках их масштабов в РФ, а также ущерба, наносимого российскими хакерами и программистами за рубежом. Следует отметить, что уже в ближайшие год-два этот перечень существенно расширится сначала в высокотехнологически развитых странах, а затем и в России. Повсеместное

распространение интернета вещей, а затем и интеграция электронных компонентов в тело человека, открывают принципиально новые возможности для различного рода преступлений, ранее никак не связанных с киберпреступностью. Наиболее ярким примером являются многократно возросшие возможности для дистанционных убийств либо при помощи вмешательства в управляющие сети домов и электронных приборов, либо в электронные устройства, регулирующие те или иные протезы или органы жизнедеятельности человека.

Темпы развития и изменяющаяся структура киберпреступности делают это направление правоохранительной деятельности одним из главных в работе ФСБ и МВД России. В ближайшие годы их деятельность будет сосредоточена в первую очередь на следующих направлениях киберпреступности:

во-первых, борьбе с киберпреступлениями в финансовой сфере, включая, в первую очередь, кардерство, преступления в сфере интернет-эквайринга, незаконное предпринимательство и мошенничество на электронном рынке Forex, а также осуществление мер совместно с критически важными для страны банками и финансовыми институтами по защите их корпоративных информационных систем и повышения уровня информационной безопасности;

во-вторых, противодействии криминалу в сфере онлайн торговли как в виде прямого, незаконного предпринимательства и мошенничества, пресечении серых схем торговли, включая реализацию контрафактных и поставленных с нарушением таможенного законодательства товаров и услуг, торговли с грубыми нарушениями правил регулирования наличного оборота;

в-третьих, пресечении легализации (отмывания денежных средств или иного имущества), осуществляемой в киберпространстве посредством операций финансовых институтов и онлайн торговли;

в-четвертых, борьбе с преступлениями в сфере интеллектуальной собственности в виде пиратства, а также незаконного предпринимательства и мошенничества, в отношении программного обеспечения и всех видов цифрового контента, включая аудио-, видео- и текстовую продукцию;

в-пятых, пресечении преступлений по вовлечению в проституцию при помощи интернет-ресурсов, социальных сетей и т.п., а также борьба с киберпреступностью в сфере интернет-педофилии (в основном в сети Tor);

в-шестых, борьбе со всеми видами преступлений в сфере компьютерной информации;

в-седьмых, пресечение образования и деятельности экстремистских сообществ в интернете, включая общедоступный интернет, социальные сети, а также так называемый «невидимый интернет» (сеть Tor и пиринговые сети);

в-восьмых, выявление и блокирование интернет- и телекоммуникационных сетей и ресурсов, а также сообщений в них, способствующих возникновению массовых беспорядков;

в-девятых, профилактике, предупреждении и пресечении преступной деятельности в сфере наемничества в отношении программистов, разработчиков, хакеров, вовлекаемых в российские и международные преступные группировки, а также в преступную деятельность отечественными и зарубежными юридическими лицами, и зарубежными государственными организациями.

Успехи в реализации указанных выше направлений работы связаны с решением двух взаимоувязанных задач. С одной стороны, структурные подразделения ФСБ и МВД России, в чьи функции входит борьба с киберпреступностью, должны быть в самые сжатые сроки не только укреплены кадрово качественно и количественно, но и обеспечены самыми передовыми программными инструментами. С другой стороны, еще более остро

стоит задача повышения квалификационного уровня и оснащения современными программами, базами данных и т.п. работников подразделений ФСБ и МВД России, напрямую не связанных с компьютерной преступностью. Учитывая проникновение информационных технологий «во все поры» социума, «во все уголки» экономики, возлагать борьбу с киберпреступностью только на специализированные подразделения является утопией. Они просто не смогут справиться со своей задачей в силу того, что буквально завтра, в прямом смысле слова, подавляющая часть преступлений будет совершаться с использованием информационных технологий, интернета и других сетей. Поэтому решающие сдвиги в борьбе с киберпреступностью связаны не только и не столько с деятельностью специализированных структур ФСБ и МВД России, сколько с успешным овладением компьютерным инструментарием всех структур и звеньев правоохранительной системы нашей страны.

# Глава 5
# ЗАГАДКА БИТКОЙНА

## 5.1. Биткойн – цифровая валюта виртуальных государств

В конце 2013 года в информационном пространстве сложилась парадоксальная ситуация, которая ненамного изменилась и в 2014 году. Одной из наиболее обсуждаемых экономических тем стала тема Биткойна. О Биткойне пишут все медиа, даже далекие от финансов и бизнеса. Как грибы после дождя растут ресурсы и блоги на эту тему. На телеканалах по всему миру появляются программы, посвященные этой криптовалюте. Парадокс состоит в том, что капитализация рынка Биткойна постоянно изменяется, и на пике составляла около 10 млрд. долларов. А в 2014 году уменьшилась примерно до 5 с небольшим миллиардов. Для сравнения мировой рынок Forex в день имеет емкость около 4 трлн. долларов. Т.е. с позиции мировой финансовой системы мы имеем дело с исчезающее малой величиной. Все это заставляет ряд экспертов считать Биткойн мимолетным явлением, а шум, поднятый вокруг нее очередным вирусным информационным мемом, которые мгновенно рождаются и столь же быстро умирают. Дополнительные аргументы в пользу незначимости Биткойна они черпают в том, что в 2014 году его курс по сравнению с пиком начала зимы 2013 года упал примерно в два раза. Однако, по нашему мнению, дело обстоит совсем не так.

Ажиотаж, стремление раздуть сенсацию и привлечь внимание читателей и зрителей, конечно, имеют место. Но суть дела намного глубже. Биткойн, как платежная система и валюта, породила разнообразные глубинные

процессы. Эти процессы относятся не только к финансам, но и затрагивают социум, политику и противоборство различных групп и структур элит, как в глобальном масштабе, так и вероятно в разрезе отдельных регионов и даже стран.

Из теории информации хорошо известно, что при передаче сигнала, наряду с собственно информацией, присутствуют шумы. Мы же ставим перед собой задачу отделить содержательную составляющую от информационного мусора, отфильтровать факты и, базируясь на них, постараться не только понять феномен криптовалют на примере Биткойна, но и главное, выяснить, кто стоит за этим феноменом, кто ему противодействует и каково инструментальное назначение Биткойна в нашем неустойчивом, турбулентном и динамичном мире.

Невиданной популярности в информационном пространстве Биткойн, конечно же, обязан экспоненциальному росту своей цены. При финансовом потребительском строе, который сегодня возобладал в мире, несомненной главной ценностью стали деньги. Соответственно деньги, чья ценность растет по экспоненте, являются наиболее привлекательным, как в материальном, так и в информационном смысле, товаром.

Если в 2009 году, когда Биткойн был создан, его цена в долларах колебалась около 0,3 цента, то к декабрю 2011 г. он вырос до 2 долларов. К декабрю 2012 года – до 30. А к декабрю 2013 г. достиг примерно 1000 долларов. После этого в силу целого ряда обстоятельств, связанных как с решениями регуляторов, так и с внутренними проблемами инфраструктуры Биткойна, его курс снизился практически в два раза. Однако в 2014 году заметно снизились колебания, или волатильность курса. При этом устойчиво растут объемы сделок с Биткойнами, включая как приобретение на них товаров, так и обмен на Биткойны привычных долларов и евро на возникших биржах

криптовалют. Число интернет-магазинов, принимающих биткойны, растет темпом около 100% в месяц.

В основе системы Биткойна находятся пять принципиальных решений.

*Во-первых*, все операции в сети Биткойн шифруются. Каждый ее участник получает собственный ключ, благодаря которому он может в зашифрованном виде осуществлять транзакции, проводить переводы средств, осуществлять добычу Биткойнов. Единственное, чего он не может, это при помощи своего ключа работать с чужими Биткойнами.

*Во-вторых*, сеть Биткойн – это пиринговая сеть. Наш привычный интернет похож на многоэтажный дом. Простые пользователи, провайдеры, хостеры, корневые сервера, наиболее посещаемые ресурсы и т.п. имеют различные возможности, полномочия и ответственность. Связь в этой обычной сети осуществляется через специальные сервера. Пиринговую сеть еще называют одноранговой. Она похожа на одноэтажный дом. Все участники сети абсолютно равны. Каждый является и клиентом, и сервером, предающим информацию. Информация в такой сети идет, конечно, медленнее, поскольку передается от одного компьютера к другому. Но зато, как говорится, нету главных. В этой сети все ее участники равны, и информация передается не через сервера различного уровня, а непосредственно от компьютера к компьютеру, которые одновременно выполняют функции и сервера, и клиента.

*В-третьих*, программное обеспечение для работы с Биткойном представляет собой свободный бесплатный софт, который каждый может скачать, чтобы подключиться к сети Биткойн и работать в ней.

*В-четвертых*, Биткойн сегодня можно получить двумя путями. Приобрести за обычные деньги вне сети. В самой же сети Биткойн, что называется, добывается. Когда в сети Биткойн происходят финансовые транзак-

ции, компьютеры участников должны проводить определенные вычисления и расшифровывать криптографические сигналы. Т.е. добыча Биткойна – это расшифровка зашифрованной информации, передающейся в сети Биткойн. При этом одновременно происходит добыча Биткойнов и обеспечиваются транзакции уже существующих Биткойнов и платежи в интернет-магазинах и т.п.

*В-пятых*, это принципы эмиссии Биткойна. Уникальность Биткойна состоит в том, что его создатель, мифический Сатоши Накамото, сразу установил, что не может быть получено более 21 млн. Биткойнов. На сегодняшний день уже добыто 11 млн. Считают, что все Биткойны будут получены к 2030 году. При этом в программу заложен принцип, что скорость появления Биткойнов в сети через определенные промежутки времени сокращается в два раза. Но и это еще не все.

Для того чтобы растущее число участников сети Биткойн быстро не «выбрало» монеты, в программе автоматически постоянно усложняется криптография. Т.е. расшифровать ее становится все сложнее и сложнее. Для этого надо затрачивать все больше и больше компьютерных мощностей.

Если в первый год Биткойны добывали любители, используя обычные компьютеры с мощными видеокартами и даже игровые приставки, то теперь для добычи (майнинга) уже создаются специальные ЦОДы (центры добычи данных). На сегодняшний день мощность таких центров более чем в 250 раз превышает суммарную мощность суперкомпьютеров, эксплуатируемых во всех странах мира. Сами центры представляют собой запрятанные в бункеры комплексы мощных серверов. Чтобы создать такой центр энтузиасты Биткойна, как правило, скидываются вскладчину и создают так называемые пулы. У них просто нет иного выхода, поскольку, чтобы добыть один Биткойн в настоящее время надо затратить компьютерных мощностей в полмиллиона раз больше,

чем в начале работы системы. И это не предел. Дальше потребуется еще больше мощностей. Чтобы получить Биткойн компьютеры производят огромные вычисления, которые и позволяют дешифровать сложнейшую криптографическую программу, лежащую в основе Биткойна. При этом сама по себе добыча Биткойнов похожа на лотерею. Ни у кого никаких преимуществ нет. Компьютеры и специальные ЦОДы подключены к сети Биткойн и работают 24 часа в сутки, поддерживая транзакции и добывая Биткойны. Кому повезет – решает случай. Однако те, у кого более мощные центры, имеют и больший шанс добыть Биткойн. Вероятность добычи Биткойна равна результату деления мощности добывающего центра на совокупную мощность всех компьютеров, задействованных в сети Биткойн.

Теперь займемся хронологией событий, связанных с Биткойном. Она важна для понимания феномена криптовалюты. В апреле 2011 года, когда мифический Накамото уже изобрел и запустил в сеть Биткойн, но им интересовался только узкий круг криптоанархистов и киберпанков, состоялась встреча генерального директора Google Эрика Шмидта, директора мозгового центра Google, в прошлом политтехнолога Хиллари Клинтон, Джареда Коэна с Джулианом Ассанжем, который в то время уже находился под следствием, а его информатор Брэдли Мэннинг сидел в американской военной тюрьме.

В ходе продолжительной встречи ее участники обсуждали насущные вопросы информационных технологий, а главное, прогнозы их проникновения во все стороны жизни людей, социальных групп и целых народов. Помимо прочего, была высказана точка зрения, что в будущем самое широкое распространение в самых различных сферах получат цифровые инструменты, которые базируются на криптографии, одноранговых, или пиринговых сетях и свободном программном обеспечении. Т.е. по сути, речь шла обо всем том, что лежит в основе

Биткойна, хотя само это слово на встрече произнесено не было.

В апреле 2013 года сайт Викиликс выложил полную стенограмму встречи, и все могут убедиться, что когда еще о Биткойнах широко ничего не было известно, вопрос криптовалюты самым активнейшим образом обсуждался.

Недавно Э. Шмидт и Д. Коэн выпустили всемирный бестселлер «Новый цифровой мир». В книге есть следующие, прямо относящиеся к нашему предмету строки: «Пока мы не знаем, насколько успешными окажутся виртуальные государства (да и, в конце концов, каковы критерии их успеха?), но сама привлекательность этой концепции уже говорит в пользу постепенного ослабления могущества традиционного государства в цифровую эпоху. Можно даже ввести уникальную виртуальную валюту».

В октябре 2012 года, когда Биткойн по-прежнему оставался уделом гиков, наркоторговцев и любителей сети TOR, Европейский Центральный банк опубликовал доклад «Virtual currency schemes». В докладе Биткойн был охарактеризован как мошенническая схема, что-то подобное пирамиде, типа знаменитой в Америке и Европе схемы Поцци, предшественницы нашей МММ. В докладе утверждалось, что никаких перспектив у Биткойна нет и, не выйдя за узкий круг нарушителей закона, она быстро умрет.

Подобной точки зрения придерживалось и большинство финансистов. Более того, такой известный человек, как Саймон Дженсер, который был главным экономистом МВФ, а сейчас является профессором знаменитой Слоуновской школы бизнеса, уже осенью этого года заявлял: «Государства сделают всё для уничтожения децентрализованной цифровой валюты. Любой банкир, который видит это, должен быть очень напуган. Правительства проведут кампанию по уничтожению децентрализованной цифровой валюты, и ей скоро придет конец».

Между тем, события развернулись совершенно по иному сценарию. В самом начале августа 2013 г., федеральный судья в Техасе, при рассмотрении одного из дел впервые в судебной практике США вынес решение о том, что Биткойн является платежным средством, т.е. валютой. Впервые Биткойн был признан в качестве валюты не криптоанархистами и гиками, а представителем власти. При этом надо понимать, что судебная система США построена в значительной степени на прецедентном праве. На практике это означает, что решение судьи из Техаса, не оспоренное в вышестоящей инстанции, а этого не произошло, становится основанием для любых судебных решений на территории США.

В средине августа того же года нью-йоркский департамент по финансовым услугам также признал Биткойн в качестве виртуальной валюты. Здесь надо иметь в виду, что этот департамент подчинялся еще действовавшему тогда мэру Нью-Йорка Майклу Блумбергу, который является не только одним из самых известных политических деятелей США и миллиардером, но и владеет крупнейшей электронной системой финансовой информации, используемой во всем мире и медиа-холдингом. Понятно, что принять такое важное решение без одобрения мэра департамент не мог.

19 августа взрывается подлинная бомба. Сверхконсервативный Минфин Германии официально признал Биткойн расчетной денежной единицей, а значит, узаконил некоторые транзакции в этой валюте на территории Германии. При этом в официальном заявлении министерство финансов сообщало, что Биткойн – финансовый инструмент, который не может быть классифицирован как электронная или иностранная валюта, а больше напоминает «частные деньги», которые могут быть использованы для «многосторонних клиринговых операций». Суть такого определения состоит в том, что Минфин разрешил использовать Биткойн в любых рас-

четах, кроме расчетов с государством, включая налоги, а также вложения Биткойнов в банки в виде депозитов или других форм банковских вкладов. С учетом особенностей финансовой системы Европы, а также роли Германии в ЕС, это признание фактически открыло ворота использованию Биткойна во всей платежной зоне евро.

Касаясь причин такого необычного поведения Минфина Германии, можно выдвинуть гипотезу, что оно, возможно, связано с имеющимся по сведениям бывшего руководителя одной из разведок Германии, генерала Герда Комоссы, подтвержденного мнением ряда других высокопоставленных отставных германских чиновников, «Канцлер-актом». Этот акт в некоторых случаях позволяет ограничить суверенитет Германии в реагировании на определенные события и процессы.

В начале сентября 2013 г. Минфин Канады дал добро на открытие сети банкоматов по обмену Биткойнов в крупнейших городах страны.

В середине октября главный интернет-поисковик Китая Baidu, принадлежащий государству, объявил о том, что он принимает Биткойны в расчет за различные платные сервисы. Его примеру последовали и крупнейшие китайские интернет-магазины. Надо отметить, что еще летом ряд ведущих международных торговых платформ, типа eBay, Amazon заявили о том, что в ближайшем времени они будут готовы широко принимать Биткойны.

В середине ноября 2013 г. состоялись слушания по вопросу о Биткойне в Комитете по национальной безопасности Сената США. Хотя такого рода заседания не предполагают принятия каких-либо нормативных и обязывающих документов, тем не менее, результаты заседаний, высказанные в ходе их мнения, а тем более, письменные заключения, играют в деловой и политической жизни Америки и мира огромную роль.

В ходе заседания госагентства США ответили на запрос Комитета Сената по поводу Биткойна. Основной

вывод их отчетов – цифровая валюта является законным финансовым инструментом, а ее широкое использование несет значительные выгоды потребителям. При этом Петер Кадзик, главный заместитель Генпрокурора, написал в отчете: «Подход ФБР к виртуальным валютам исходит из того, что электронные платежные системы, как централизованные, так и децентрализованные, предлагают законные финансовые услуги... Как и любая финансовая услуга, системы цифровых валют могут быть использованы для незаконной деятельности, хотя централизованные и децентрализованные платежные системы могут различаться по типу и степени рисков, которые они представляют с точки зрения незаконной финансовой деятельности».

На совещании сообществу Биткойн было рекомендовано, так или иначе, в течение обозримого времени присоединиться к Financial Crimes Enforcement Network и включиться в систему мер по противодействию отмыванию преступных доходов. От лица сообщества на совещании присутствовал руководитель Bitcoin Foundation Патрик Марк.

Наиболее важной, как для настоящего, так и для будущего Биткойна была позиция ФРС, изложенная в письме за подписью ее председателя Бена Бернанке. Он сообщил: «Несмотря на то, что Федеральная резервная система в целом следит за развитием событий в сфере виртуальных валют и других инновационных платежных систем, мы не имеем права непосредственно контролировать или регулировать эти нововведения или компании, которые предоставляют их на рынке». При этом в письме отмечено, что Биткойн – это «виртуальная валюта, которая может рассматриваться в качестве одной из форм «электронных денег» или технологии платежной системы, которые развиваются на протяжении последних 20 лет». Тем самым, Бернанке не только осторожно, но достаточно ясно одобрил Биткойны, но и, что гораз-

до более важно для дальнейшего, признал, что они не подпадают под юрисдикцию ФРС и представляют собой не просто расчетное средство, не просто технологию онлайн платежей типа кредитной карты, а могут являться «электронными деньгами».

В самом начале декабря 2013 г. Биткойн поддержал Банк Англии. Он санкционировал выпуск Королевским монетным двором Великобритании памятных монет, номинированных в Биткойнах для мини-государства Олдерни, входящего в состав Нормандских островов, и находящихся под суверенитетом Британской короны. Банк Англии фактически пошел дальше всех. Памятную монету, которая, тем не менее, является обычными деньгами маленького островного государства, он разрешил номинировать в Биткойны, т.е. признал их, по сути, полноценными деньгами.

На фоне осторожной поддержки Биткойна ФРС, министерствами финансов Германии, Канады, Банком Англии, Китай занял иную позицию. 5 декабря 2013 г. Народный банк Китая и еще пять министерств высказали свою позицию по криптовалюте Биткойн. В опубликованном документе в частности говорится, что «в целях защиты прав собственности и интересов общества, для защиты правового статуса юаня как валюты, чтобы предотвратить риски отмывания денег и поддерживать финансовую стабильность... уведомляем, что Bitcoin не является валютой или заменой денег, не имеет правового статуса и денежного эквивалента, не может и не должна использоваться в качестве денег при обращении на рынке. По сути, это всего лишь специфический виртуальный товар. Финансовым учреждениям не разрешается принимать и проводить платежи в Биткойнах, как если бы это была официальная валюта. Интернет-сервисы должны соблюдать все правила по противодействию отмыванию средств, полученных незаконным путем». Китайский банк своим письмом создал интересную конструкцию.

Он отметил, что Биткойн не является деньгами ни в каком смысле, но согласился, что она представляет собой товар и может быть использована для платежей в китайских интернет-магазинах и сервисах. Каждый, кто учил политэкономию по Марксу, или экономикс по Бену Бернанке (Б. Бернанке не только был председателем ФРС, но и является автором самого популярного учебника), знает формулы Товар-Деньги-Товар или Деньги-Товар-Деньги. Деньги являются ничем иным, как специфическим товаром. Поэтому Народный банк Китая пошел своим особым путем. С чем связан этот путь, и почему он такой извилистый, мы расскажем ниже.

При этом Китай подчеркнул, что разрешает своим гражданам покупать и продавать Биткойны, а сервисам и интернет-магазинам осуществлять расчеты в них. Но делать они должны это на свой страх и риск и Национальный банк Китая ответственности за это не несет. Интересно, что позиция Китая изменилась буквально в последние недели, поскольку еще в ноябре представители китайской Биткойн-биржи BTC China провели успешные переговоры о потенциальном развитии Биткойна, как региональной валюты.

С учетом того, что китайские интернет-сервисы и магазины продолжают работать с Биткойнами, а гражданам разрешены операции с ними, ключевым в заявлении представляются слова о том, что «Биткойн не является валютой или заменой денег».

В целом в 2013 году курс Биткойна заоблачно вырос, и на своем пике достиг 1100 долларов за 1 Биткойн. После заявления Национального банка Китая курс упал менее чем до 600 долларов за 1 Биткойн. В 2014 г. по Биткойну был нанесен еще один мощнейший удар. Он связан с закрытием крупнейшей Биткойн-биржи MtGox, владельцы которой украли или позволили украсть сторонним хакерам средств на сумму более 140 млн. долларов. Многие финансовые эксперты и журналисты опубликовали мате-

риалы о кончине Биткойна. Однако этого не произошло. Биткойн устоял. Более того, его курс стабилизировался в интервале 400-500 долларов за 1 Биткойн, а объемы торгов продолжают стремительно нарастать. Все это позволяет сделать вывод о том, что криптовалюты обладают несомненным потенциалом развития даже вне зависимости от судьбы конкретного их вида – Биткойна.

### 5.2. Криминология Биткойна

В течение первых двух-двух с половиной лет после появления Биткойна, он интересовал практически только шифропанков, хакеров, криптоанархистов и сетевых либертарианцев. Соответственно, главным местом использования Биткойна в качестве платежного средства была сеть Tor. Именно эта сеть является прибежищем маргинальных и криминальных киберсубкультур.

Сеть Tor создана разведкой ВМФ США для осуществления специальных операций в киберпространстве. В 2003 году проект был рассекречен, переведен в ранг свободного софта и пущен в вольное плавание. При этом основная команда разработчиков плавно перешла из разведывательных структур в специально созданный фонд. А проект, наряду с прочими, продолжили финансировать агентство Пентагона DARPA, Американский научный фонд, тесно связанный с разведывательным сообществом, Google, одно из шведских правительственных агентств и целый ряд других организаций. На словах заявляется, что эта сеть, по своим компьютерным составляющим весьма близкая к сети Биткойн, должна помогать демократическим группам и диссидентам в их борьбе против тоталитарных режимов.

Однако на деле вышло иначе. Tor стал, по сути, криминогенной сетью. Не так давно ведущий эксперт ЕС в области компьютерной безопасности Пьерлуиджи Паганини провел наиболее полное на сегодняшний день исследование, относительно структуры ресурсов Tor.

Согласно его итогам самую большую долю в сети Tor занимают хакерские ресурсы, где содержится либо различного рода документация, либо объявления о продаже хакерских инструментов и программ с их кратким описанием. На долю таких ресурсов приходится 28% от общего числа сайтов.

Устойчивое второе место занимают ресурсы, относимые к киберпреступности, где первенствуют продажи оружия, краденных кредитных карт, наркотиков, живого товара, трансплантатов и т.п. Таковых 23%.

На почетном третьем месте – ресурсы, связанные с терроризмом: от сайтов знаменитых террористических организаций всех стран и идеологических ориентаций, до учебников, как изготовить смертельный вирус или самостоятельно произвести мощную бомбу. Таковых в сети Tor 17%.

Если прибавить к откровенно преступным ресурсам еще и 4%, приходящиеся на ресурсы с педофильским и порно контентом, то Tor на 72% состоит из откровенно криминальных ресурсов, подпадающих под уголовное законодательства практически всех стран мира.

Соответственно, Биткойн в первые годы своего существования превратился в своего рода валюту сети Tor. В полном объеме это проявилось в октябре 2013 года, когда ФБР арестовало владельца крупнейшей торговой площадки Tor – интернет-магазина SilkRoad Уильяма Ульбрихта. Главным товаром магазина были наркотики. Хотя здесь же можно было купить оружие, хакерские программы и многое другое. Общий оборот магазина за время его существования составил более 1,2 млрд. долларов по курсу Биткойнов на момент закрытия магазина. При аресте У. Ульбрихта у него было изъято 144 тыс. Биткойнов, а еще 111 тыс. Биткойнов реквизировано ЦРУ в электронном кошельке, принадлежность которого Ульбрихту не установлена. В совокупности с ранее изъятыми из различных источников Биткойнами, ФБР на

сегодняшний день принадлежит чуть меньше 5% всей криптовалюты, находящейся в обороте.

Операция SilkRoad побудила многих экспертов за рубежом и в нашей стране назвать Биткойн криптовалютой наркомафии. Но это далеко не так. Реальный мир гораздо сложнее. Еще в конце 2011 года В.П. Иванов, глава ФСКН РФ, выступая на крупнейшей конференции, организованной ведущей «фабрикой мысли» в Вашингтоне, сказал буквально следующее:

«Анализ показывает, что в условиях кризиса хроническая нехватка ликвидности и стремление удержаться наплаву стимулирует не только толерантность к криминальным деньгам, но и поощрительное отношение к их наличию.

Более того, именно это обстоятельство, то есть, возможность перманентного восполнения столь необходимой ликвидности, – во многом является движущей пружиной финансово-экономического и социального заказа на продолжение наркопроизводства.

Наркоденьги и глобальный наркотрафик при этом являются не просто значимыми частями, но, выступая донорами столь дефицитной ликвидности, по сути, являются жизненно необходимым, неотъемлемым сегментом всей монетарной системы».

То есть, по сути, наркоденьги пронизывают всю мировую финансовую систему. По словам В.П. Иванова: «Общий размер потоков грязных денег транснациональной организованной преступности оценивается... более чем в триллион долларов, или в 1,5% от глобального ВВП, причём, не менее 70% этих денег отмывается через финансовые институты».

Иными словами, Ужасный пират Роджерс, в миру Уильям Ульбрихт, не более чем детсадовец, по сравнению с топ-менеджментом крупнейших мировых банков. А широко разрекламированная операция SilkRoad с изъятием Биткойнов, – это мелкая акция на фоне ежеднев-

ных операций с наркоденьгами системообразующих финансовых институтов.

В условиях ажиотажного спроса на Биткойны постоянно приходят сообщения о многочисленных кражах так называемых электронных кошельков Биткойнов, а также иного рода мошенничествах, связанных с криптовалютой. Надо сказать, что сеть Биткойн, требующая определенных знаний в информационных технологиях и компьютерных навыков, предоставляет широкие возможности для хакеров извлекать деньги у технически неподкованных пользователей.

При этом необходимо подчеркнуть, что Биткойн также не является уникальным феноменом. С широким распространением в самых различных сферах бизнеса и повседневной жизни информационных и других высоких технологий, значительно расширяются возможности для преступности. Пользователи различного рода программ, сервисов, высокотехнологичных бытовых устройств все чаще не обладают необходимыми знаниями об особенностях их эксплуатации, способах работы, различного рода каналах доступа к ним и т.п. При этом, в отличие от пользователей, преступники, оперирующие в сфере высоких технологий, как правило, имеют высокий образовательный и профессиональный уровни, знают до тонкостей все технические и программные составляющие объектов криминальной активности.

Любые новые информационные и технические решения резко расширяют сферу применения киберпреступности и создают условия для повышения эффективности деятельности криминальных хакеров. По этой причине киберпреступность в мире растет более быстрыми темпами, чем все иные виды преступности. Если еще в конце 2012 года размеры мирового ущерба от киберпреступности оценивались на уровне примерно 200 млрд. долларов, то в 2013 году, по различным независимым оценкам сумма уже составляет около 300 млрд. долла-

ров. С учетом объема капитализации Биткойна, понятно, что преступность с криптовалютой пока является каплей в море. Хотя это слабое утешение для уже не сотен, а тысяч инвесторов, обманутых хакерами, специализирующихся на Биткойн-кошельках.

По мнению экспертов «Лаборатории Касперского», «Киберпреступники, как и инвесторы, собираются там, где нажива. Думаю, вы уже догадались, что недостатка в нападениях на цифровую валюту не было. Есть даже вредоносная программа, которая атакует Биткойны с использованием бот-сетей и троянов, пытается скомпрометировать «кошельки Bitcoin» или даже выпотрошить их. Ботнет Kelihos содержал встроенную функцию кражи Bitcoin. А ранее в этом году был обнаружен образец вредоносной программы, объединяющей компьютеры в бот-сеть для майнинга (добычи) Биткойнов, а распространялся червь через Skype».

Особо быстрыми темпами растут крупномасштабные мошенничества, связанные с Биткойнами. Так в конце октября 2013 года китайский обменник GBL просто исчез, а вместе с ним – 4,1 млн. долларов в Биткойнах. Потом 1,2 млн. долларов, украли из австралийского хранилища inputs.io. Спустя еще неделю были обворованы европейские кошельки Bidextreme.pl и Bitcash.cz (украдено не менее 100 тыс. долларов), а недавно платежный сервис BIPS потерял 1 млн. долларов во время DDoS-атаки.

Но все это меркнет перед аферой с Биткойнами, которая была проведена в декабре 2013 года. 96 тыс. Биткойнов, а это почти 100 млн. долларов, по состоянию на текущий момент, было выведено со счетов клиентов, поставщиков и администраторов сайта SheepMarketplace (SMP), расположенного в сети Tor. SMP был одной из главных площадок, пришедших на замену SilkRoad. Теперь в результате аферы закрыт и сам SMP. На данный момент известно, что злоумышленнику (одиночке или группе людей) удалось подделать остатки средств на

счетах пользователей, показывая, что у них были Биткойны в электронных кошельках, хранящихся на ресурсе, в то время как на самом деле кошельки уже опустошены, а средства уже переведены. В течение недели весь сайт планомерно опустошался, а когда администрация сайта поняла, что что-то происходит, и закрыла площадку, со счетов пользователей было списано гигантское количество средств. Эта афера стала одним из крупнейших похищений в истории и стоит в одном ряду с крупными «реальными» преступлениями, такими как кража алмазов на 108 млн. долларов в магазине Harry Winston в Париже в 2008 году.

Достаточно интересно, что крупномасштабные аферы или успешное завершение операций, связанных с кибермошенничеством, где фигурируют Биткойны, типа закрытия ресурса SilkRoad, могут и не повлиять на курс Биткойна, а также на его распространение в качестве платежного средства. Как говорил по другому поводу почти 150 лет назад Карл Маркс: «Перед жаждой наживы не устоит ни один страх, ни одно другое стремление буржуа». Кроме того любая крупная реквизиция уменьшает количество Биткойнов в свободном обороте и соответственно даже при неизменном спросе увеличивает их курс.

Крупнейшей аферой, связанной с Биткойнами является, несомненно, крах Биткойн-биржи номер один MtGox. В последние недели существования биржи, ее руководство пыталось уверить инвесторов в том, что неизвестные хакеры похитили у них Биткойны на сумму более чем 119 млн. долларов. Затем биржа закрылась с общим долгом более 140 млн. долларов. Проведенный аудит и мероприятия правоохранителей показали прямую вину хозяев биржи в случившемся. Все руководство биржи, ее учредители были арестованы.

Несомненно, серьезной проблемой, связанной с Биткойном, стало ее использование для вывода и инве-

стирования «грязных денег». По данным наиболее известной и осведомленной структуры в области оценки и отслеживания нелегальных финансовых потоков Global Financial Integrity, за 2001-2011 годы из стран БРИКС а также развивающихся стран было выведено нелегальным образом более 6 трлн. долларов. Первенство по выводу держит Китай. По имеющимся оценкам, в настоящее время только на зарубежных счетах хранится от 500 до 700 млрд. долларов нелегальных денег китайских граждан.

В конце ноября один из руководителей Global Financial Integrity Е. Фаган опубликовал в американской прессе статью «Биткойн и международная преступность». В статье он отметил, что дальнейшее развитие системы Биткойн возможно только в том случае, если держатели кошельков Биткойн перестанут быть анонимными, и будут заключены соответствующие договоры между системой Биткойн и органами, контролирующими легальность денежных переводов и происхождения денег.

Представляется, что Народный банк Китая, учитывая масштабы нелегального вывода капитала из страны, при публикации своего заявления руководствовался, прежде всего, функцией Биткойна как анонимной платежной системы. Поэтому Народный банк Китая запретил именно банковские операции с Биткойном, т.е. превращение привычных денег в Биткойны.

Далее хотелось бы обратить внимание на одну интересную особенность Биткойна. Если разбираться в технических деталях проекта Биткойн, то несложно понять, что между платежной системой Биткойн и любыми другими традиционными платежными системами имеется одно, но очень принципиальное отличие. Межбанковские системы, типа SWIFT, системы кредитных карт или платежные системы типа Qiwi, Yandex и т.п. не могут контролироваться клиентами. Все производимые в них транзакции являются секретными, зашифрованными и

известны лишь процессинговым центрам, т.е. либо хозяевам компании, либо, как в случае со SWIFT, уполномоченному органу.

Система Биткойн является анонимной, но не по критерию транзакций, а по критерию владельцев счетов. Т.е. если речь не идет об АНБ или нарушении закона, то обычная банковская система на сегодняшний день анонимна по факту в квадрате. Во-первых, законы пока еще не запрещают во многих странах держать анонимные счета. Например, в оффшорах на номинального директора. Во-вторых, сами по себе переводы для тех, кто находится вне системы или является простым ее клиентом, неизвестны, т.е. анонимны. Между тем, «историю жизни» каждого Биткойна можно отследить вплоть до каждой транзакции с момента рождения монеты. При этом все участники этих транзакций остаются для системы анонимными. Идентификатор электронного кошелька генерируется самим пользователем, а количество создаваемых кошельков ничем не ограничено – хоть делай новый кошелёк на каждую очередную транзакцию.

В сети Биткойн каждому ее участнику, является ли он пользователем кошелька или передающим центром, могут быть известны при его желании абсолютно все осуществленные транзакции. Как говорят специалисты, такая ситуация позволяет вести в режиме реального времени полный сетевой анализ системы Биткойн. Еще более важно, что анализ можно проводить не только в режиме реального времени, но, строго говоря, с момента появления сети.

Более того, анонимность владельцев кошельков Биткойн является таковой лишь до того момента, пока не происходит обмен Биткойна на традиционные валюты, либо реализация за Биткойны товаров и услуг вне сети Tor, в законопослушном секторе экономики, т.е. в подавляющей части интернет- и обычных магазинах, сети обменников, на биржах, в банках и т.п. В настоящее вре-

мя в большинстве государств банки, другие финансовые институты, а иногда и торговые структуры обязаны при наличии запроса предоставлять информацию о покупателях. Более того, часть этой информации мониторится в автоматическом режиме. Не сложно также понять, что достаточно жесткие рекомендации Комитета по национальной безопасности Сената США, мнение бывшего главы ФРС Б. Бернанке и в определенной мере заявление Народного банка Китая как раз и принуждают сообщество Биткойн отказаться от анонимизации кошельков и раскрыть их владельцев.

Лучшим доказательством этой гипотезы является тот факт, что буквально спустя несколько дней после решения Народного банка Китая, крупнейшая биржа Биткойнов BTC China, расположенная в Китае, сообщила клиентам: «В ответ на недавнее изменение политики, BTC China в настоящее время требует от пользователей представить идентификацию или номер паспорта. Существующие пользователи должны предоставить эту информацию при открытии каждой торговой сессии. Приносим свои извинения за предоставленные неудобства».

Тем самым, строго говоря, Биткойн при широком его распространении и выходе за пределы маргинальной субкультуры и торговли в сети Tor становится не более, а менее анонимной платежной системой, чем используемые ныне системы, связанные с традиционными валютами.

Существует еще один тонкий момент. Криминогенным, но не всегда юридически наказуемым, является наличие в экономической системе или институте неких скрытых и особенно сознательно скрываемых правил, условий и процедур, позволяющих манипулировать системой в ущерб ее участникам, целенаправленно нарушая внутренние, объявленные правила ее функционирования. Существуют некоторые подозрения, что система Биткойн имеет подобный недостаток. Исследователи из

Корнельского университета Иттай Эяль и Эмина Ган Сирер опубликовали статью, в которой говорится о принципиальных недостатках системы Биткойн, которые могли бы дать относительно небольшой группе участников сети возможность получить значительный уровень контроля над системой. Кроме того, исследователи указали, что если эта группа «майнеров-эгоистов» получит контроль над более чем 25% мощностей Биткойн, то они смогут отменять проведенные платежи и делать бесполезными усилия других участников системы по майнингу (добыче Биткойнов).

«Иттай Эяль и я набросали примерный план нападения, при котором небольшая группа «шахтеров» может получить доходы, превышающие их положенную долю, и продолжит расти до критической точки. После чего стоимость Биткойн-предложения начинает резко снижаться из-за того, что оно контролируется одним лицом, которое определяет, кто может участвовать в операции, какие сделки совершать, а также может даже получить определенный процент от совершенных сделок. Это снежный ком, который будет расти и развиваться не по причине появления какого-то злодея, как в фильмах о Бонде, а вследствие того, что кто-то захочет заработать чуть больше, чем остальные», – пишут исследователи в своем блоге.

Относительно системы Биткойн пока только высказываются предположения о возможных встроенных механизмах криминализации. Более того, целый ряд разработчиков и программистов уже предложили свои решения, как избежать этой проблемы и устранить выявленные «дыры» и недоработки. Между тем, в мире реальных, а не виртуальных валют 15 крупнейших банков оказались под подозрением американских, британских, европейских и гонконгских регуляторов и правоохранительных органов. Регуляторы интересуются действиями следующих банков: Barclays, Citigroup, Deutsche Bank,

Goldman Sachs, HSBC, JP Morgan, Morgan Stanley, Royal Bank of Scotland, Standard Chartered и UBS. Еще пять банков пока не раскрываются. Речь идет о манипуляциях на рынке с ежедневным оборотом в 4 трлн. долларов. Более того, мошенничества на рынке Forex являются лишь звеном в цепи криминальных нарушений крупнейшими банками практически на всех основных финансовых рынках, включая рынки золота, межбанковских кредитов и ипотечных бумаг. Банки платят уже миллиардные штрафы и неустойки в результате наложенных на них санкций. Так что криптовалюте Биткойн очень далеко до обычных и вроде бы легальных и добропорядочных доллара, фунта, евро и т.п.

Несколько слов о Биткойне в России. По имеющейся информации российские инвесторы по объемам покупок на спекулятивном рынке Биткойнов занимают третье место после американцев и китайцев.

В этой связи следует подчеркнуть, что на территории Российской Федерации Биткойн не может являться законным платежным средством. Соответственно, любые операции купли-продажи, использующие Биткойны как платежное средство, являются противозаконными. Дело в том, что в статье 75 Конституции Российской Федерации денежной единицей называется рубль, эмиссию которого вправе осуществлять только Банк России. Введение и эмиссия других денег в Российской Федерации прямо запрещена». Кроме того, Федеральный закон «О Банке России» запрещает выпуск «денежных суррогатов» – то есть знаков, вводимых организациями или гражданами самовольно и выполняющих все или некоторые функции законной денежной единицы. Примером могут служить появившиеся во время перестройки «уральские франки», или недавние «шаймуратики», которыми расплачивались в селе Шаймуратово Республики Башкортостан.

Нормативные документы относительно использования Биткойна в России, по состоянию на весну 2014 года

отсутствуют. Единственным, если можно так выразиться официальным документом относительно Биткойна, является информация пресс-службы Центрального банка Российской Федерации «Об использовании при совершении сделок «виртуальных валют», в частности, Биткойн». В информации указано: «Банк России отмечает, что в последнее время в мире получили определенное распространение так называемые «виртуальные валюты», в частности, Биткойн. По «виртуальным валютам» отсутствует обеспечение и юридически обязанные по ним субъекты. Операции по ним носят спекулятивный характер, осуществляются на так называемых «виртуальных биржах» и несут высокий риск потери стоимости.

Банк России предостерегает граждан и юридических лиц, прежде всего кредитные организации и некредитные финансовые организации, от использования «виртуальных валют» для их обмена на товары (работы, услуги) или на денежные средства в рублях и в иностранной валюте.

Согласно статье 27 Федерального закона «О Центральном банке Российской Федерации (Банке России)» выпуск на территории Российской Федерации денежных суррогатов запрещается.

В связи с анонимным характером деятельности по выпуску «виртуальных валют» неограниченным кругом субъектов и по их использованию для совершения операций граждане и юридические лица могут быть, в том числе непреднамеренно, вовлечены в противоправную деятельность, включая легализацию (отмывание) доходов, полученных преступным путем, и финансирование терроризма.

Банк России предупреждает, что предоставление российскими юридическими лицами услуг по обмену «виртуальных валют» на рубли и иностранную валюту, а также на товары (работы, услуги) будет рассматриваться как потенциальная вовлеченность в осуществление со-

мнительных операций в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».

### 5.3. Есть ли сила у Биткойна

Ключевым вопросом для понимания Биткойна является определение его экономической природы. В конечном счете, любое экономическое явление представляет собой отношения между людьми по поводу производства, обмена, распределения, потребления различного рода продуктов и услуг, а также их производных в условиях ограниченности ресурсов. Поэтому необходимо понять, какие отношения устанавливает, а какие отменяет Биткойн. Это поможет выяснить, кто стоит за сетью, кто в Биткойне заинтересован, а кто нет. И, наконец, какие силы пытаются использовать это явление в своих интересах.

Едва ли не главный вопрос это – выяснение, является ли Биткойн деньгами/валютой, или нет. Сам мифический Сатоши Накамото дал понимание природы Биткойна в названии своей главной статьи – «Биткойн: цифровая пиринговая наличность». Наличность – это, конечно же, деньги. При этом Накамото объединил в Биткойне собственно валюту с платежной системой. В той же статье он в частности указывал: «Необходима платежная система, основанная на криптографии, а не на доверии, которая позволила бы любым двум участникам осуществлять перевод средств напрямую, без участия посредников». В качестве валюты он предлагал использовать «электронную монету, как последовательность цифровых подписей».

Биткойн, по мнению участников этой сети, выступает электронной валютой и платежной системой в одном флаконе. Известно, что современный термин «валюта» происходит не столько от итальянского наименования

мелкой монеты valuta, сколько от более древнего латинского слова valere. Оно означало – «быть сильным», «иметь возможность», «обеспечить получение», «приобретение» и происходило от индоевропейского корня «вал». «Вал» же имел, по сути, единственное значение – «быть сильным», «самый сильный». По сути, любая валюта, в конечном счете, обеспечивается уровнем доверия, широтой распространения и силой, стоящей за ней. И Биткойн – не исключение.

Следует подчеркнуть, что подавляющее большинство регуляторов вне зависимости от степени благожелательности к Биткойну, прямо не признают ее полноценными деньгами. Так, достаточно лояльно настроенное к Биткойну министерство финансов Германии утверждает, что «Биткойн – это финансовый инструмент, который не может быть классифицирован как электронная или иностранная валюта, а больше напоминает «частные деньги», которые могут быть использованы для «многосторонних клиринговых операций».

Когда представителя Минфина Германии попросили объяснить, в чем состоит различие между валютой и законным платежным средством для многосторонних клиринговых операций, он отметил, что с Биткойном нельзя проводить банковские операции и можно использовать только в расчетах между гражданами или компаниями.

При общем положительном отношении в Биткойну любопытную позицию заняли госагентства США и особенно ФРС на слушаниях в комитете Сената по поводу Биткойна. Они назвали Биткойн цифровой валютой и отметили, что она является законным финансовым инструментом. На это в частности указал представитель ФБР. Что же касается конкретно ФРС, то в письме, подписанном Б. Бернанке, применительно к Биткойну употребляются термины «виртуальная валюта» и «инновационная платежная система». Налоговая службы США в 2014 году однозначно отнесла Биткойн не к валюте, а к вполне ле-

гальной собственности или активам. Весьма терпимо отношение к Биткойну у министерства финансов Великобритании.

Совершенно иную позицию заняли многие другие страны. Об отношении ЦБ России писалось выше. Народный банк Китая жестко заявил, что «Биткойн не является валютой или заменой денег, не имеет правового статуса и денежного эквивалента, не может и не должна использоваться в качестве денег при обращении на рынке. По сути, это всего лишь специфический виртуальный товар. Финансовым учреждениям не разрешается принимать и проводить платежи в Биткойнах, как если бы это была официальная валюта. Интернет-сервисы должны соблюдать все правила по противодействию отмыванию средств, полученных незаконным путем».

Столь же жестко отказали в праве Биткойну быть валютой – хоть цифровой, хоть виртуальной, хоть какой-либо еще – министерства финансов Франции и Норвегии. Такая позиция Китая, ряда европейских стран, Казахстана и некоторых других, базируется, прежде всего, на решительном отказе в праве каким-либо институтам, либо сообществам эмитировать деньги или валюту. Они четко исходят из посылки, что это является исключительной прерогативой либо государства, либо надгосударственной структуры (как в случае с евро), которой свое суверенное право добровольно передали государства.

Заметно различаются позиции в отношении Биткойна и у крупнейших мировых банков и инвестиционных фондов. Например, Bank of America и City Bank высоко оценивают перспективы Биткойна. В то же время многие иные банки заявили о своей неготовности работать с Биткойном, в значительной мере в силу его высокой волатильности и рискованности как финансового актива.

Таким образом, налицо несомненный раскол регуляторов и других финансовых институтов, отражающих общий раскол в мировой элите относительно крипто-

валюты. Наличие любого раскола показывает, что соответствующий социально-экономический процесс зашел достаточно далеко. В подобных случаях возможность торможения процесса, а тем более поворот его вспять всегда вероятностен и зависит от динамично меняющегося баланса противоборствующих сил.

В этой связи целесообразно посмотреть, чем фактически является на сегодняшний день сеть Биткойн. Каковы ее проявившиеся достоинства, в чем состоят документировано подтвержденные недостатки. Какова политэкономическая подоплека этого явления, т.е. какие отношения между людьми, их группами и т.п. стоят за ней.

Следует отметить, что, несмотря на бурные темпы развития, в общем и целом Биткойн, как собственно платежный и финансовый инструмент, не приобрел сколько-нибудь широкого распространения. При удвоении ежемесячно числа торговых точек, принимающих Биткойны, на сегодняшний день вне сети Tor таких насчитывается чуть более тысячи. По разным оценкам, только от 2 до 5% Биткойнов за время его существования участвовало в торговых операциях за пределами сети Tor и выступало как платежное средство за легальные товары и услуги, исключая обмен на традиционные валюты (доллары, евро, фунты, юани и пр.).

Биржевые операции с Биткойном в настоящее время проводят около 50 электронных биржевых площадок и обменников. Все успехи Биткойна связаны с его функцией, как спекулятивного финансового актива. За период с апреля 2010 года по декабрь 2013 года курс Биткойна против доллара вырос в 400 тыс. раз, с трех центов во время первой транзакции в апреле 2010 года до почти 1200 долларов за один Биткойн на пике в декабре 2013 года. А потом «рухнул» до 400-450 долларов к весне 2014 года. В этом смысле, очевидно, что финансовые регуляторы, даже благожелательно настроенные к Биткойну, например, США и Великобритании, абсолютно

правы, когда относят ее к рискованным финансовым инструментам.

Теперь рассмотрим очевидные достоинства сети Биткойн.

*Во-первых*, Биткойн обладает очень низкими, стремящимися к нулю транзакционными издержками для всех участников сети, включая плательщиков, торговые точки, владельцев бирж и т.п. Многими независимыми экспертами рассчитано, что платежи, осуществляемые в Биткойнах, намного дешевле платежей с использованием всех других известных платежных систем, включая кредитные карты, электронные системы типа PayPall или Яндекс.Деньги, а также системы, типа Western Union.

Чрезвычайно важно, что низкие транзакционные издержки несут не только плательщики, но и те, кто принимает платежи, т.е. интернет-магазины, биржи и т.п. Им не нужно разворачивать специальные программные модули, заниматься сопряжением интернет-магазинов, электронных торговых площадок с электронными платежными системами и т.п., вести отнимающий много времени и требующий денежных затрат документооборот.

*Во-вторых*, с каждым месяцем использование сети Биткойн становится проще и доступнее для всех ее участников. В отличие от процедур получения кредитных карт, открытия счетов в традиционных платежных системах, отнимающих время, требующих определенных навыков и т.п., в сети Биткойн все упрощено. Это обстоятельство потенциально делает сеть доступной для самых широких слоев населения, в том числе бедных людей, которым банки отказываются заводить кредитные карты и т.п. Предельно упрощен и сам порядок проведения платежа.

*В-третьих*, система Биткойн базируется на так называемом «золотом стандарте» программного кода и, будучи свободным софтом, развивается постоянно растущим сообществом высококвалифицированных

программистов. По сути, модель совершенствования программного обеспечения Биткойна подобна модели развития Linux. В рамках этой модели обнаруживаемые недочеты постоянно устраняются всем сообществом. Каждый участник сообщества вправе предложить свое решение, расширить базовый функционал и т.п. За счет того, что исходный программный код Биткойна очень гибок, он позволяет генерировать самые разнообразные решения. В результате многие недостатки или несовершенства функционала системы Биткойн устраняются буквально на глазах. К такого рода недостаткам относилась, например, невозможность отменить уже совершённую транзакцию. Сегодня есть решения, позволяющие в случае, если участники транзакции согласны на ее отмену, при несоблюдении тех или иных условий сделки, практически сделать это. Также недавно появилась функция осуществления сделок с использованием залогов.

Внимательно анализируя достоинства сети Биткойн несложно обнаружить, что все они относятся не к валюте Биткойн, а к сети Биткойн, как платежной системе.

Теперь наступила очередь недостатков Биткойна, как платежного средства. В первую очередь, традиционно говорят об анонимности, а соответственно широких возможностях использования Биткойна для отмывания преступных и коррупционных доходов. Любой непредубежденный человек, конечно же, согласится с данным утверждением, но не преминет отметить, что не только наличные деньги, но и привычные безналичные электронные расчеты представляют для отмывания не меньшие возможности. Могут возникнуть сомнения относительно утверждения о малой подконтрольности безналичного оборота. Однако, как показывают данные независимых организаций, а также агентств различных стран по противодействию отмыванию преступных доходов, только тотальный контроль над электронными платежами, как на уровне стран, так и на трансграничном

уровне может частично решить эту задачу. А тотального контроля пока нет.

Другой недостаток системы Биткойн, по мнению некоторых экспертов, состоит в том, что Биткойн имеет дефляционную природу. Размеры эмиссии ограничены, а рынок растет. Соответственно растет и потребность в платежном средстве. Как следствие, стоимость валюты в этом случае должна все время возрастать, т.е. наблюдаться дефляция. В то же время хорошо известно, что дефляция, как правило, сопровождается стагнацией, а соответственно не позволяет расширять экономику, оперирующую Биткойнами. Следует отметить, что само по себе ограничение размеров эмиссии не может привести ни к дефляции, ни к инфляции. Все зависит от емкости рынка, где используются Биткойны, т.е. количества субъектов хозяйственной деятельности, оперирующих этим платежным средством, и объемов деятельности. Математико-алгоритмическое ограничение эмиссии само по себе никак не связано с динамикой стоимости валюты и поэтому не может рассматриваться ни как достоинство, ни как недостаток платежного средства.

Реальные недостатки Биткойна, как платежного средства, лежат в иной плоскости. Причем, эти недостатки имеют не абстрактно-вычислительную природу, а связаны с реалиями сегодняшнего дня, конкретными условиями существования системы Биткойн. Главный из них проявляется как сверхспекулятивная природа Биткойна, его чрезвычайно высокая волатильность и способность к созданию гигантского пузыря.

Чтобы глубже понять этот ключевой недостаток, необходимо сделать краткий экскурс в современную денежную теорию. Как известно, марксистская теория денег выделяет пять функций денег: мера стоимости, средство обращения, средство образования сокровищ, средство платежа и мировые деньги. Неоклассическая школа, или как ее сегодня называют «экономикс», в лице

виднейших своих представителей С. Фишера, Р. Дорнбуша, Р. Шмалензи, признает четыре функции денег: первая – средство обмена и средство платежа, вторая – единица счета, третья – средство сохранения стоимости, четвертая – мера отложенных платежей.

В своем «Трактате о денежной реформе» Дж. Кейнс определяет деньги «как прокламируемое государством законное платежное средство для выполнения денежных обязательств». Позднее в «Общей теории занятости, процента и денег» он выдвинул на первый план функцию денег как средства сохранения стоимости в качестве наиболее ликвидного актива. В дальнейшем теорию денег применительно к постбреттонвудскому периоду в своих поздних лекциях сформулировал виднейший представитель неортодоксального посткейсианства Х.Ф. Мински. Опираясь на работы Дж. Кейнса, учитывая труды К. Маркса и переосмысливая реалии финансового капитализма, он выделил, наряду со счетной, четыре ведущих функции денег:

*Во-первых*, средство платежа, обслуживающее текущие торговые операции. Т.е. операции купли-продажи товаров, услуг в самых различных секторах экономики, за исключением сектора капитальных благ, или упрощенно – прямых инвестиций.

*Во-вторых*, инвестиционное средство. Это деньги, затрачиваемые на приобретение инвестиционных товаров с целью создания новых или расширения/модернизации действующих производств, компаний и т.п. Их еще называют деньгами для приобретения капитальных благ. Фактически эти средства направляются на расширенное воспроизводство.

*В-третьих*, средство спекуляции. Это деньги, используемые как актив, либо затрачиваемые на приобретение производных финансовых инструментов с целью получения прибыли в результате динамики цен на активы. По-русски говоря, спекулятивные средства – это

средства для проведения операций – купить дешевле, чтобы продать дороже.

*В-четвертых*, средство сбережения. Принципиально мыслимо, что средства находятся без движения. Просто для того, чтобы в нужный момент быть использованными. Как говорят по этому поводу в России, лучше всего хранить деньги в банке, желательно в трехлитровой.

Несложно заметить, что деньги, как средство платежа и инвестиционное средство различаются с точки зрения участия в воспроизводственном процессе. А функция денег, как средства спекуляции или средства сбережения в случае, если активом выступают не производные финансовые инструменты, например, деривативы, а сами деньги, зависит от того, насколько стабильна их цена относительно других товаров. Если цена стабильна, то сами по себе деньги могут выступать только средством сбережения. А как спекулятивное средство – использоваться при приобретении различного рода финансовых инструментов, особенно производных. Если же цена денег динамична, как, например, в случае с Биткойном, то само по себе обладание активом делает Биткойн средством спекуляции.

Эффективность любой валюты помимо емкости рынка ее использования, доверия к ней и сил, ее поддерживающих, в решающей степени зависит от встроенных механизмов сбалансирования указанных функций. Именно механизм баланса, реализуемый через монетарную политику должен обеспечивать жизнеспособность и динамику экономики. Если механизм работает плохо, либо не работает вообще, то валюта будет слабой, а экономика неэффективной.

Если рассматривать с этих позиций систему Биткойн, то она не может быть признана сколько-нибудь эффективной. Если с 2010 по начало 2013 года из четырех функций реализовывались функция сбережения и функция платежного средства, преимущественно в сети Tor

для торговли криминальными товарами, то в 2013 году монопольное положение, по сути, заняла функция Биткойна как средства спекуляции. И лишь в 2014 году вместе с некоторым, по крайней мере, временным снижением волатильности Биткойн все шире используется как платежное средство.

Несоответствие Биткойна критериям эффективной валюты, отсутствие механизма структурного сбалансирования функций связано с принципиальной чертой Биткойна – отсутствием адаптивного (подстраивающегося под изменение ситуации) регулятора системы Биткойн. К чему ведет отсутствие подобного регулятора применительно к денежному обращению и экономической динамике убедительно показали на огромном массиве данных Дж. Купер в своей книге «Природа финансовых кризисов: Центральные банки, кредитные пузыри и заблуждения» и К. Рейнхарт, К. Рогофф в книге «На этот раз все будет иначе. Восемь столетий финансового безрассудства».

Нельзя не подчеркнуть, что переход от сберегательно-платежной к спекулятивной фазе системы Биткойн при полном игнорировании инвестиционной функции был не случаен и спрогнозирован. Произошел он в 2013 году, когда в мировой финансовой системе скопились огромные масштабы денежной ликвидности, ищущей спекулятивные активы. С другой стороны, была подготовлена разветвленная, рассчитанная на разные типы инвесторов и географически распределенная структура электронных бирж по торговле Биткойнами. И, наконец, была проведена мощнейшая медийная кампания во всех видах СМИ буквально на всех континентах.

Указанные обстоятельства позволяют с высокой степенью вероятности сделать вывод, что проект Биткойн – это не результат деятельности самоорганизующегося сообщества свободолюбивых либертианцев-гиков. Это серьезный, имеющий за плечами мощные ресурсы

всех видов проект, использующий «втемную» указанное сообщество как добровольную рабочую силу в соответствии с модным ныне принципом краудсорсинга, и одновременно как оперативное прикрытие реальных инициаторов и движущих сил проекта.

Возникает вопрос, является ли структурная, встроенная слабость Биткойна, как полноценной валюты, непреодолимой или нет. Расчеты показывают, что в рамках имеющегося математико-алгоритмического решения именно системы Биткойн отмеченный недостаток преодолеть невозможно. Однако он вполне преодолим, как мы обоснуем в последующих статьях цикла, в рамках виртуальной криптовалюты, построенной на несколько иной математико-алгоритмической базе. Данный вывод позволяет сделать предположение о том, что проект Биткойн – это крупномасштабный, что называется, «натурный» эксперимент по отработке эффективной криптовалюты. Эксперимент ставит перед собой сразу несколько целей. В их числе – зондирование мнений, а главное, действий различных политических сил, государственных регуляторов, инвесторов, программистского сообщества, общественного мнения на криптовалюту, имеющую внегосударственный характер.

Совершенно очевидно, что разработчики Биткойна были не только высококвалифицированными программистами и криптографами, но и отлично разбирались в тонкостях экономической теории и практики. Как мы уже отмечали, Сатоши Накамото в своей программной статье особый упор делал на минимизацию, вплоть до пренебрежимо малых величин, именно транзакционных издержек у всех участников сети Биткойн. Между тем, лауреат Нобелевской премии, основоположник неоинституциональной экономики, автор знаменитой теории фирмы и транзакционных издержек Рональд Коуз показал, что, в случае отсутствия или предельной минимизации транзакционных издержек, действия традиционных

социальных институтов становятся неважными. А они сами – ненужными.

В рамках неоинституциональной экономики социальные институты включают в себя как организованные – в виде государств, банков, фирм, учреждений и т.п., так и неформальные – в виде сложившихся норм, ценностей, стандартов сделок и т.п.

Фактически, вводя Биткойн как валюту и платежную систему без или со сверхминимальными транзакционными издержками, авторы проекта претендуют не на введение еще одной валюты, а на коренное изменение всей привычной системы политической и экономической жизни, базирующейся на сложившихся организованных институтах. Не больше, и не меньше.

Именно поэтому с первых шагов система Биткойн предполагала:

• отсутствие какого-либо единого эмиссионного центра в виде организованного института. Наряду с отсутствием эмиссионного центра отрицается и необходимость наличия какого-либо регулятора, который мог бы влиять на курс, контролировать эмиссию, блокировать счета и т.п.;

• система Биткойн при осуществлении платежей полностью независима от сложившегося финансового мира. Она не предполагает включения в себя каких-либо финансовых, банковских и инвестиционных институтов. Как исключение предусматривается лишь наличие точек соприкосновения системы Биткойн с системами обычных валют через биржевые площадки;

• система Биткойн игнорирует не только государства, но и любые надгосударственные организованные институты. Участниками системы Биткойн являются анонимные владельцы кошельков без государственной принадлежности и какой-либо иной идентификации. Строго говоря, необязательным является даже, чтобы владельцем электронного кошелька был человек. Принципиаль-

но возможны и уже реализованы торговые программы-роботы, которые сами добывают Биткойны, заводят электронные кошельки и расходуют средства, например, на спекуляции с Биткойнами по заранее написанной программе.

Понятно, что авторы столь амбициозной программы прекрасно отдавали себе отчет во внутренне обусловленных критических недостатках системы Биткойн, как полноценной валюты. Для того чтобы разгадать загадку, почему Биткойн запущена именно в таком виде и какие силы за ней стоят, необходимо тщательно изучить доступные фактические, а не спекулятивные или оценочные данные об истории и предыстории создания сети Биткойн и развертывания ее внешней инфраструктуры, вплоть до 2013 года.

### 5.4. Предыстория Биткойна

Не будет преувеличением сказать, что Биткойн, а точнее криптовалюты в целом начинают отсчет своей истории с 1975 года. В том году Фридрих Август фон Хайек, лауреат Нобелевской премии по экономике, кумир либертарианцев, столп австрийской экономической школы, неутомимый борец с государством и социализмом, один из основателей общества «Монт Пелерин», сыгравшего зловещую роль в истории новой России, опубликовал знаменитую книгу «Частные деньги».

Есть все основания полагать, что для создателей Биткойна это была настольная книга. В ней фон Хайек пишет: «Моя идейная основа проста... Валюту следует считать обычным коммерческим товаром и потому производить рыночным способом.

Мое предложение состояло в том, что правительство следует лишить монополии на эмиссию денег. Теперь у меня не осталось сомнений, что частные предприятия, если бы им не мешало правительство, давно предоставили бы обществу широкий выбор валют...

Расхожее представление, будто существует четкая разграничительная линия между деньгами и неденьгами – а закон обычно пытается провести такое разграничение – на самом деле неверно... Мы обнаруживаем здесь скорее некий континуум, в котором объекты с разной степенью ликвидности и с разной (колеблющейся независимо друг от друга) ценностью постепенно переходят друг в друга постольку, поскольку они функционируют как деньги. Обычное договорное право делает все необходимое безо всякого закона.

В отсутствии государственной валюты и центрального банка сложатся совершенно иные институты эмиссионных, инвестиционных и кредитных услуг».

Фактически в этих абзацах и шире, в тексте книги, расписана методология, подходы и принципы системы Биткойн, включая даже ограничение на рост денежной массы. Что же касается последствий введения «частных денег» для экономической и политической жизни, их институтов, включая государство, то это было четко прописано в работах «Природа фирмы» и «Проблема социальных издержек», опубликованных соответственно в 1937 и в 1960 годах будущим Нобелевским лауреатом Р. Коузом и в книге «Институты, институциональные изменения и функционирование экономики» еще одного Нобелевского лауреата Д. Норта.

К экономическим основам в 1996 году добавилась работа, где обосновывалась сама возможность существования электронной криптовалюты. Ее название «Как сделать монетный двор: криптография анонимной электронной валюты» (How to make a mint: the cryptographic of anonymous electronic cash). Отчет был подготовлен департаментом криптографии офиса исследований и технологий информационной безопасности Агентства национальной безопасности.

В работе широко используются термины «цифровые валюты», «электронные валюты», «криптовалюты»,

подробно разбираются методы обеспечения анонимности криптовалют. В качестве лучшего из таких методов предлагается метод асимметричного шифрования, который и используется в системе Биткойн. При этом надо отметить, что работа описывает традиционную архитектуру платежных систем, а не решение, использованное в системе Биткойн, где электронные деньги и платежные система как таковые представляют собой единое неразрывное целое. При традиционной архитектуре в платежной системе могут использоваться самые различные валюты, как электронные, так и обычные, типа доллара или рубля. В сети Биткойн платежная система может оперировать только Биткойнами или созданными на их основе клонами типа Лайнкоина и др.

Отчет дал несомненный импульс развитию криптовалют и показал наиболее эффективные решения в ряде областей, связанных с цифровыми деньгами. Однако он не может считаться, как полагают некоторые эксперты, описанием системы Биткойн.

Вслед за отчетом АНБ идеи криптовалюты «b-money» описал в 1998 году В. Дай (Wei Dai). Также свои предложения сделал Н. Сабо (Nick Szabo) под названием «Bitgold».

Еще до опубликования доклада АНБ доктор по информатике и менеджменту Калифорнийского университета Д. Чаум выдвинул идею использования интернета для организации платежной системы. Эта система получила название eCash. Система оперировала электронными деньгами eCash, фактически долларами, которые хранились в электронном кошельке, устанавливавшемся тогда вручную на компьютере. А все расчеты осуществлялись по интернету. Сама по себе система предусматривала анонимные цифровые денежные единицы. Но была централизованной, использовала обычные интернет-каналы и управлялась из единого центра. Оригинальная система не получила большого распространения. В ней

участвовало только около одной тысячи пользователей. После чего компания, эксплуатировавшая систему, обанкротилась. Однако позднее технология Д. Чаума была воспринята практически всеми традиционными платежными системами – от WebMoney до Яндекс.Деньги. Применительно к Биткойну Д. Чаум выступал предшественником, как первый человек, практически запустивший платежную систему в электронных сетях среди массовых пользователей. И, кроме того, предусмотрел возможность проведения анонимных платежей.

Далее наступил черед практики. Первая полноценная электронная валюта E-Gold была запущена в 1996 году. Некоторые называют ее первой мощной платежной системой. Но более правильно вести речь все же о платежной системе и электронной валюте в одном флаконе. Дело в том, что платежная система не оперировала привычными денежными единицами, типа доллара, фунта, йены. В качестве платежных единиц в ней использовались единицы, так называемое «электронное золото» или E-Gold, обеспеченные самыми настоящими драгоценными металлами, прежде всего, золотом, а также серебром, платиной и палладием. Например, золота хранилось 2,5 тонны. Качество драгоценных металлов и их сохранность заверяли ведущие мировые аудиторские компании, охрану хранилища несла одна из самых известных в мире специализированных фирм. Кроме того, в хранилище были установлены видеокамеры, которые вели трансляцию 24 часа в сутки. Соответственно, любой пользователь системы мог убедиться, что золото находится в сохранности и лежит в хранилище. В этом смысле E-Gold отличалась от ФРС США, которая вот уже длительное время не дает провести аудит своих золотых запасов.

Вступая в систему, каждый новый участник приобретал за традиционные деньги определенное количество платежных единиц, которым соответствовало опреде-

ленное количество золота и других драгоценных металлов. Т.е. «электронное золото» и все его транзакции имели стопроцентное золотое покрытие. Это, кстати, отличало E-Gold от любого банка с так называемым частичным резервированием.

Надо сказать, что система представляла собой в каком-то смысле анонимную электронную валюту. Для регистрации, открытия счета, внесения средств или получения денег не требовалось паспорта, водительского, либо какого-либо другого удостоверения личности. Не было также ограничений и на количество открываемых счетов. При этом на входе в систему, т.е. при осуществлении стартового платежа и, при желании, на выходе из системы при осуществлении расчетов, использовались обычные денежные единицы, в основном доллары. Все же расчеты внутри системы велись в E-Gold.

Систему «электронного золота» создали два человека, весьма далекие от интернета и программирования. Один из них, Д. Джексон, был весьма успешным врачом-онкологом. Он служил в армии США, занимался закрытыми темами, связанными с радиационной онкологией. После этого открыл частную клинику, в которой лечились многие представители американского истеблишмента. Его коллега по бизнесу Б. Дауни был успешным адвокатом, автором известных юридических трудов. И более того, работал в святая святых американской юстиции – Верховном суде США.

На своем пике число открытых аккаунтов системы достигло 5 миллионов, а сумма транзакций за год составила около 2 млрд. долларов. И здесь на компанию обрушились обвинения. E-Gold вменялось в вину, что она способствует противозаконной деятельности по созданию финансовых пирамид, отмывает деньги наркопреступников, порнографии, потворствует педофилам и т.п. Делалось все это на основе положения Патриотического Акта. Самое забавное в этой истории то, что в 2002 году

военно-морская разведка США рассекретила свой проект – сеть Tor, и сделала программное обеспечение проекта свободным софтом. Тут же в сеть Tor, как говорится, толпой кинулись наркоторговцы, педофилы, торговцы оружием, киберпреступники всех мастей и подобная публика.

Еще более парадоксален финал истории E-Gold. Летом 2008 года, т.е. накануне того, как мифический Сатоши Накамото опубликовал свой файл о Биткойне, Дуглас Джексон, его брат Рейд и Барри Дауни, наконец, согласились признать свою вину и пойти на судебный процесс. По американским меркам процесс состоялся практически немедленно, в конце 2008 года. По итогам процесса всем троим обвиняемым дали по три года условно с отбыванием полугода под домашним арестом, не покидая территорию дальше 10 км от дома. Дугласа Джексона приговорили к штрафу в 200 долларов (это не опечатка). А его брата и Барри Дауни обязали внести несколько больше – 2500 долларов с каждого. Всех приговорили к 300 часам общественных работ по своему выбору. Компанию обязали продать драгметаллы и вернуть средства владельцам счетов. Правда, на счет раскрытия анонимности счетов ничего в решении суда не было. В завершение компания Gold and Silver reserve, которая собственно и занималась системой E-Gold, закрыта не была. Ей было рекомендовано в тот момент, когда она решит возобновить работу, получить необходимые лицензии и провести процедуры регистрации новых счетов в соответствии с законодательством. Недавно Дуглас Джексон заявил, что в планах у него – возобновить работу компании. Тем более что ни одного иска от клиентов в адрес компании за прошедшие годы подано не было.

В завершение саги о E-Gold хотелось бы обратить внимание на одно любопытное обстоятельство. Американское судопроизводство имеет привычку хранить буквально все материалы судебных процессов в интер-

нете, где они доступны для любого желающего. Из материалов дела против «электронного золота» выясняется пикантная подробность. В ходе переписки владельцев компании с правоохранительными органами, Джексон и Дауни на любые вопросы недоуменно отвечали, цитируем дословно: «E-Gold работает легально и не потворствует лицам, пытающимся использовать его для преступной деятельности. E-Gold имеет долгую историю сотрудничества с правоохранительными органами в США, как на территории страны, так и во всем мире, включая предоставление данных и помощь в осуществлении расследований. Наши сотрудники участвовали в сотнях расследований и операций, проводимых FBA, FTC, IRS, SEC, DIA и других». С ФБР, налоговиками, специалистами по финансовым расследованиям и профессионалам из комиссии по ценным бумагам – все понятно. А DIA – это военная разведка США. Интересно, в каких расследованиях с ними участвовало «электронное золото»?

Биткойн, как известно, это платежная система практически с нулевыми затратами на транзакции, ориентированная на интернет-экономику. В этом смысле она стала следующим шагом в развитии подхода, реализованного знаменитой PayPal. Не зря в декабре 2013 года генеральный директор PayPal публично выразил поддержку Биткойну и сообщил, что сам инвестирует в этот актив.

PayPal создавалась как система с минимальной стоимостью транзакций, ориентированная на интернет-экономику. Поэтому история PayPal и ее действующие лица вписываются в сагу о Биткойне.

Как известно, PayPal была основана в 1998 году Питером Тилем и киевским программистом Максимом Левчиным, или по-американски Максом Левчиным. Их компания называлась Confinity. Компания занималась разработкой независимой денежной платежной системы, способной ослабить государственный контроль за

денежными потоками, которой они дали название PayPal («приятель, помогающий расплатиться»). Это было неслучайно, поскольку М. Левчин был программистом, а Питер Тиль философом и юристом, выпускником Стэндфордского университета и редактором либертарианской газеты «Стэндфордское обозрение». Но чего не было у компании, так это серьезных по меркам стартапа денег и финансистов. Все это привел с собой ныне знаменитый в Америке инвестор Э. Маск, сейчас – член знаменитой «Мафии PayPal», хозяин Tesla Motors и многих других компаний. После слияния компания стала называться PayPal.

Дальше между соучредителями развернулась настоящая война, которая описана в знаменитом бестселлере Эрика М. Джексона «The PayPal Wars: Battles with eBay, the Media, the Mafia, and the Rest of Planet Earth». Война шла, прежде всего, за руководство компанией. В итоге военных действий за явным преимуществом победил П. Тиль и его либертианская группа, которые возглавили компанию. В 2002 году компания была продана eBay за 1,5 млрд. долларов. При этом следует иметь в виду, что eBay развивала собственную платежную систему, но в итоге отказалась от нее и приобрела PayPal.

Все действующие лица этой истории особо не спорили с книгой Э. Джексона, более того, дали благожелательные отзывы и, несмотря на прошедшую войну, до сих пор сохраняют тесные деловые отношения, образуя «Мафию PayPal».

Из книги становится понятным, что собственно решения, на которых построена PayPal, были известны еще до М. Левчина и Тиля и использовались несколькими другими стартапами. В случае PayPal решение было упаковано в первоклассную программу, в чем и состоит главная заслуга Макса Левчина. Элон Маск дал деньги, опыт и финансовую команду. Возникает вопрос, а в чем же ключевая роль Питера Тиля? Как ни странно, прямо

в книге об этом не пишется, но зато там приведены конкретные факты.

Буквально в течение года с небольшим Питеру Тилю удалось волшебным образом договориться с десятками стран мира, которые разрешили платежной системе действовать на своих территориях. Затем он был столь же убедителен в переговорах с главным владельцем eBay Пьером Омидьяром. Т.е., как говорят в России, Питер Тиль – это, прежде всего гениальный решальщик. Это, кстати, неудивительно. Многое становится понятным, если внимательно прочитать его слова относительно целей PayPal: «Необходимость PayPal огромна. Каждый человек в мире нуждается в деньгах... В XXI веке людям нужны деньги, которые более удобны и безопасны, к которым можно получить доступ с любого места с помощью КПК или подключения к Интернету... Большинство обычных людей никогда не имеют возможности открыть офшорный счет или получить в свои руки больше, чем несколько счетов стабильной валюты, такой как доллар США. В конечном счете, PayPal сможет это изменить... Для коррумпированных правительств станет почти невозможным украсть состояние своих граждан через старые методы, потому что если они попытаются это сделать, люди перейдут на доллары, фунты или йены, по сути, выбрасывая бесполезную местную валюту и заменяя её на что-то более безопасное.» Кстати, основную часть полученных в результате продажи PayPal денег Питер Тиль инвестировал в самую известную ныне шпионскую программу Palantir. Также он был первым крупным инвестором Facebook.

Буквально несколько слов о покупателе PayPal – eBay. Как сообщил осенью этого года высокопоставленный немецкий чиновник Питер Шаар, eBay, хотя и не засветилась в списках Э. Сноудена, активно передавала данные о покупателях Агентству национальной безопасности. Что же до основателя eBay Пьера Омидьяра, то

как сообщил осенью 2013 года интернет-ресурс Pando, кстати, финансируемый Питером Тилем, в ноябре Питер Гринвальд и Лаура Пойтрас передали все имеющиеся у них материалы Эдварда Сноудена за 250 млн. долларов некоей некоммерческой организации, которую они основали с Пьером Омидьяром.

Есть основания полагать, что создатели Биткойна внимательно проанализировали и опыт QQ Coin (QQC). В 2002 г. крупнейший государственный китайский интернет-провайдер выпустил свою виртуальную валюту QQC. QQC представлял собой виртуальную валюту в самом житейском смысле этого слова. Это были условные денежные единицы, за которые можно было покупать различного рода игровые предметы, одежду героям игр, игровое оружие для китайских онлайн-игр – клонов известных игр, таких как «Виртуальная жизнь», «Ферма» и т.п. QQC продавались за юани, и имелось в виду, что они будут иметь хождение только в рамках онлайн-игр. При этом QQC не имели собственной платежной системы, а операции с их приобретением осуществлялись либо через обычные банковские переводы, либо при помощи китайского клона PayPal.

Действительность превзошла все ожидания. Прежде всего, провайдера поразило число людей, приобретавших QQC. Из 200 млн. клиентов 20–30% в первый же год купило QQC. Далее ежегодно число людей, приобретавших виртуальную валюту, росло в среднем на 15% в год, вплоть до конца 2008 года, когда китайское правительство приняло жесткие меры по нецелевому использованию QQC. Исходно QQC, если можно так сказать, эмитировал интернет-провайдер и он же исключительно продавал их по цене чуть менее одного юаня за монету. При этом обратно QQC интернет-провайдер не выкупал.

К 2005 году сформировался вторичный рынок QQC. Они стали покупаться/продаваться на китайском аналоге eBay – Taobao, который также контролировался госу-

дарством. К концу 2008 года вторичный оборот по разным оценкам составлял от 600 до 900 млн. долларов в год. При этом, начиная с 2006 года, курс QQC рос на 40-70% в течение года. Формирование вторичного рынка, где можно было купить/продать QQC, и рост их курсовой стоимости был связан с тремя обстоятельствами.

Во-первых, интернет-магазины китайской диаспоры в Сингапуре, Гонконге, других странах Южной Азии стали принимать QQC наравне с обычными деньгами. Соответственно в условиях неконвертируемости юаня для китайцев это стало легальным путем приобретения за рубежом товаров, которые в самом Китае стоили намного дороже.

Во-вторых, внутри Китая QQC стали использоваться как средство оплаты подпольных казино, в системе оказания сексуальных услуг и т.п., т.е. в сфере нелегального бизнеса. Поэтому в гонконгской прессе они получили название «международная валюта триад». Поскольку все серьезные материалы по QQC имеются только в частично закрытых китайских источниках, то иностранным исследователям до сих пор не удалось выяснить, каким же образом в системе полного контроля над интернетом, происходила анонимизация QQC. В этой связи подавляющая часть экспертов высказывает мысль о том, что никакой анонимизации не было, а расплату QQC брали те ресурсы, которые имели то или иное административное коррупционное прикрытие.

Наконец, в-третьих, в условиях неконвертируемости юаня, QQC активно покупали иностранцы для того, чтобы в Китае приобрести на них различного рода предметы старины, имеющие художественную и историческую ценность, и иные изделия, которые запрещено было приобретать иностранцам и вывозить из страны. При этом вопрос вывоза иностранцы решали, а вот обойти государственную банковскую систему для них было более трудным делом. Так или иначе, к концу 2008 года мас-

штабы и динамика курса QQC и его привлекательность для различных групп пользователей оказались таковы, что Народный банк Китая и правоохранительные органы страны приняли строгие меры, закрыв все вторичные рынки QQC, и, прежде всего, возможность торговать ими на Taobao. При этом сами QQC не были запрещены, но впредь было разрешено использовать их только по прямому первоначальному назначению.

После закрытия E-Gold, ограничения оборота QQC и победного шествия по планете экономичного, технологичного и лояльного к властям США PayPal, грянул экономический кризис. В первый момент большинство обычных людей и так называемые эксперты решили, что впереди, буквально в ближайшие месяцы грянет экономический апокалипсис. В эти грозные месяцы всеобщей растерянности и неопределенности на арену выходит Сатоши Накамото с системой Биткойн.

За последние годы одна из любимых тем средств массовой информации это выяснение, кто такой Сатоши Накамото. В фаворитах пять человек: профессор Вашингтонского университета Ник Сабо, глава фонда Биткойн Гэвин Андерсен, Ужасный пират Рождерс, владелец SilkRoad, ныне сиделец ФБР, британский программист Майкл Клир и основатель первой крупной биржи Биткойнов, а ныне создатель собственной платежной системы Джед Маккалеб. Людей так достали в прямом и переносном смысле представители СМИ, что Сабо, Клир и Маккалеб письменно, кто под присягой, а кто у нотариуса сообщили, что они не имеют никакого отношения к Накамото. Гэвин Андерсен сказал, что просто смешно становиться главой фонда самого себя и, кроме того, он не обладает такими глубокими знаниями в ряде областей, которые требовались для создания Биткойна.

Между тем, для тех, кто знает японский в целом все ясно и понятно. Сатоши по-японски имеет вполне конкретное значение – «мудрость», а Накамото озна-

чает «находящийся внутри закрытой (сложной, могущественной) общности (целостности)». Англоязычные эксперты тут же перевели чисто по-западному – «человек мыслящий внутри сложной системы». Хотя понятно, что исходя из духа японского языка, имеется в виду именно мудрость, находящаяся внутри закрытой общности. Термин «система» – это западный термин. О единственном роде (человеке) тоже речи нигде не идет. Т.е. авторы псевдонима достаточно ясно сказали, что Биткойн – это творение некоей группы, находящейся в закрытой, или могущественной общности.

Каждый сам волен искать такие группы и общности. Далее мы выскажем некоторые собственные предположения на этот счет. А пока еще несколько слов о Накамото. Согласно проведенным независимыми экспертами расчетам, до сих пор в кошельке Накамото, который известен, находится примерно миллион Биткойнов из общего числа 11 миллионов. Кроме того, по мнению ряда специалистов, крупнейшая сделка с Биткойнами, проведенная с кошельков, заведенных до февраля 2010 года, в ходе которой неизвестному инвестору незадолго до обвала курса были проданы Биткойны на 147 млн. долларов, также с высокой степенью вероятности связана с Сатоши Накамото.

Теперь коротко о семействе Биткойна. Следуя логике фон Хайека, вслед за созданием Биткойна появилось достаточно большое число криптовалют. По некоторым данным живых и уже почивших в бозе систем к настоящему времени насчитывается более 50. Наиболее активно развиваются шесть.

Устойчивое второе место после Биткойна занимает Litecoin. Объем ее рынка примерно в 20 раз меньше. Litecoin имеет два больших преимущества. Если для майнинга Биткойнов необходимы целые компьютерные фабрики, то транзакции Litecoin, а соответственно и их добычу можно осуществлять с использованием мощных

видеокарт. Т.е. так, как дело обстояло с Биткойнами в самом начале их истории. Кроме того, переводы денег в Litecoin осуществляются в несколько раз быстрее, чем в системе Биткойн.

Третье и четвертое места делят между собой новые криптовалюты, которые примерно равны и периодически они меняются местами по объему рынка. Это NameCoin и PPCoin. Обе они имеют существенные новшества по сравнению с Биткойном.

NameCoin, добывается совместно с Биткойном, как своего рода побочный продукт. Это значит, что при майнинге NameCoin на выходе получается еще и Биткойн. Правда, если NameCoin добывается пока много и регулярно, то Биткойн – чрезвычайно редко, если сильно повезет. Кроме того, сеть NameCoin сконструирована так, что NameCoin практически нельзя отнять.

PPCoin, в свою очередь, отличается так называемой добавленной технологией генерации монет. Если «обычные» криптовалюты работают по принципу «Proof-of-Work» («Докажи стоимость работой, своей мощностью»), т.е. вероятность обработки транзакций и добычи Биткойна зависит от доли ресурса в суммарной мощности сети, то у этой криптовалюты все по-другому. Новые монеты появляются в кошельке не только благодаря майнингу, но и оттого, что их у обладателя кошелька относительно много. В Евангелии от Матфея этот принцип описывается следующим образом: «Кто имеет, тому дано будет еще и приумножится, а кто не имеет, у того отнимется и то, что имеет». Преимущества здесь не очень большие и введены они для того, чтобы максимально стимулировать активность и кооперацию участников сети, заставляя вычислительные мощности работать без простоев.

Кроме того, недавно появилась криптовалюта PrimeCoin. Это первая полноценная криптовалюта, работающая по принципу Биткойна, но вычисляющая не простые числа, а определенные последовательности, кото-

рые нужны для научных исследований. Тем самым, когда майнятся PrimeCoin, происходит не просто совершенно бессмысленный процесс, сжигающий электричество, а обработка массивов числовой научной информации, поступающая в сеть с серверов американских университетов.

С каждым месяцем число валют множится. Более того, заявлено, что в начале следующего года появится новое, второе поколение криптоденег Nxt. Но следующее поколение криптоденег мы рассмотрим после того, как вплотную исследуем тему столкновения элитных групп на поле криптовалют. Об этом следующая статья.

### 5.5. Конспирология Биткойна

В качестве введения в тему как нельзя лучше подходит цитата из книги Джулиана Ассанжа «Шифропанки: свобода и будущее интернета»: «Финансовые вопросы – самые опасные... Распределённая валютная система, не требующая центрального сервера, который был бы привлекательной целью для принудительного контроля – это то, что действительно ново в Биткойне. В системе действуют алгоритмы, обеспечивающие распределенное доверие. В сети Биткойн принуждение к отказу от мошенничества достигается не с помощью закона, регулирования или аудита, а за счёт вычислительной сложности, которую каждая часть сети должна преодолеть, чтобы доказать, что делает именно то, о чём заявляет. Таким образом, принуждение к честному биткойновому «банкирству» встроено в архитектуру системы... Думаю, что игра, которую нужно провести с Биткойном, состоит в том, чтобы добиться его принятия интернет-провайдерами и крупнейшими интернет-сервисами, интернет-магазинами и т.п. А когда система криптовалюты будет хорошо принята основными игроками интернет-индустрии, они сами наймут лобби, или другими способами решат необходимые вопросы с государством и международными регуляторами».

Некоторые горячие головы спешат видеть в Биткойне угрозу доллару. На уровне идеи это предмет для обсуждения, но банкиры – люди прагматичные. Они исходят из цифр, а не эфемерных идей. С этой позиции цифровые валюты, по крайней мере, в близком будущем, вряд ли станут конкурентом доллара, либо любой другой валюты мощного государства.

Однако наличие цифрой валюты важно для соотношения сил внутри мировой финансовой элиты. За последние 15-20 лет там сформировалась мощная группа, которую писатели и журналисты назвали «Квантами». Это инвестиционные и хедж-фонды в основном США, Великобритании, Германии и Сингапура, возглавляемые математиками и программистами, которые делают деньги не на эмиссии, не на кредитовании, а на финансовых спекуляциях и биржевой игре на высоковолатильных и других финансовых рынках. Их успех в решающей степени зависит от вычислительных мощностей и качества математических алгоритмов. Этой мощной группе посвящены книги С. Паттерсона «Кванты. Как волшебники от математики заработали миллиарды и чуть не обрушили фондовый рынок» и Д. Уэзеролла «Физика фондового рынка. Краткая история предсказаний непредсказуемого». Некоторые из таких структур рождением обязаны людям из власти, а также из военно-разведывательного сообщества. Ярким примером такого рода структур является знаменитый Blackstone, о котором книга Д. Морриса, Д. Кэри «Король капитала. История невероятного взлета, падения и возрождения Стива Шварцмана и Blackstone». «Кванты», которые заинтересованы в появлении все новых классов финансовых активов, являются тактическими союзниками тех, кто старается дать жизнь различного рода криптовалютам. Цифровые валюты дают им как новый инструмент для спекуляций, так и позволяют усилить их позиции в отношении традиционных банкиров, которые не понимают и не знают специфики

высоких информационных технологий и сложных систем криптографии.

Однозначно против новых цифровых валют настроены корпоратократы. В этой группе наднациональной элиты взаимодействуют и борются между собой транснациональные производственные и торговые компании, принадлежащие традиционной экономике, сложившиеся в рамках второй производственной революции. Такая позиция связана не с какими-либо идеологическими предубеждениями, а с чисто прагматическим подходом, что называется «это просто бизнес, ничего личного».

Транснациональные корпорации в конечном счете реализуют эффект масштаба, который позволяет достигать тотального превосходства над остальными компаниями за счет низких издержек, сложной логистики и возможности диверсифицировать риски за счет множества производимых и торгуемых товаров и услуг. В своей совокупности это, грубо говоря, компании конвейера и сетевых торговых центров. Их благоденствие в условиях низких темпов экономического роста, свойственных уже долгие годы мировой экономике, возможно только при тотальном и все увеличивающемся подавлении среднего и малого бизнеса. Для них, чем выше уровень централизации, тем лучше.

Строго говоря, им крайне невыгодно любое снижение издержек, связанных с производством и обращением, которое доступно не только для уже существующих гигантских корпораций. Один раз эти компании уже обожглись, проспав интернет-революцию и допустив появления новых торговых гигантов типа Amazone, eBay и т.п. Теперь они ни в коем случае не хотят допустить даже намека на создание платежных систем с нулевыми, либо близкими к нулевым платежными издержками. В этом смысле главными лоббистами мер на правительственном уровне против цифровых валют выступают даже не столько центральные банки, которые пока угрозы в этих

валютах не видят, сколько корпоратократы, особенно из транснациональных торговых сетей.

Правда имеется возможность одного достаточно любопытного исключения из описанного выше правила. Речь идет о государственных компаниях традиционного сектора. В строгом смысле этого слова, государственная компания в своей деятельности может не руководствоваться критерием максимизации своей собственной прибыли, а решать иные необходимые политическому руководству задачи. Поэтому в чисто гипотетическом плане можно представить себе ситуацию, когда в силу тех или иных причин торговые или производственные государственные компании могут поддерживать те или иные цифровые валюты.

У этой же возможности есть и оборотная сторона. Цифровые валюты тесно связаны с информационными технологиями и в целом с технологическим пакетом третьей производственной революции. Этот пакет базируется на мини-предприятиях, способных удовлетворить персонифицированный, а не массовый спрос. Весьма вероятно, что в недалеком будущем менеджмент государственных компаний в различных странах мира может постараться использовать ресурсы своих компаний для вложений в такого рода предприятия, принадлежащие уже не государству, а им самим. Кстати, в Китае, согласно ряду появившихся в последнее время публикаций, такую возможность рассматривают как весьма вероятную. Более того, есть все основания полагать, что решение Народного банка Китая по отношению к Биткойну связано не столько с надуманной угрозой Биткойна могучему юаню, сколько с реальностью использования системы Биткойн для массированного вывода средств из государственного сектора китайской экономики, а также отмывания коррупционных и других нажитых преступным путем денег.

Очевидные сторонники системы цифровых валют это – часть мировой элиты, связанная с высокими тех-

нологиями. Хотя гиганты информационных технологий, которые являются сегодня несущей конструкцией новой производственной экономики, стараются пока не высказываться на тему цифровых валют, некоторые выводы сделать, тем не менее, можно. Прежде всего, бросается в глаза количество бывших топ-менеджеров, разработчиков, ключевых программистов из интернет-гигантов, включая Google, Facebook, Amazon и т.п., которые либо вкладывают собственные средства, либо непосредственно участвуют в компаниях, связанных с цифровыми валютами вообще и с системой Биткойн в частности. Ряд компаний, например, PayPal, которые казалось бы, должны выступать конкурентами цифровых валют, в лице своего генерального директора Д. Маркуса, приветствуют их появление. Крупнейшая мировая торговая площадка eBay сообщила, что по мере того, как Биткойн утратит сверхвысокую волатильность, в компании готовы рассмотреть возможность использовать ее в качестве платежного средства.

Когда мы говорим о бывших работниках Google, Facebook и т.п., то здесь, как в известной шутке о спецслужбах, можно сказать, что «бывших работников не бывает». В мире информационных технологий, особенно в Соединенных Штатах, разработчики, ключевые программисты, инвесторы связаны теснейшими личными отношениями, и стараются на протяжении карьеры наращивать свой социальный капитал или систему связей и доверительных отношений между собой. Поэтому, прежде чем участвовать в каком-либо деле, сколько-нибудь известные люди из мира информационных технологий, как правило, обсуждают эти вопросы с коллегами, друзьями, советуются с людьми, с которыми поддерживают доверительные деловые отношения.

Что же выигрывает высокотехнологичная элита от массового использования цифровых валют:

• во-первых, они получают собственную, понятную и адекватную для себя систему платежей, валютных

единиц и способов их обработки. Надо понимать, что современные информационные технологии базируются, прежде всего, на Больших Данных и когнитивных вычислениях. Системы типа Биткойн с их свойством хранить все произведенные транзакции, позволяют в режиме реального времени работать с Большими Данными, осуществлять когнитивные вычисления и на этой основе реализовывать более гибкие, а потому эффективные, алгоритмы эмиссии и регулирования, чем в нынешней системе Биткойн. Вычислительный способ регулирования эмиссии отсекает от нее финансистов и корпоратократов, и позволяет использовать криптовалюты в качестве собственной внутренней платежной системы новой экономики. Кроме того, алгоритмический характер эмиссии устраняет потенциальные конфликты внутри высокотехнологичной элиты относительно доступа к печатному станку;

• во-вторых, наличие мощных и развитых систем цифровых валют различных типов дает в руки силовиков действенный инструмент для переговоров с другими элитными группами и правительствами, а также надгосударственными структурами. Предметом переговоров в этом случае будет являться режим сосуществования электронных валют с действующими, традиционными денежными системами, а также законодательные нормы регулирования цифровых валют и платежных систем и способы их налогообложения. Само по себе наличие такого инструмента является несомненным ресурсом в межэлитной борьбе;

• в-третьих, хотя сами по себе цифровые валюты, как правило, связываются с либертарианским движением, на практике они позволяют осуществлять гораздо более жесткий контроль за денежными потоками, а главное их использованием, чем нынешняя денежная система. Для того чтобы такой контроль стал реальностью необходимо отказаться в цифровых деньгах от анонимности

электронного кошелька. Судя по тому, что представители фонда Биткойн постоянно контактируют с государственными органами различных стран по этому поводу, а один из ведущих разработчиков платформы Биткойн – Д. Гарзик прямо сообщил, что поддерживает отношения с государственными структурами США, можно предположить, что ради легитимизации и широкого распространения цифровой валюты, ее инициаторы могут пойти на отказ от анонимности платежного кошелька.

Таким образом, система Биткойн, другие цифровые валюты, а также последующее поколение цифровых платежных систем и виртуальных валют обостряют противоречия между различными группами наднациональной мировой элиты. Исход этой борьбы в значительной степени зависит от общей ситуации в мировой экономике и финансах, а также темпов разворачивания третьей производственной революции. Соответственно в краткосрочном плане возможны любые повороты ситуации с системой Биткойн. Однако в долгосрочной перспективе цифровые криптовалюты с высокой степенью вероятности постепенно будут занимать все более заметное положение в мировой финансовой системе.

Часто конспирологию связывают с параноидальными фантазиями, изложенными в форме псевдоисторических сочинений, или с порождением поверхностного тенденциозного знания, рассчитанного на невежественных потребителей. Между тем, интеллектуальная конспирология – это тщательное исследование скрытой или скрываемой подлинной канвы событий на основе опирающихся на перекрестно подтвержденные источники фактов. Вот интеллектуальной конспирологией сети Биткойн мы и займемся. Изучив фактографию и хронологию сети Биткойн, и исходя из понимания гетерархии элит, можно выдвинуть гипотезу относительно инициаторов инновации «сети Биткойн» и системы криптовалют в целом.

Ключевым для конспирологического понимания динамики криптовалют является термин «инновация». Он противоположен используемому в нашем Отечестве к месту и не к месту термину «проект». Проект во всех случаях предполагает ясно очерченную цель, заранее установленный путь ее достижения, четко прописанные сроки, наличие плана, увязанного по ресурсам, исполнителям, времени и т.п. Между тем, инновация представляет собой совершенно иной вид предпринимательской деятельности. Процитируем профессора из Йеля Д. Старка. «По-настоящему фундаментальные предпринимательские решения, или инновации рождаются таким типом поиска, в процессе которого мы даже не знаем, что конкретно ищем. Однако сразу распознаем искомое, как только его обнаружим... Мы чувствуем, что существует принципиальное различие между теми случаями, когда мы ищем решение в рамках установленного набора параметров, т.е. реализуем проекты и другими случаями, полными неопределенности и одновременно, благодаря этой неопределенности, полными новых возможностей, к которым относятся инновации». Создание системы криптовалют это – несомненно, инновация.

Чтобы реализовать крупномасштабные инновации, а главное, иметь способность долгое время управлять этим процессом, нужно совершенно уникальное сочетание качеств команды, разрабатывавшей тот или иной продукт. В нашем случае – системы Биткойн. Есть основания полагать, что систему Биткойн исходно создала сплоченная группа, обладающая зашкаливающим уровнем предпринимательской наглости, здоровым деловым цинизмом, богатым инвестиционным опытом, большими деньгами, широкими связями в самых различных кругах и, наконец, мощной силовой поддержкой. Кроме того, группа должна являть пример внутренней сплоченности, самодисциплины, умения быстро и успешно переходить от одной деловой роли к другой. Вполне возможно, что,

по крайней мере, некоторые из членов инициативной группы хорошо известны СМИ и общественности в других своих публичных ипостасях.

По своей ментальности, типу организационного взаимодействия, характеру связей и т.п. такая группа достаточно близка к знаковой для Америки «Мафии PayPal», в которую входят основатели таких знаменитых компаний, как PayPal, Facebook, LinkedIn, знаменитого шпионского Palantir и т.п. Очевидно, что в состав группы в личном качестве, скорее всего, входят и сотрудники разведывательных структур, связанные с криптографией и программированием (не будем показывать на них пальцем).

Кстати, один из самых ярких членов «Мафии PayPal», П. Тиль, мультимиллиардер и знаменитый инвестор Силиконовой Долины, хозяин любимой программы АНБ Palantir заявил, что он верит «в потенциал Биткойна вывести из равновесия и навсегда изменить мир финансов». Выступая на саммите Thiel Foundation для молодых предпринимателей, Тиль сказал: «Еще в 1999 году я предсказал конец госмонополии на деньги и появление криптовалюты, которая «изменит мир». По его мнению, «Биткойн является первой, но не последней цифровой валютой, которая имеет такой потенциал».

Инициативная группа, типологически похожая на «Мафию PayPal», вероятно взяла на себя разработку отправной идеи, составление технического задания, написание базовых алгоритмов и подбор первой команды программистов, члены которой в настоящее время составляют в значительной мере Bitcoin Foundation. Затем инновация была пущена в свободное плавание, используя лавинный принцип Linux или Open source. При этом за собой инициативная группа оставила корректирующее или импульсное управление динамикой инновации, предусматривающее целенаправленное воздействие на переход системы Биткойн из одной в другую стадию своего развития.

Практический запуск сети Биткойн был точно приурочен к той фазе всемирного финансово-экономического кризиса, когда в мире господствовали апокалиптические настроения относительно будущего доллара и других резервных валют. Первыми адептами и одновременно пропагандистами Биткойна выступили шифропанки и хакеры, сторонники нового криптомира от Джулиана Ассанжа. Именно они составили ядро первых пользователей системы и соответственно майнеров.

Когда система Биткойн пустила прочные корни в подполье кибермира, настал этап вывода ее в более широкие массы. Произошло это в 2011 году, когда на волне Арабской весны средства массовой информации во всем мире устроили бесплатную, беспрецедентную PR-кампанию сети Tor, созданной в свое время военно-морской разведкой США. Побочным результатом этой кампании стал расцвет незаконного бизнеса в сети Tor и прежде всего знаменитого SilkRoad, который осаждали гики, либертарианцы-программисты и другие любители чего-нибудь покурить. Инициативная группа со свойственным ей деловым цинизмом исходно сознательно проектировала систему Биткойн, как анонимную систему. Дело в том, что только такой подход мог на первом этапе создать необходимую критическую массу пользователей и соответственно устойчивый прирост денежного оборота.

К 2013 году было завершено создание, в том числе, с привлечением средств крупных инвесторов и опосредованно интернет-гигантов, полноценной инфраструктуры сети Биткойн, облегчающей доступ к ней неискушенных в компьютерных премудростях рядовых пользователей и инвесторов. Наступила пора нового этапа развития системы. Переходу на этот этап способствовали несколько на первый взгляд независимых друг от друга обстоятельств. Во-первых, в результате массированной эмиссии традиционных денег на счетах не только крупных, но и мелких

инвесторов оказались значительные суммы свободных средств. А когда средств много, то возрастает склонность к рисковым вложениям в высоковолатильные активы. Во-вторых, был нанесен мощный удар по нелегальной платежной системе Биткойн в сети Tor. ФБР арестовало Ужасного пирата Рождерса, владельца SilkRoad, и в результате стало обладателем второго по величине кошелька Биткойн. Удар был нанесен удивительно своевременно, поскольку в глазах инвесторов достаточно четко дистанцировал систему Биткойн от ее применения в сети Tor для нелегальной и противозаконной торговли. Наряду с прочими эффектами, акция ФБР может рассматриваться как классическая операция по ребрендингу Биткойна и отбеливанию его репутации. В-третьих, сразу же после падения курса Биткойна весной этого года начал свою причудливую миссию Э. Сноуден. Помимо прочего, разоблачения Э. Сноудена привели к скачкообразному и распространяющемуся подобно эпидемии спросу на средства борьбы с Большим Братом, и обеспечению минимальной приватности денежных переводов, которые также контролировало АНБ. Данное обстоятельство стало просто подарком для системы Биткойн, поскольку обеспечило ей невиданную PR- и GR-кампанию. На волне этой кампании курс Биткойна стремительно пошел вверх. В сеть Биткойн устремились свободные, ликвидные средства из Китая, США и в меньшей степени Европы. Свою лепту внесло и знаменитое заседание Комитета по безопасности Сената США, на которому присутствовал только один сенатор – глава Комитате, но зато благожелательно высказались все основные правоохранительные агентства США, а Б. Бернанке даже написал сочувственное письмо от имени ФРС. Сам по себе экспоненциальный рост курса превращался в новость номер один для всех финансовых порталов мира. Они 24 часа в сутки сообщали об этом и привлекали все новых спеку-

лятивных инвесторов. Формировался типичный пузырь, который мог неконтролируемо лопнуть.

В этих условиях главной задачей для инициативной группы Биткойн стало обеспечение контролируемого сдувания пузыря и переход в несколько менее волатильный и предсказуемый режим динамики системы Биткойн. Возникла задача, как решить эту проблему. Выскажем гипотезу, что путь ее решения был найден чисто вычислительным путем.

С учетом распределения средств, вложенных в Биткойны в региональном разрезе, стало понятным, что необходимо каким-либо образом воздействовать на Национальный банк Китая с тем, чтобы обеспечить отток китайских вкладчиков из системы Биткойн, как максимум, и/или не допустить притока новых, как минимум. Т.е. по сути, встала задача осуществить рефлексивное управление, спровоцировав китайцев на принятие репрессивных мер в отношении Биткойна. В начале декабря 2013 года такие меры действительно были объявлены. Курс Биткойна рухнул практически в два раза. А затем приобрел гораздо более сглаженную и менее волатильную чем раньше динамику курса, что и требовалось гипотетической инициативной группе.

Может возникнуть вопрос, а есть ли хоть одно доказательство, что решение Народного банка Китая не было обусловлено чисто внутренними обстоятельствами и не являлось заранее предусмотренным плановым мероприятием. Такие доказательства есть. Любой квалифицированный китаист отметит, что в Китае в отличие от многих других стран, правая рука в системе управления всегда знает, что делает левая. А решения на самых различных уровнях принимаются согласованно в рамках единой политики. Между тем, в конце лета крупнейший поисковик Китая Baidu разрешил платежи за свои сервисы в Биткойнах. Более того, буквально за несколько дней до решения Народного банка Китая крупнейший госу-

дарственный интернет-провайдер China Telecom объявил о том, что начинает принимать платежи в Биткойнах и работать с ними. В Китае такого просто не бывает, за исключением случаев, когда в дело вмешиваются чрезвычайные обстоятельства.

Можно высказать версию, что китайцы смогли (им сильно помогли) получить информацию, что через систему Биткойн отмываются деньги людей из центральной, либо региональных китайских элит. Руководство Китая чрезвычайно ревностно относится к подобным вопросам, поскольку старается не допустить возможности шантажа иностранными государствами, либо негосударственными структурами ответственных китайских работников. В случае если такой факт действительно имел место, то мы наблюдаем типично китайскую, мгновенную и предельно жесткую реакцию.

Таким образом, инициаторы проекта Биткойн справились с еще одной сложной задачей и, осуществив накануне рождественских праздников 2013 года мощную коррекцию курса Биткойна и параметров его динамики, предоставили необходимое время на осмысливание процесса всем участникам системы Биткойн, подготавливая новый этап в развитии системы.

Затем в рамках все той же очевидной логики наступил этап жесткого гашения волатильности и удержание курса Биткойна в строго определенных пределах. Это необходимо для того, чтобы Биткойн вернул себе функцию платежного средства и перестал ассоциироваться исключительно со спекуляциями. Соответственно используя различного рода события внутри инфраструктуры Биткойн, часть из которых могла быть организована самой командой, в 2014 году удалось резко снизить волатильность Биткойна и обеспечить его курс на достаточно высоком уровне к доллару.

Подытоживая, можно сказать, что в каком-то смысле феномен Д. Ассанжа, миссия Э. Сноудена и явление

криптовалют, включая систему Биткойн, являются знаками новой реальности и коренятся в неких глубинных процессах развития технологий, элитных структур, политики и экономики в целом.

### 5.6. Биткойн: итоги и перспективы

Несмотря на пятилетнее существование Биткойна, до сих пор нет ясности, чем она является. На собственном сайте Биткойн характеризуются как «цифровая валюта». В официальных отчётах Всемирного банка, ЕЦБ и ФБР – «виртуальная валюта». По классификации комиссии по финансовым преступлениям (FinCEN) при министерстве финансов США Биткойн относят к «децентрализованным виртуальным валютам». Часто Биткойн называют «криптовалютой». Министерство финансов ФРГ считает Биткойн вариантом частных денег, которые могут быть использованы для «многосторонних клиринговых операций». Чтобы впредь не путаться в терминологии, предлагаем использовать достаточно нейтральное, но полностью соответствующее сути дела название «дикойн» (digital coin или «цифровая монета»).

С высокой степенью вероятности можно предполагать, что цифровые валюты, или дикойны пришли в мировую хозяйственную систему надолго. Подобно джину из известной арабской сказки, если их однажды выпустить на волю, то очень трудно уничтожить или сделать вид, что дикойнов никогда не было. Безусловно, в будущем будут меняться конкретные виды цифровых денег, их функционал, сферы, юридический режим использования и т.п. Но феномен дикойнов будет, по всей видимости, существовать.

Краткосрочные перспективы цифровых валют и, прежде всего, системы Биткойн зависят от позиции основных акторов экономической жизни. Начнем с государственных институтов. Есть все основания полагать, что все государственные регуляторы, включая тех, кто

благожелательно, либо нейтрально настроен к Биткойнам, либо другим криптовалютам в ближайшее время главное внимание будут уделять решению анонимности электронных кошельков Биткойнов и других цифровых валют, а также недопущению возможности их использования в криминальных целях и отмывании преступных доходов.

Это связано, по меньшей мере, с тремя обстоятельствами.

Во-первых, по данным Global Financial Integrity, ежегодно в течение последних 15 лет растут масштабы незаконных и преступных денежных потоков в мировой финансовой системе. Понятно, что эти потоки осуществляются в традиционных валютах. Тем не менее, по мнению и данной организации, и подавляющего числа других регуляторов, Биткойн при сохранении анонимности электронных кошельков создает новые риски для незаконных финансовых трансфертов и сужает возможности правоохранительных органов для борьбы с ними.

Во-вторых, наличие анонимных кошельков и соответственно неконтролируемых финансовых транзакций при достаточно широком распространении анонимных криптовалют, негативно скажется на собираемости налогов. Практически во всех странах, где складывается Биткойн-экономика, регуляторы в настоящее время активно обсуждают вопросы налогообложения доходов от продажи товаров и услуг за Биткойны, либо доходов от спекуляции Биткойнами как активами.

В-третьих, сохранение анонимных кошельков Биткойнов при широком распространении этой платежной системы, как показывают расчеты российской компании Infowatch, может в ближайшем будущем вызвать лавину кибервымогательств, связанных с блокированием компьютеров. Масштабы кибервымогательств прямо связаны с вероятностью обнаружения преступников. Чаще всего это происходит при выплате выкупа. Ано-

нимизация получателя средств делает фактически невозможным его обнаружение, а соответственно в разы повышает привлекательность кибервымогательства как криминального бизнеса.

В этой связи регуляторы и правоохранительные ведомства тех стран, где достаточно благожелательно на сегодняшний день относятся к Биткойнам, включая США, Великобританию, Германию, Японию и т.д. будут без сомнения усиливать нажим для обеспечения в конечном счете деанонимизации электронных кошельков Биткойнов.

Этот нажим с чрезвычайно высокой степенью правдоподобия приведет к окончательному расколу в движении биткойнеров. Одну часть составят те, кто уже ищет и будет готов искать точки соприкосновения с государственными органами и соответственно вырабатывать решения, обеспечивающие существования Биткойнов и других криптовалют в правовом поле. Другая, вероятно, меньшая часть образуется из биткойнеров-экстремалов, принципиально настроенных против любых контактов с государственными органами и более того, считающих эти контакты предательством Биткойн-движения. Такой раскол уже произошел.

Поскольку система Биткойн все больше превращается в большой, охватывающий сотни тысяч, а скоро и миллионы людей бизнес, то есть основания полагать, что основные участники Биткойн-движения будут тесно взаимодействовать с государственными и международными регуляторами и общественными организациями.

Представляется, что, так или иначе, либо биткойнеры откажутся от анонимности платежных кошельков в тех же пределах, в которых происходит отказ от анонимности в отношении счетов в традиционных валютах, либо Биткойн будет вытеснена на обочину и его место займет другой дикойн. Поскольку же в инфраструктуру Биткойна уже вложены большие деньги, гораздо бо-

лее вероятен первый вариант событий. В программно-вычислительном аспекте уже имеются решения, которые с одной стороны обеспечивают предусмотренные в различных странах конституционные гарантии приватности, а с другой стороны, делают Биткойн приемлемым для правоохранительных и налоговых органов тех стран, которые заинтересованы в развитии электронных валют.

Без сомнения подавляющая часть криптоанархистов, шифропанков, воинствующих программистов-либертарианцев, и просто романтиков Биткойна откажется идти на компромиссы с государствами в любых формах, принимать во внимание интересы инвесторов в инфраструктуру цифровых валют, крупных торговых и инвестиционных компаний и выберут путь сохранения и даже усиления полной анонимности и непроницаемости.

Прямым подтверждением этому стало заявление разработчика Zerocoin Мэтью Грина. Первоначально Zerocoin планировался как расширение Биткойна, способствующее повышению конфиденциальности транзакций внутри платежной сети Биткойн. Уже в этом году Мэтью Грин объявил о том, что Zerocoin будет являться альтернативной криптовалютой, независимой от Биткойна. На своей пресс-конференции он особо подчеркнул, что это будут первые, по-настоящему полностью анонимные цифровые монеты и абсолютно закрытая, никак недоступная государствам, платежная система.

Можно предположить, что именно Zerocoin, а не Биткойн превратится в настоящий кошмар для регуляторов и именно в эту платежную систему уйдет подавляющее большинство теневых транзакций. Именно эта платежная система будет обслуживать подавляющую часть и преступности, и спецслужб, которые, как показывает сеть Tor, в одних случаях борются, а в других – переплетаются друг с другом. Впрочем, это происходит и в оффлайне.

Ключевой для перспектив системы Биткойн и других криптовалют представляется позиция крупных за-

падных интернет-продавцов. В прошлом ни один из них не тестировал применение Биткойнов в своих торговых системах. В этом году ситуация изменилась. С начала года Биткойны принимает в качестве оплаты гигант социальных игр, компания Zynga. Еще более значимым стало решение с начала 2014 года принимать Биткойны в качестве платежного средства одним из крупнейших американских розничных интернет-магазинов Overstock. Имеется целый ряд заявлений и других компаний из различных сфер торговли. Понятно, что в настоящее время решение об использовании Биткойна в качестве платежного средства имеет в значительной степени рекламный характер, а кроме того является элементом продуманной, исподволь проводимой кампании поддержки разнообразных цифровых валют. Что же касается широкого использования Биткойнов, либо других цифровых валют в розничной онлайн-торговле, то для этого необходимо, во-первых, окончательное урегулирование вопросов с государственными регуляторами, а, во-вторых, разработка Биткойн-кошельков, надежно защищающих их владельцев от киберпреступиков.

Крайне любопытные процессы в отношении дикойнов происходят в недрах главных интернет-гигантов мира. В недавнем прошлом ряд из них собирался создать тот или иной вид виртуальных денег. Некоторые даже от слов перешли к делу. Однако до поры до времени они были вынуждены решать более реалистичные рыночные задачи и даже сворачивать хождение своих виртуальных валют. Наглядный пример – Facebook Credits, от которых компания Марка Цукерберга отказалась через полтора года после запуска. Еще один пример – валюта Microsoft Points, которая не вызывает симпатии у пользователей из-за сложной системы конвертации в доллары.

В этой связи особое значение имеет сделанное в самом конце 2013 года заявление компании eBay о подаче патентной заявки 20130339188. Мало того, что компа-

ния подала патентную заявку, она позаботилась, чтобы сообщение об этом было вынесено на первые полосы ключевых мировых СМИ.

Любопытно, что и в заявке, и в пояснениях патентуемая платформа называется одновременно и подарочной системой, и системой маркеров, и платежным инструментом. Из чтения заявки становится понятным, что речь идет о своего рода полноценных электронных корпоративных деньгах, т.е. еще одном виде криптовалюты.

Для того чтобы пользоваться проектируемой eBay системой, в ней не нужно открывать специальный счет, как этого требуют все нынешние системы. Более того, сам получатель подарка, маркера, либо платежного инструмента, что одно и то же, может оставаться анонимным. Жестко определяется лишь отправитель, который обязательно должен иметь регистрацию в системе eBay. Патентуемая заявка, в отличие, например, от системы Биткойн, предполагает возможность программного встраивания самых различных фильтров, ограничителей для получателя маркера или платежного средства. В частности, в заявке записано, что: «Маркер может быть ограничен для использования только в конкретном магазине, определенной группе магазинов, или указанной сети магазинов. Маркер может быть ограничен покупкой только определенного вида товара или услуги. Маркер может быть ограничен в использовании географически – определенным городом, штатом, государством, регионом и т.п. Наконец, маркер может быть ограничен определенным временем своего использования. Например, только будними днями, выходными днями, с 11:00 до 1:00 вечера в будние дни, и / или в любое другое время».

Нетрудно понять, что платежное средство, как его ни называй – маркером, либо подарком, за спиной которого стоят гигантские международные торговая компания eBay и платежная система PayPal, обладающее невидан-

ной гибкостью, избирательностью, сочетающее жесткий контроль с определенной приватностью, имеет просто фантастические перспективы для своей экспансии в мире платежных средств.

В последнее время Биткойн, Litecoin и другие дикойны начали активное проникновение в альтернативные экономические уклады. Вопреки сложившемуся мнению, денежная экономика не является единственным мировым хозяйственным укладом. Так, по данным крупнейшей международной бартерной ассоциации International Reciprocal Trade Association только в число ее членов входит почти 500 тыс. предприятий с годовым оборотом более 12 млрд. долларов.

Во многих слаборазвитых странах, где финансовые системы находятся в удручающем состоянии, последние три-четыре года все активнее происходят эксперименты с бартерными соседскими сетями, локальными союзами взаимопомощи и т.п. При всем их разнообразии в целом их можно описать как различные виды коммунитарной экономики, базирующиеся на общине, на обмене результатами деятельности и отказе от ростовщичества.

Одним из самых известных в мире в этой сфере стал эксперимент с локальной валютой эко-песо на севере Кении. Его организовал в 2010 году специалист в области физики высоких энергий из США Уилл Раддик. Менее чем за год доходы в общине выросли на 30%, закипела хозяйственная жизнь. Причем, контраст между общиной, использующей локальные деньги, с демереджем и остальной Кенией был столь велик, что кенийские власти заключили американца в тюрьму. Лишь после вмешательства ООН и Фонда Рокфеллера, который взял эксперимент под свой патронаж, американец был вызволен из тюрьмы, а эксперимент распространен более чем на 50 общин страны.

В этом году объявлено, что впредь в качестве эко-песо будет использоваться специально разработанный

для развивающихся стран вариант Litecoin, приспособленный для использования и хранения на простых дешевых мобильных телефонах. Были сделаны специальные обучающие видеоролики. Одновременно предусматривается использовать эту платежную систему и для международных переводов средств многочисленных кенийских рабочих, занятых в богатых аравийских странах. Сегодня за перевод они платят 8%, а система будет брать комиссионные менее 1,5%. Уже в этом году объявлено, что подобную систему возьмут на вооружение более 50 общин в другой части мира – в Бразилии, расположенных вокруг города Форталеза. В случае успеха бразильский вариант дикойна будет использоваться в сельских общинах 16 штатов Бразилии.

Кстати, интересно, что в настоящее время в мире идут большие дискуссии относительно эффективности применения так называемых свободных денег С. Гезелля. Про свои деньги он писал: «Только деньги, которые устаревают, подобно газетам, гниют, как картофель, ржавеют, как железо, и улетучиваются, как эфир, способны стать достойным инструментом для обмена картофеля, газет, железа и эфира. Поскольку только такие деньги покупатели и продавцы не станут предпочитать самому товару. И тогда мы станем расставаться с товарами ради денег лишь потому, что деньги нам нужны в качестве средства обмена, а не потому, что мы ожидаем преимуществ от обладания самими деньгами». Смысл этих денег состоит в том, что их ценность уменьшается год от года. А это стимулирует не накопление, а расходование денег. Соответственно, активизирует спрос и дает шансы для предложения. В конце прошлого года программисты и разработчики создали на основе платежной системы Биткойн альтернативную валюту Freicoin, которая полностью реализует принципы свободных денег С. Гезелля. Можно ожидать, что в странах, где законодательство позволяет использовать частные деньги, например,

в Швейцарии, в Германии Freicoin уже в этом году может получить распространение на уровне общин.

В условиях ширящихся контактов Биткойн-сообщества с государственными регуляторами, увеличением числа компаний и финансовых институтов, готовых работать с криптовалютами, расширением круга регионов и имущественных групп, охваченных электронными деньгами, ростом разнообразия цифровых криптовалют и дикойнов всех видов, инвесторы все более активно вкладывают средства в инфраструктуру дикойнов. Наряду с созданием ширящегося числа бирж и торговых площадок, включая социальные сети – торговые площадки, обменники, появляется все больше специализированных организаций по предоставлению конкретных услуг. В первую очередь они связаны с решениями в сфере безопасности пользования и хранения криптовалют. Не так давно одна из подобных организаций смогла заполучить в партнеры всемирно известную страховую компанию Ллойд. По оценке инвестиционных аналитиков на ближайшие годы бизнес, связанный с созданием инфраструктуры обслуживания цифровых платежных систем станет одним из самых выгодных сегментов высокотехнологичного бизнеса.

Просматривается и еще один совершенно неожиданный оборот в теме цифровых валют. Известно, что цифровые валюты порождены программистским сообществом. А, как известно, мировая столица информационных технологий это – Силиконовая долина. В 2012 года один из самых преуспевающих и богатых людей Силиконовой долины Тим Дрейпер, венчурный предприниматель в третьем поколении, собрал предрождественскую конференцию в университете, который он сам же в свое время и учредил. На пресс-конференции он предложил раздробить штат Калифорния на несколько более мелких штатов. При этом было предложено отдельно выделить Силиконовую долину со столицей штата в Сан-

Хосе. В качестве аргумента он сказал: «Всякий раз, когда я пытаюсь поговорить с людьми в Сакраменто, я вижу, что они вообще не понимают целей, которые мы преследуем в Кремниевой долине. Скажем, мы работаем над новыми коммуникационными системами, однако эти системы на несколько порядков опережают нашу бюрократию. Поэтому бюрократы постоянно пребывают в роли догоняющих, а мы не понимаем, как они собираются нами управлять». Далее он пояснил на примерах автомобилей-роботов Google, дронов, которые будут доставлять пиццу и прочих новинок, что нынешнее поколение компьютерщиков состарится, пока власти штата узаконят их использование и напишут соответствующие нормативные документы.

Разделить Калифорнию вряд ли конечно удастся. Но в том же декабре The Seasteading Institute объявил о том, что в 2014 году он практически приступает к строительству двух автономных морских поселений, каждое примерно на тысячу человек. Одно из этих поселений будет расположено за пределами зоны юрисдикции США у берегов Калифорнии, как раз напротив Силиконовой долины. А второе – в морском заливе, рядом с Никарагуа и Сальвадором. Второе морское поселение будет заниматься созданием аквакультуры и добычей полезных ископаемых из морской воды. А вот первое как раз будет предназначено для жизни сегодняшних обитателей Силиконовой долины. Имеется в виду, что оба острова не будут подпадать под юрисдикцию Соединенных Штатов. Сейчас практически решается вопрос с юрисдикцией этих островов.

Предусматривается, что денежно-финансовой системой этих островов станет специально созданная криптовалюта, либо одна из модификаций Биткойна. Все это могло бы показаться шуткой, если бы не три обстоятельства. В проект вложены очень серьезные ресурсы. Архитекторами и подрядчиками-исполнителями высту-

пают ведущие компании. Главным инвестором проекта стал чрезвычайно серьезный и известный во всем мире Питер Тиль и его товарищи по «Мафии PayPal». Касаясь причин, побудивших его участвовать в этом проекте, Питер Тиль сказал: «Никто не смотрит в будущее, на 15-20 лет вперёд, как наши родители. Планы строят только краткосрочные. Большая часть из того, что сделали наши родители – Манхэттенский проект, сеть федеральных автострад и т.д., невозможно сделать сейчас... Как бы то ни было, после 40-летних блужданий нелегко найти путь назад в будущее. Если мы хотим, чтобы это будущее всё-таки наступило, очень важно думать о нём гораздо больше, чем все эти годы. Первый и самый важный шаг для этого – увидеть, что мы все сейчас находимся посреди пустыни, а отнюдь не в заколдованном лесу».

Кстати о планах создания подобных островов, начиная с этого года, и размещения на них зон сверхновых технологий заявили правительства Японии и Израиля. Они уже подыскивают места дислокации плавучих поселений и определяют тех, кто на них будет вести работы. Кстати, предусматривается, что на этих островах будут созданы специализированные финансово-экономические режимы, возможно, с использованием цифровых валют.

Если же вернуться от островов в океане к российским реалиям, то применительно к цифровым валютам с учетом позиции, изложенной в информации ЦБ, можно солидаризироваться с мнением главы Сбербанка Г. Грефа. Недавно он заявил журналистам, что «в теории возможна эмиссия виртуальной валюты. У нас есть «Яндекс. Деньги», пока это не эмитируемая валюта, но первый шаг в эту сторону. Мы не спешим с этим... Надо посмотреть весь коммерческий смысл и привлекательность для клиентов. Мир уже не остановить, он пошел в этом направлении, и я думаю, что те грандиозные эксперименты, которые проходят с Bitcoin, должны закончиться один-два

раза крахом с тем, чтобы было выработано глобальное регулирование».

Вместе с тем, цифровые валюты не всегда требуют сразу же глобального регулирования. Несмотря на то, что мир глобализован, первоосновой финансовой системы является национальный суверенитет. Соответственно, любая цифровая валюта, будет ли она международной, страновой или будет носить корпоративный или локальный характер, должна строго соответствовать законодательству той страны, в киберпространстве которой она используется.

Однако в ключевой позиции Г. Греф прав. Платежные электронные системы и валюты – это несомненная реальность. Более того, с некоторым авансом можно сказать, что они являются своего рода третьей денежной революцией. Первая была связана с появлением золотых и серебряных денег, как универсального платежного средства, имеющего собственную ценность, удобного для расчетов, легкого в хранении и транспортировке. Эти деньги были основаны на взаимодействии людей и их взаимном доверии. Затем произошла революция бумажных денег, где доверие было заменено иерархией силы эмитента, его возможностью принудить к использованию денег. В каком-то смысле электронные валюты с их распределенной сетью доверия являются возвратом к первоначальным деньгам, базирующимся именно на доверии. Но электронные платежные системы с требованием создания мощной инфраструктуры, согласованием платежных режимов, вписыванием в реальные, уже сложившиеся, национальные и мировые финансовые отношения, предполагают, конечно же, наряду с распределенной сетью доверия и наличие иерархии, связанной с фактором национального суверенитета. Возможные будущие дикойны будут иметь в основе сочетание горизонтали распределенного доверия и вертикали государственной власти.

Прав Г. Греф и еще в одном обстоятельстве. Несомненно, нынешние электронные деньги представляют собой первое поколение цифровых монет. В частности, им свойственна статичность. Например, в Биткойне наперед заданы параметры эмиссии, недостаточно проработаны вопросы безопасности платежной системы и простоты ее использования для рядового пользователя, даже обладающего хорошими компьютерными навыками. В этой связи надо отметить, что у российских программистов есть целый ряд наработок, связанных с новым динамичным, или адаптивным поколением криптовалют, где все их параметры могут гибко меняться в зависимости от изменений внешней среды.

В условиях, когда многие финансовые аналитики прогнозируют новый этап глобального экономического кризиса, наличие и развитие Биткойна и иных виртуальных криптовалют выгодно целому ряду глобальных и локальных финансово-экономических групп для начала построения новой макроэкономики и новой модели мировой финансовой системы. И игнорировать эту реальность было бы неосмотрительно.

# Глава 6
# ПЯТЬ ЛЕТ ПОСЛЕ КРИЗИСА

## 6.1. Другой капитализм

В пятилетнюю годовщину финансово-экономического кризиса появилось множество научных, аналитических и экспертных публикаций, посвященных его причинам и следствиям, сегодняшнему состоянию мировой экономики. Одной из самых заметных стала статья Нобелевского лауреата Джозефа Стиглица «Пять лет между небом и землей». Еще в своей книге 2010 года «Крутое пике и новый экономический порядок» Д. Стиглиц сделал вывод, что «кризис выявил фундаментальные недостатки в капиталистической системе или, по крайней мере, в той ее своеобразной разновидности капитализма, которая сложилась в Соединенных Штатах Америки». Преодоление кризиса Нобелевский лауреат связывает с новой «альтернативной моделью капитализма», которая базируется на «балансе ролей рынка и ролей правительства, достижимого во многом благодаря деятельности нерыночных и неправительственных институтов».

В статье Стиглиц подводит некоторые итоги. Он отмечает, что за эти годы «проблемы так и остались неразрешенными, а отчасти еще и усугубились». Резюмируя пятилетние усилия по преодолению кризиса, он отмечает, что «финансовая система, может, и стабильнее, чем была пять лет назад, но это низкая планка – в те времена она балансировала на краю пропасти. Представителям правительства и финансового сектора, которые поздравляют себя с тем, что банки вновь стали прибыльными, а в

регуляторной системе произошли небольшие, хотя и достигнутые с большим трудом изменения к лучшему, следует сосредоточиться на том, что еще не сделано. Стакан в лучшем случае полон на четверть; для большинства же людей он на три четверти пуст».

Фактически Д. Стиглиц говорит о том, что необходим капитализм с большим государственным регулированием, меньшей ролью финансового сектора и большим упором на социальные вопросы и интересы среднего класса. Эти мысли он развивает в недавно вышедшей книге «The Price of Inequality: How Today's Divided Society Endangers Our Future Paperback». Однако представляется, что дела обстоят на порядок серьезнее. На наших глазах происходит своего рода трансформация несущих конструкций глобальной и национальных экономик. Причем эта трансформация по своей неумолимой логике, отнюдь не ведет в сторону усиления социального характера государства и уменьшению неравенства. Этой же теме посвящен едва ли не главный политэкономический бестселлер 2014 года, который наперебой цитируют Дж. Йеллен, Ф. Оланд, Б. Обама и др., – «Capital in the Twenty-First Century» Т. Пикетти.

Чтобы разобраться с происходящими процессами, необходимо присмотреться к сложившейся парадоксальной ситуации.

Достоверно известно, что более ста экономистов, аналитиков, инвестиционных экспертов, специалистов вычислительных наук, принадлежащих к зачастую противоположным школам, придерживающихся разных идеологических убеждений, достаточно точно предсказали сроки и масштабы кризиса. Это говорит о том, что само по себе предсказание кризиса не может выступать фактором подтверждения правоты той или иной теории или подхода.

Гораздо более интересно нечто другое. Практически никто в течение пяти лет не смог спрогнозировать теку-

щую и краткосрочную динамику. Как правило, преобладали либо апокалиптические оценки, предрекающие крушение мировой экономики в ближайший год или даже месяцы, либо расчеты, ориентированные на начало периода процветания и благоденствия. Как мы знаем, не произошло ни того, ни другого.

Традиции экономических школ и экспертные оценки, базирующиеся на фактах докризисного мира, оказались неэффективными в посткризисной действительности. Можно говорить о том, что кризис начал формировать новую реальность. Соответственно, первостепенной задачей становится выработка понимания ее главных черт и движущих драйверов. Нужно понять, что в новой реальности сохранилось от докризисного мира, а в чем состоит новизна, сбивающая с толку экспертов и прогнозистов.

Начнем с фундаментальных черт докризисного мира, которые определяют и новую реальность. Первая, и главная черта – это тотальная финансиализация экономики. Ее масштабы таковы, что позволили гениальному русскому мыслителю А. Зиновьеву в своей книге «Запад. Феномен западнизма», написанной в 90-е годы прошлого века, назвать поздний капитализм финансизмом. Кризис в этом плане ничего не изменил, а более того, ситуацию усугубил. Едва ли не самая наглядная характеристика финансиализации экономики – это то, что на один доллар торговых операций с товарами и услугами, приходится десять долларов операций с финансовыми активами всех видов. Не менее красноречивы данные международной исследовательской организации FSB. Если в 2002 г. активы 28 крупнейших банков составляли 48% мирового ВВП, в предкризисном 2007 г. – около 60%, то сейчас подбираются вплотную к 66%. Сегодняшний мир это, в первую очередь, мир секьюритизации и торговли финансовыми активами, и во вторую, подчиненную – производства реальных товаров и услуг.

Вторая ключевая черта – это усиление неравновесности экономических систем – от глобальной экономики до отдельных корпораций. В главной составляющей глобальной экономики – сфере капитальных товаров и финансовых активов – невидимая рука рынка не действует. Эти рынки исходно неравновесны. Эта неравновесность сыграла роль катализатора кризиса, разразившегося в 2008 г. Продолжает она усиливаться и в новой реальности. В посткризисный период цены на акции, включенные в основной фондовый индекс S&P 500, растут почти в 10 раз быстрее, чем экономика. Значительная часть финансовых аналитиков полагает, что надувается новый, на этот раз фондовый пузырь, который неизбежно в свое время лопнет.

Третьей ключевой чертой, перешедшей из докризисного мира в новую реальность, стал пирамидальный характер финансовой системы позднего капитализма. Он не только сохранился, но и усилился. По своему экономическому смыслу и математическому выражению нынешняя глобальная финансовая система мало чем отличается от схем Понци и Мавроди. Все хорошо знакомы с ситуацией с государственными долгами, которые во многих странах мира долгое время растут по экспоненте. Прежде всего, это относится к США, Японии и Великобритании.

Гораздо менее известен тот факт, что основа основ современной западной экономики, а именно, банковская система, также построена как пирамида. Базисным институтом рыночной капиталистической экономики является банковская система, покоящаяся на депозитах. Пирамидальный характер этой системы подтверждается следующим фактом. На сегодняшний день в Соединенных Штатах Америки каждому обладателю депозита гарантированы вклады на 250 тыс. долларов. Но это бумажная гарантия. Соотношение фонда страхования депозитов к общей сумме страхуемых депозитов до кризи-

са составляло чуть более 1%, а сейчас всего 0,4%, по данным А. Турбанова, генерального директора ГК «Агентства страхования вкладов», почерпнутым из официальных американских источников. Такое соотношение характеризует только пирамидальные схемы.

В качестве четвертой определяющей черты глобальной экономики остается долговременное падение многофакторной эффективности производства. Это падение нагляднее всего выражается в длящемся вот уже 50 лет падении темпов роста ВВП в развитых богатых странах. Если в 60-е годы прошлого века ВВП рос ежегодно на 5,5%, в 70-х – 3,8%, в 80-х – 3,2%, в 90-х – 2,8%, в начале этого века, до экономического кризиса – 2,1%, то в 2009-2012 гг. – всего 0,4%.

С долговременным снижением многофакторной производительности транснациональные корпорации пытаются бороться путем сохранения системы международного разделения труда, сложившейся в 90-е и нулевые годы. Эта система базируется на том, что основные центры прибыли и создания добавленной стоимости, осуществление НИОКР транснациональные корпорации оставляют на территории собственных стран, а трудоемкие, малоприбыльные операции переносят в так называемые новые, развивающиеся страны. Тем самым поддерживается и закрепляется экономическое неравенство и технологическое превосходство. Это хорошо видно на примере Китая. Вот уже долгое время подавляющая часть экспертов, а также средств массовой информации прочат этой стране замечательное экономическое и технологическое будущее. Между тем, как до, так и после кризиса, более 75% экспорта из Китая осуществляется транснациональными компаниями, их филиалами или дочерними и совместными предприятиями. К чему это ведет?

Посмотрим на примере производства iPhon. В продажной цене iPhon 64% составляли доходы Apple, 36% –

китайского сборщика. Статистически эти 36% в долларовом виде включаются в показатели экспорта Китая. Но с точки зрения собственности и распределения цены дела обстоят не так. На долю добавленной стоимости, созданной в самом Китае, приходится лишь 1,3%. Остальная часть идет поставщикам комплектующих изделий, которые в подавляющем большинстве расположены вне страны. Сходная, хотя возможно и чуть лучшая картина характерна и для другой технологической экспортной продукции Китая и других новых индустриальных стран.

В ходе кризиса не только не уменьшилось, но и упрочилось господство финансовой элиты в мировой глобальной экономике. Это пятая ключевая черта, характеризующая как докризисный мир, так и новую реальность. Суть дела наиболее полно раскрывает работа исследователей Федерального института технологий в Цюрихе. Они изучили данные по 37 млн. наиболее крупным предприятиям и компаниям мира. При этом, следует иметь в виду, что восемь тысяч крупнейших корпораций производят по данным McKinsey около 90% мирового ВВП. Выяснилось, что 40% всех компаний контролирует 147 корпораций. Причем, указанные 147 корпораций, в конечном счете, находятся под контролем 40 крупнейших структур, из которых 29 относятся к финансовому сектору, и представляют собой либо банки, либо инвестиционные и другие фонды. Т.е. одна миллионная доля компаний контролирует всю глобальную экономику. Причем, есть все основания полагать, что контроль за ключевыми финансовыми институтами осуществляется хотя и большим, но ограниченным кругом групп, семей и кланов.

Внимательный анализ отмеченных выше черт послекризисного мира, показывает, что кризис не только не решил и даже не сгладил, а, наоборот, обострил противоречия, свойственные докризисной глобальной экономике.

Особый интерес представляет выделение новых черт, проявившихся уже в посткризисный период, и по сути выступающих главными драйверами складывающейся на наших глазах реальности.

Во-первых, сегодня для США, Японии и Западной Европы как о свершившемся факте можно говорить о наличии как минимум трех экономических укладов и методов их регулирования. Прежде всего, это клановый, дружеский, бандитский или блатной капитализм. Этот уклад базируется на прямых и обратных связях по конвертации власти и собственности через финансовые ресурсы. По сути, на формировании нового явления для капитализма – появлении новой субстанции – «власть собственности», пользуясь термином А. Фурсова. Т.е. власть превращается в финансы, а затем в собственность и наоборот. Лучшим подтверждением этого является деятельность ФРС. Согласно частичному аудиту, в период кризиса ФРС передала в обмен на токсичные активы, либо предоставила фактически на беспроцентной основе более 16,3 трлн. долларов крупнейшим американским и международным банкам. Об этом можно прочитать на с. 131 материалов аудита ФРС, опубликованных на сайте сенатора Б. Сандерса. Из них более 3 трлн. долларов, как признала ФРС в результате расследования агентства Bloomberg, составили долгосрочные беспроцентные кредиты, т.е. фактически даровые деньги. Следует отметить, что этот процесс продолжается без перерыва вот уже пятый год в виде так называемых мер по количественному смягчению, или QE. Совокупные его размеры значительно превышают на сегодняшний день 3 трлн. долларов. Причем 10% от этой суммы составляют прямые спекулятивные доходы первичных банков-дилеров, т.е. тех крупнейших финансовых институтов, которые контролируют американскую и глобальную экономику.

Второй уклад можно охарактеризовать как государственно-монополистический, программно-сетевой

уклад. В его рамках действуют крупнейшие ТНК, особенно из военно-промышленного, биотехнологического, информационного и иных технологических кластеров. В рамках этого уклада опять-таки практически не действуют рыночные методы регулирования. Перераспределение средств осуществляется через государственный бюджет, в виде госзаказов, подрядов и контрактных программ. Несомненными лидерами в этом укладе являются США, Германия и Франция. В э тих странах через государственный бюджет перераспределяется от 55% – во Франции до 41% ВВП – в США. Причем размеры финансирования государственных программ, выполняемых частными подрядчиками, главным образом в высокотехнологической сфере выросли за посткризисный период в США, Западной Европе и Японии. Например, в США они составляют в настоящее время более 200 млрд. долларов в год.

Таким образом, собственно рыночные отношения и соответственно традиционные методы формирования капитала продолжают действовать в основном для среднего и малого бизнеса в средне- и низкотехнологичных отраслях, производящих в основном товары и услуги для населения, а также в сырьевом секторе.

Свободного рынка частных производителей и традиционного капитала, о которых грезят либералы, на Западе больше не существует. В посткризисную эпоху там складывается совершенно иной, сложный строй, в котором представлены уклады с разными методами регулирования и развития, которые находятся между собой в состоянии симбиоза и конфликта одновременно. Правительства и центральные банки пытаются «в ручном режиме» отрегулировать взаимодействия между этими противоречивыми укладами.

Во-вторых, драйвером новой реальности является финансово-кредитная политика, осуществляемая центральными банками и, прежде всего, ФРС, как главным эмиссионным и финансовым институтом мира.

Главная ошибка подавляющего большинства прогнозистов и состояла в том, что анализируя политику центральных банков, проводящих последние несколько лет согласованную эмиссию, они, мысля в рамках докризисного периода, уверенно предсказывали гиперинфляцию, либо катастрофу доллара. Однако, ни первого, ни второго пока не произошло.

Сложилась парадоксальная ситуация. Только ФРС в рамках QE 1,2,3 провела на сегодняшний день эмиссию более 3 трлн. долларов. При этом, инфляция не превышает 1%. Сходная картина складывается в Европе и в Японии, где центральные банки также проводят масштабные эмиссии при отсутствии инфляции.

Как это могло произойти? В новой реальности финансово-денежная политика носит не рыночный, а программный характер и строится на основе не законов свободного рынка, а соглашений между эмиссионными центрами, правительствами, крупнейшими банками и корпорациями.

Анализ статистических данных за 2008-2013 гг. показывает, что основная сумма средств, влитых в экономику, пошла на финансовые рынки и на финансирование государственных расходов, а значит, в немалой степени на осуществление программ, ориентированных на высокотехнологичные сектора экономики. Причем, распределение средств между финансовыми рынками перестало носить свободный рыночный характер. Имеется достаточно много фактологических подтверждений того, что последние пять лет центральные банки фактически согласуют с первичными дилерами, т.е. крупнейшими банками и финансовыми институтами, направления расходования выделяемых в процессе эмиссии средств.

Главным направлением являются рынки ценных бумаг. Среди этих рынков первенство принадлежит рынкам государственных ценных бумаг, в первую очередь, США, а также фондовому рынку, где без сомнений и

вполне регулируемо надувается новый пузырь. Именно с тем, что деньги направляются, прежде всего, на рынок финансовых активов в виде акций и связаны рекордные показатели индексов DJ, Nasdaq и проч. Т.е. фактически инфляция доллара, евро и иены происходит весьма заметными темпами, но происходит она в отношении активов, т.е. цены акций, облигаций и т.п. Это парадоксальным образом ведет к увеличению богатства обладателей этих активов. Дело в том, что в новой реальности произошло полное размежевание рынков реальных товаров и услуг и рынков финансовых активов. За счет роста богатства, полученного на основе стремительного подорожания финансовых активов, резко возрастают возможности прямых инвестиций и осуществления операций по приобретению капитальных активов на внебиржевых рынках или на биржевых рынках, где операции осуществляются по предварительному согласованию.

Что же до сырьевых рынков, как рынков активов, то складывается впечатление, что в настоящее время центральные банки ограничивают возможности финансовых институтов к вложениям на этих рынках, что ведет либо к сохранению, либо к падению цен на сырьевые товары. В их цене в последние годы до 50% приходится на так называемую спекулятивную составляющую, зависящую от цены фьючерсов и других производных на эти товары.

Поскольку основная часть средств от эмиссий центральных банков в послекризисный период идет на финансовые рынки активов, то соответственно деньги почти не поступают в реальную экономику, а соответственно и не происходит инфляция. Еще одним, едва ли не важнейшим фактором, почему не происходит инфляции, являются ограничения по кредитованию со стороны заемщиков. Сегодня сложилась ситуация, когда банки и другие финансовые институты под завязку забиты кэшем, т.е. ликвидностью и готовы предоставлять кредиты

даже под 3-5% годовых. Однако кредиты у банков не берут ни корпорации, ни домохозяйства.

Докризисную экономику можно было охарактеризовать как закредитованую экономику. Вот уже без малого 30 лет в ней все жили в кредит, взаймы у будущего. По факту, на сегодняшний момент ситуация остается прежней, но в новой реальности все сильнее проявляется иная тенденция. Крупные корпорации не берут кредиты, поскольку они им не нужны. В условиях роста цен и спроса на финансовые активы, включая низкопроцентные корпоративные облигации, у них огромные запасы ликвидности от операций на рынке ценных бумаг. Средний, а тем более малый бизнес не берет кредиты, поскольку нет платежеспособного спроса. Реально даже так называемая оживающая экономика США покажет по прогнозам в этом году темпы роста не более 2%. С учетом же американской статистики, которая вовсю использует так называемые гедонистические индексы и другие статистические ухищрения, скорее всего экономического роста как такового нет вообще. В Западной Европе и Японии даже по официальной статистике имеет место рецессия. А если нет роста и расширения, то зачем брать кредиты. Домохозяйства также намного менее активно, чем раньше, берут кредиты. В условиях не растущих длительное время доходов, высокого уровня фактической безработицы, необходимости покрытия ранее взятых кредитов и особенно процентов по ним, перед домохозяйствами стоит задача снижения кредитной зависимости. Остаются правительства. Они продолжают выступать заемщиками, но делают это более осторожно, чем раньше. Повсеместно вводится режим строгой экономии для того, чтобы уменьшить темпы нарастания госдолга. Они предпринимают все меры для того, чтобы выйти на ситуацию уверенного обслуживания выплаты процентов по долгу. Ведь хорошо известно, что тем, кто исправно платит проценты, спокойно реструктуризируют долги.

Третьей новой чертой посткризисной реальности стала фрагментация и хаотизация глобальной экономики. Сегодня с уверенностью можно говорить, что финансовая экономика живет по одним законам, а реальный сектор – по другим. Внутри хозяйств наиболее развитых стран существует как минимум три уклада. Разнородные факторы определяют динамику отдельных видов финансовых активов. Нет синхронизации в экономической динамике США, Европы, Японии. Внутри самой Европы также сильно различаются реалии северной и центральной ее части – с одной стороны, и юга и востока – с другой. Различны динамика и ее драйверы в странах БРИКС. Этот перечь можно продолжать очень долго. Т.е. глобальная экономика, становится все более фрагментированной.

Одновременно происходит и хаотизация экономики. О чем идет речь? В привычном для нас докризисном мире четко можно было выделить причины и следствия. Иными словами, ограниченное число факторов и параметров определяли экономическую жизнь в целом. В новой реальности различные фрагменты экономики живут, можно сказать, своей обособленной жизнью и приводятся в действие собственными драйверами. Если раньше при изменении одного параметра изменялся другой, то теперь все чаще каждый из параметров изменяется по собственной логике. Тому много подтверждений.

Одним из самых наглядных является рынок деривативов. т.е. производных ценных бумаг, связанных с рисками. Объем этого рынка превышает 650 трлн. долларов, т.е. более чем в 8 раз больше мирового ВВП. Покупка и продажа деривативов, в конечном счете, означает покупку и продажу рисков. Можно, конечно, подойти к деривативам, как к чисто спекулятивному инструменту и говорить об их искусственном происхождении. Однако простой здравый смысл подсказывает, что покупать и продавать можно лишь то, что пользуется спросом. А в основе любого финансового продукта лежат вполне ре-

альные экономические процессы и отношения. В основе деривативов лежат риски. Огромный рынок деривативов является убедительным подтверждением тезиса о хаотизации мировой экономики. Чем сильнее хаотизация экономики, тем выше риски, а соответственно и больше объем финансовых продуктов, их секьюритизирующих.

Из теории систем известны три их типа. Первый – это детерминированные системы. В таких системах ограниченное число факторов полностью определяет динамику системы на протяжении всей ее истории. Такая ситуация была характерна для капитализма, который описывал Маркс. Второй – это динамические системы. Именно эти системы характеризуются наличием точек бифуркации, про которые, если не знают, то слышали все. Эти системы изучает синергетика. В них в определенные периоды времени скачком меняются параметры, определяющие динамику системы. Таков был докризисный мир. Третий тип – это стохастические, или хаотические системы. В этих системах, сохраняющих целостность, отдельные ее элементы и сама система управляется различными параметрами. Каждый из блоков системы имеет свои драйвера. Эти системы изучаются теорией сложности. Есть много подтверждений, что новая реальность и представляет собой стохастическую, или хаотическую систему. О том, может ли она существовать сколько-нибудь продолжительное время, можно только гадать, поскольку необходимого эмпирического материала нет, а есть только модели.

Зато с уверенностью можно сказать, что в рамках хаотической неустойчивой системы, которой на сегодняшний день является мировой социум и глобальная экономика, неизбежно должны нарастать процессы криминализации, усиливаться социальная напряженность и как результат всего этого, обостряться борьба элит, чреватая глобальной, холодной, а местами и горячей гражданской войной.

### 6.2. Несбыча мечт

Скучные партийные пропагандисты в Советском Союзе тщетно пытались убедить народ в том, что капитализм – это общество потребления, базирующееся на кредитной экономике, ростовщичестве и эксплуатации. Они так и не смогли донести до новой исторической общности, что в долгосрочной перспективе богатые становятся богаче, бедные – беднее, а средний класс обречен. Уже нет ни партийных пропагандистов, ни Советского Союза. Зато есть новая реальность глобальной финансиализированной экономики, в которой мы живем. И сколько-нибудь радужных социальных перспектив для 99% населения развитых стран мира она не открывает.

В этом году одним из лауреатов Нобелевской премии по экономике стал Роберт Шиллер. На своей пресс-конференции по поводу присуждения премии, отвечая на вопрос: «Какую проблему Вы считаете на сегодня самой важной?», он сказал: «Самая важная проблема, с которой мы сталкиваемся сегодня, по моему мнению, это рост неравенства в Соединенных Штатах и других странах мира».

Новая кризисная реальность, в которой мир живет уже более пяти лет, ускорила социальные процессы, начавшиеся примерно три десятилетия назад. В результате обострились социально-экономические противоречия, практически повсеместно скачкообразно выросло имущественное неравенство. Мутация позднего капитализма в глобальный финансово-корпоративный строй привела к подрыву социальных устоев, на которых базировалась западная цивилизация и поставила под угрозу основу основ этого строя – общество потребления.

Глобализированная экономика имеет три центра силы – США, Европу и в значительной мере Китай. Каждому из центров глобального хозяйства свойственны свои социальные напряжения, типы экономического не-

равенства и обостряющиеся социально-экономические противоречия.

«Ковбойский», по выражению О. Герземанна, капитализм в США вдохновлялся американской мечтой. Его экономика базировалась на домохозяйствах. Опорой Америки традиционно считался средний класс. В новой экономической реальности все это не просто поставлено под сомнение, а начинает разрушаться.

Пожалуй, главным процессом, происходящим сегодня в Америке является размывание и сокращение среднего класса. Впервые в мире развернутый прогноз размывания и существенного уменьшения доли среднего класса в социальной структуре дал в середине 90-х годов Андрей Фурсов в своей работе «Колокола истории».

Точного определения, кого относить к среднему классу ни в Америке, ни в мире не существует. Предлагаются различные критерии. Традиционно в Америке к среднему классу относятся люди, обладающие определенными сбережениями и накопленным имуществом, живущие без роскоши, но с комфортом, имеющие твердую уверенность в завтрашнем дне и подушку финансовой безопасности.

При всем различии оценок подавляющее большинство американских экономистов дают следующие цифры. Если в 60-90-е годы средний класс составлял примерно 60% населения США, 20% относили к низкодоходным и бедным слоям населения, и примерно 20% – к богатым, то в настоящее время пропорция составляет 45-40-15. В прошлом году одна из самых известных исследовательских организаций Per Research Center, используя данные государственного Бюро переписи и ФРС, опубликовала работу, в которой содержатся такие данные. С 1971 по 2011 годы доля среднего класса в Америке упала с 71% до 51%. Причем, три пятых сокращения пришлось на последние 20 лет.

В настоящее время 60% американцев не имеют акций и сбережений. У 45% долги превышают имеющееся имущество. Причем, две трети из них относятся к среднему классу. Оно и понятно, поскольку у большей части бедных закладывать просто нечего.

Согласно опросу Wall Street Journal, проведенному в этом году, только 42% американцев относят себя к среднему классу. Он необратимо лишился уверенности в будущем и все с большей тревогой вглядывается в личные перспективы. При этом из числа тех, кто считает себя средним классом, около 43% полагают весьма вероятным, что в течение ближайших пяти-семи лет они переместятся из среднего класса в более бедные слои населения. Согласно данным опроса, проведенного Институтом Гэллапа, почти 60% американцев из среднего класса считают возможным ухудшение своего положения в ближайшем будущем. При этом более 55% среднего класса убеждено, что не сможет дать детям достаточно качественное высшее образование, чтобы их уровень жизни был выше, чем у родителей. Но и высшее образование не решает проблем. The Cronicle of higher Education («Хроника высшего образования») как раз 20 октября сетовала на то, что в США, помимо 47 миллионов получателей продовольственной помощи, более 317000 человек с законченным высшим образованием (из них свыше 8000 с докторской степенью (степень «доктора» на Западе соответствует нашему кандидату наук)) зарабатывают себе на жизнь официантами, также 5057 докторов наук работают швейцарами, 80000 выпускников высшей школы работают барменами, а 18000 – сторожами автостоянок. В целом 17 миллионов американцев с законченным высшим образованием, согласно сведениям американского ведомства по статистике труда, работают по специальностям, которые требуют куда меньшего уровня образования чем бакалавр.

Если еще в конце 80-х гг. американский средний класс устойчиво входил в тройку самых богатых средних классов мира, то в 2012 году по данным всемирно признанного источника – Global Wealth Data Book, он скатился на 27 место и почти в пять раз уступает по уровню богатства самому состоятельному среднему классу из Австралии.

Американская мечта воплощалась в карьерах Рокфеллера, Джобса, основателя крупнейшей розничной сети Валмарта, которые из самых низов выбились в миллиардеры. В прошлом году агентство Bloomberg и телеканал Fox провели независимые опросы. В их центре стоял вопрос, работают ли в Америке социальные лифты, и можно ли при помощи упорного труда, таланта и удачи пробить себе дорогу из низов общества в самые верхи. Еще 15 лет назад положительные ответы на эти вопросы давало более двух третей американцев. На этот раз их количество уменьшилось до чуть более двух пятых. От 10 до 14% не верят больше в наличие социальных лифтов вообще. Раньше такой показатель был исчезающе мал, и составлял менее 5%.

Американская мечта для среднего и даже небогатого американца воплощалась в собственном доме с лужайкой, свободном от долговых обременений, в неплохом районе. Если в 2000 г. доля домохозяйств, обремененных долгами, составляла 40%, то в 2012 г. – уже 74%. Причем средний размер задолженности вырос с тех пор на 40% и составляет более 70 тыс. долларов, что примерно соответствует годовому доходу типичного домохозяйства американца, принадлежащего к среднему классу. При этом средние американцы в условиях кризисной экономики и высокого уровня безработицы все чаще отказываются от кредитов и все большую часть доходов направляют на покрытие ранее взятых займов. Поэтому после острой фазы кризиса не только не вос-

становился, но и даже уменьшился объем вновь взятых кредитов домохозяйств.

На фоне стремительного размывания и сжимания подобно шагреневой коже среднего класса, процветают богатые американцы. На смену американской мечте пришел принцип: победителю достается все. По данным официальной статистики в настоящее время верхний 1% самых состоятельных американцев распоряжаются 90% всех акций. Они увеличили свои доходы с 1980 года на 300%, тогда как доходы средних американцев выросли только на 40%, и то в основном в период до 1995 года. Состояния топ-1% населения США больше, чем суммарные состояния оставшихся 99%.

В новой реальности основной прирост доходов концентрируется в верхней части имущественной пирамиды. По данным авторитетных американских исследователей Эммануэля Саеза и Томаса Пикетти, верхние 10% работников получили более половины от всех доходов домохозяйств в 2012 г. А верхний процент – соответственно более 22%. Это самые высокие показатели за все время ведения официальной имущественной и доходной статистики с 1913 года. При этом на богатых приходится в настоящее время 90% установленных правительством США налоговых льгот и других чисто финансовых преференций.

На этом фоне в новой реальности национальной проблемой США стала бедность. Более 45 млн. американцев получают бесплатные талоны на питание и другие виды товаров первой необходимости. К совсем бедным относят себя в настоящее время, согласно уже упомянутому опросу Wall Street Journal 12% американцев, тогда как в 1998 году таковыми себя считали 6%. Согласно изданию New York Times, примерно 100 млн. жителей США живет в бедности или на самой ее границе. При этом по данным официального Бюро переписи США, приблизи-

тельно 6,7% американцев проживают в экстремальной бедности.

Главная причина увеличения бедности – это высокий уровень фактической безработицы. Согласно официальным данным она составляет чуть выше 7%. Однако, по альтернативным расчетам, использующим официальные статистические данные, а также ежегодному обследованию Института Гэллапа, уровень безработицы составляет несколько менее 17%. Но даже эта цифра не показывает реальное положение вещей. Согласно все той же официальной статистике в настоящее время в течение полного рабочего дня на постоянной (а не временной, сезонной и проч.) работе занято только 45% американцев, находящихся в трудоспособном возрасте.

При этом по данным обследования, проведенного по заказу Associated Press осенью этого года, четверо из пяти американцев, которые не работают полный рабочий день в течение всего года на постоянной основе, живут на грани или за гранью бедности. Характерно, что если раньше бедность имела ярко выраженный этнический характер, и распространялась в первую очередь на афроамериканцев и испаноговорящих американцев, то в настоящий момент бедняками становится все большее число белых американцев. Сейчас более 19 млн. белых американцев опустились ниже официальной черты бедности, которая составляет 23 тыс. долларов на человека в год. Они составляют более 40% обездоленных страны.

В результате размывания среднего класса, роста сверхбогатства и увеличения числа американцев, живущих вблизи, на уровне или за гранью бедности, резко выросло неравенство. Если по коэффициенту Джини американцы со своим показателем 0,45 находятся в середине мирового списка, то по уровню имущественного неравенства, включающего неравенство не только в денежных доходах, но и обладании недвижимостью, акциями и другими видами собственности, США занимает

четвертое место в мире (первую тройку составляют Россия, Украина и Ливан).

Несколько иные проблемы в Европе. Согласно все тому же О. Герземанну, здесь создан «уютный капитализм» и функционирует социальное рыночное хозяйство. Этому в немалой степени поспособствовал тот факт, что в послевоенный период в основных странах Евросоюза значительное, а иногда и подавляющее время у власти находились социал-демократы, либо центристы, проводящие социально-ориентированную политику.

В результате, в основных странах Евросоюза, например, в Германии, Франции, странах Бенилюкса, Скандинавии, а также в Швейцарии коэффициенты Джини, характеризующие неравенство доходов в полтора-два раза ниже, чем, например, в Соединенных Штатах и России. В этих же странах самый низкий уровень имущественного неравенства. Здесь же самая высокая доля среднего класса, доходящая до 65-70% населения. Эти же страны характеризуются высоким уровнем доходов государственных бюджетов к внутриваловому продукту, и соответствен доле расходов в том же ВВП. Если, например, в США доля расходов составляет 40%, в России – 37, то в Германии 44, а Франции 56. В значительной мере такая мощная социальная роль государства в экономике осуществляется за счет высокого уровня налогов, как на частных лиц, так и на бизнес.

Однако, и в Европе в новой кризисной реальности социально-экономические проблемы нарастают со скоростью лавины. Если с начала 90-х гг. с учетом инфляции доходы среднего класса в основных странах Евросоюза не увеличивались, то после острой фазы кризиса, они, например, в Германии и во Франции даже несколько снизились. Например, в благополучной Германии по данным Фонда Бертельсмана (Bertelsmann-Stiftung) и Немецкого института экономических исследований (DIW) за последние 15 лет доля среднего класса сни-

зилась с 65 до 58% от всего населения. В то же время на почти четыре миллиона возросло число граждан с низким уровнем зарплаты, а число людей с наиболее высокими доходами возросло всего на 500 тысяч. Бедность наступает и в Европе. Международная федерация обществ Красного креста и Красного полумесяца (IFRC) опубликовала в Риме и Женеве обзор «достижений» экономики, или, вернее, ее боссов. Согласно этому документу уровень жизни миллионов людей в Европе резко упал. В общей сложности 43 миллиона европейцев из-за уровня своих доходов не могут в достаточной степени прокормить себя самостоятельно и поэтому зависят от благотворительных суповых кухонь и пожертвований продуктов. В целом по сведениям Красного креста примерно 120 миллионов европейцев находятся непосредственно у черты бедности. Из собранной организациями в 42 странах информации следует, что за прошедшие три года количество людей, которым приходится получать еду от различных благотворительных организаций, в 22 странах Европы выросло примерно на 75%. К тому же цены за необходимые для существования товары и услуги выросли значительно сильнее, чем зарплаты тех, кто еще смог гарантировать себе рабочее место на все больше сокращающемся рынке рабочей силы.

Одновременно, при значительном притоке мигрантов из новых стран Евросоюза, в основном бывших социалистических стран и из-за пределов Евросоюза, значительно растут расходы на различного рода социальные пособия, включая выплаты, связные с безработицей, воспитанием детей, низким уровнем доходов и т.п. По оценкам европейских экономистов, при сохранении этой тенденции в ближайшие годы рост этих расходов не позволит ассигновать сколько-нибудь значительные средства на государственную поддержку высокотехнологичного сектора, научные исследования, повышение качества образования и здравоохранения. При нулевых

темпах экономического роста не только дальнейшее увеличение, но и сохранение на нынешнем уровне социальных пособий и льгот вследствие наращивания массы их получателей становится серьезной угрозой для среднего класса и будущего ключевых стран Евросоюза.

Второй угрозой является стремительное старение населения Евросоюза, а соответственно увеличивающаяся с каждым годом нагрузка на одного работающего для изыскания необходимых средств по выплате пенсий лицам, вышедшим из трудоспособного возраста. Расчеты, проведенные в последние год-два, как специалистами различных комиссий Евросоюза, так и независимыми экономистами показывают, что при сохранении нулевых, или даже незначительных темпов экономического роста, в силу отмеченных выше причин, социальное рыночное государство просто не имеет перспектив. Соответственно, не имеет перспектив и средний класс, который привык получать от государства различного рода социальные подушки безопасности, включая в значительной мере бесплатную медицину, образование, высокий уровень пособий по безработице и т.п.

Кто-то должен был сказать это вслух. И эта роль была поручена королю Нидерландов Виллему-Александру. Сделано это не случайно. Во-первых, правящая в Голландии Оранская династия теснейшим образом связана с правящими кругами и старой аристократией Германии, Италии, Великобритании. Во-вторых, Голландия входит в число стран-основательниц Евросоюза и принимает на своей территории ряд важных институтов и органов Сообщества. В-третьих, в культурном плане Голландия в равной степени связана с Францией, Германией и Великобританией. К тому же сам Виллем-Александр является одновременно самым молодым монархом в Европе и королем, который пользуется самой большой поддержкой своих подданных. В сентябре 2013 года Виллем-Александр обратился со специальным послани-

ем к народу Нидерландов по национальному телевидению, которое транслировалась всеми государственными телеканалами стран ЕС, и в котором он подытожил: «Социального государства XX века больше не существует. На его место приходит общество активного участия. В этом обществе люди должны взять ответственность за свое собственное будущее, заботиться о себе и создавать собственную социальную и финансовую безопасность с меньшей долей участия правительства. Это в первую очередь касается социального страхования и долгосрочного медицинского обеспечения. Эти реформы требуют времени и упорства».

Когда заходит речь об ухудшении имущественного положения среднего класса в США и в Европе, усилении неравенства в странах НАФТА и Евросоюза, лоббисты глобализации и сторонники либерального дискурса утверждают, что это временные трудности, которые происходят на фоне небывалого расцвета среднего класса в новых индустриальных странах и, прежде всего, в Китае.

Недавно консультант крупнейших американских банков и промышленных компаний Хелен Ванг опубликовала бестселлер «Китайская мечта: крупнейший мировой средний класс». По словам Ванг, в Китае проживает примерно 300 млн. человек, которых можно причислить к представителям среднего класса. Это примерно 25% от всего населения страны и почти 50% от всего городского населения.

Есть и другие оценки. В выполненном при участии китайского правительства докладе Азиатского банка развития, численность среднего класса в Китае обозначена в размере 820 млн. человек. Специалисты Азиатского банка развития в качестве критерия посчитали превышение расходов в расчете на одного человека двух долларов – в сельской местности, и пяти долларов – в городах.

Несложно посчитать, что и в первом, и во втором случае желаемое выдается за действительное. Мало

кто знает, но, например, автомобиль среднего класса китайской сборки от ведущих автоконцернов в Китае стоит дороже, чем в Европе и США. То же относится к качественной электронике, мебели, не говоря уже о стоимости соответствующего стандартам комфортности жилья. В Поднебесной все это дороже, чем в Европе и Америке. Гораздо более обоснованные критерии дают директор Института социальных наук Нанкинского университета Джоу Сяохун и один из крупнейших в России и в мире китаист Бронислав Виногродский. Они, независимо друг от друга, исходят из того, что стоимость жизни одного человека, относящегося к среднему классу в Пекине, составляет примерно 1000 долларов на человека в месяц с учетом покупательной способности юаня (доход среднего класса по районам Китая с учетом различий между городом и деревней определяется исходя из этой базисной цифры). При таких доходах можно примерно до половины средств тратить на приобретение электроники, предметов длительного пользования, отдыха, развлечений, путешествий и т.п. С оценками Джоу Сяохуна и Бронислава Виногродского солидарна крупнейшая консалтинговая фирма McKinsey & Co. Ее специалисты полагают, что в настоящее время большинство жителей Китая – работающие, живущие в домохозяйствах (в составе четырех человек) с чистым годовым доходом между 6000 и 16000 долларов, чего едва хватает на покрытие основных потребностей. Средний класс с чистым годовым доходом 16000 – 34000 долларов США составляет лишь 6% городского населения. Верхний средний класс и богатые потребители, чей чистых годовой доход превосходит 34000 долларов США, составляют всего 2% городского населения. ОЭСР определяет глобальный средний класс как те домохозяйства, которые могут позволить себе ежедневные траты от 10 до 100 долларов на члена семьи, с учётом паритета покупательской способности.

Что расширяет численность среднего класса в Китае до 10% от всего населения.

Как показывают обследования, подавляющая часть китайского среднего класса – это чиновники, топ-менеджеры, в первую очередь иностранных компаний, их филиалов и совместных предприятий, партийные функционеры, и, в небольшой части, высококвалифицированные инженеры, программисты и т.п.

Увеличение китайского среднего класса происходит на фоне усиления имущественной дифференциации, роста различий в доходах между экспортно-ориентированными южными регионами и центральным и северным Китаем, между жителями города и деревни.

Несмотря на несомненные успехи в борьбе с нищетой, уровень бедности в Китае остается весьма значительным. Согласно данным Государственного Совета КНР более 10% сельских домохозяйств имеют ежедневный доход менее 1 доллара. В нищете в Китае продолжают жить больше 150 млн. человек. При этом число богатых домохозяйств в Китае с доходом более 36,5 тыс. долларов в год превысило 40 млн. В них проживает более 150 млн. китайцев. На сегодняшний день в Китае 1,3 млн. долларовых миллионеров или примерно 0,1% от численности населения (это примерно соответствует уровню России, где число долларовых миллионеров составляет более 130 тыс. при 143 млн. населения). Что касается миллиардеров, то их в Китае сейчас 315 человек. Нельзя не подчеркнуть, что около 60% богатых китайцев с состоянием более одного миллиона долларов, согласно данным China Daily, хотели бы покинуть Китай и уехать в США, и в меньшей степени, в Европу. Одновременно они хотели бы вывезти свои капиталы. Кроме того, Китай вышел в последние годы на первое место в мире по объемам нелегального вывоза капитала из страны, и уровню теневого предпринимательства. Согласно результатам многочисленных обследований, 90% детей

этих богатых китайцев или уже учатся, или собираются учиться на Западе и родители не хотели бы их возвращения в Китай.

Таким образом, в Китае цена возрастания среднего класса формирования слоя новых богатых в ходе процессов глобализации оказывается весьма велика. Это отмечается и в последних решениях китайского руководства. В частности, решению указанных проблем будет посвящен предстоящий Пленум ЦК КПК.

Подводя итоги можно сделать вывод, что структурный кризис и макроэкономическая рецессия глобальной финансиализированной экономики, по сути, подрывают основополагающие принципы социального контракта, до поры примирявшего конфликтующие слои и группы населения во всех основных центрах мирового хозяйства.

Средний класс лишился имущественной стабильности, социально-экономического комфорта и жизненной уверенности. Он уменьшается в размерах, падает его экономическая роль, снижается стабилизирующий потенциал в рамках социально-экономических и политических структур современного мира.

Небогатые и бедные слои, не успевшие вкусить в достаточной степени плоды общества потребления и повышения уровня жизни, по сути, потеряли перспективы перехода в средний класс. Для них первостепенной задачей становится – не скатиться в экстремальную бедность. В решении этой задачи они во все возрастающей степени уповают на социальную помощь государства. Государство же, в противоположность этому, практически повсеместно старается сократить долю социальных расходов в государственных бюджетах.

Богатые, хотя и значительно увеличили свои доходы и нарастили собственность, крепко запомнили более чем 25-процентное падение стоимости имущества в период острой фазы кризиса. Большая часть верхних 10% отдает

себе отчет в виртуальном характере значительной части своего богатства, воплощенного в переоцененных акциях, сверхволотильных финансовых инструментах и малоликвидных в тяжелые годы недвижимости и различного рода коллекционного имущества.

Пока доволен и уверен только 1% и его элита, составляющая 0,01%. Но в условиях глубоких и комплексных технологических перемен, турбулентности макроэкономики, неустойчивости мировых финансов и чрезвычайно низких темпов или полного отсутствия роста экономики, господство элиты, расколотой внутри себя, оказывается под большим вопросом.

Все хуже работающие социальные лифты, практически повсеместное отчуждение общества и основных его слоев и групп от государства, растущий разрыв между социальными ожиданиями и экономическими возможностями ведут к исчерпанию возможностей социальной системы, базирующейся на кредитной экономике и потребительском консенсусе, со всеми вытекающими последствиями.

# Глава 7
# ЭЛИТНЫЙ ПАРАДОКС

К середине 2010-х годов сложилось парадоксальное положение. Профессиональные и социальные СМИ заполнены статьями о господствующих элитах. Телевидение и видеоканалы интернета постоянно транслируют сюжеты об одном проценте населения, который господствует над миром. В Соединенных Штатах и континентальной Европе выходит большое количество литературы об элитах. При этом основная часть подобных книг написана в жанре нон-фикшн и является не столько результатом глубоких аналитических исследований, сколько журналистским обобщением горячих, интересующих общественность, тем. Характерными примерами таких книг являются: «The Global Power Elite and the World They Are Making» Давида Роткопфа, «Plutocrats: The Rise of the New Global Super-Rich and the Fall of Everyone Else» Кристи Фриланд и им подобные.

Сложившееся положение резко контрастирует с ситуацией, существовавшей до второй половины 70-х годов. В тот период велась скрупулезная академическая работа, базирующаяся на обобщении огромного статистического материала по выявлению структуры и конкретного состава элитных групп. Параллельно осуществлялись глубокие исследования по теории элит, связанные с разработкой концептуальной базы элитного анализа. Именно к середине прошлого века сложились основные направления теории элит, разработанные Гаэтано Моска, Вильфредом Парето и Робертом Михельсом, а также Самуэлем Липсетом, Чарльзом Миллсом и др.

В конце 60-х – начале 70-х годов были написаны основные работы, где подводились итоги документального анализа финансово-экономических элит. Среди них следует выделить, прежде всего, книги «Богачи и сверхбогачи: о подлинных правителях Соединенных Штатов» Ф. Ландберга, «Сильные мира сего: бизнес и бизнесмены в американской истории» Б. Селигмена и «Властвующие элиты» Ч. Миллса и т.п., оперативно и качественно переведенные на русский язык и изданные в СССР.

Странность сложившегося в настоящее время положения с изучением элит усугубляется рядом дополнительных обстоятельств:

• во-первых, имеются и пополняются практически в режиме реального времени огромные массивы материалов, характеризующие собственников, управленцев, стейкхолдеров практически всех компаний, а также все существенные факты, касающиеся сколько-нибудь заметных субъектов экономической деятельности в подавляющем большинстве стран мира. Сегодня открыты огромные базы и архивы подобной информации, охватывающей все основные страны мира и отрасли экономики. Иными словами, для исследователей доступны просто необозримые «залежи» первичного, фактографического материала. Удивительно, что в настоящее время сделана лишь она попытка такого анализа, проведенная группой исследователей из Цюрихского технологического университета «The network of global corporate control» Stefania Vitali, James B. Glattfelder and Stefano Battiston. Работа имела оглушительный резонанс;

• во-вторых, сегодня в распоряжении исследователей имеется множество платных и бесплатных компьютерных программ, позволяющих работать с Большими Данными, вести детальный сетевой анализ, распутывать сложные клубки взаимосвязей, находить в массивах информации неочевидные закономерности, сведения о лицах, событиях, взаимосвязях и т.п. При наличии огром-

ных архивов цифровых СМИ, переведенных в цифровую форму практически по всем основным странам мира, это позволяет применить в полном объеме методы расследовательской аналитики и по наблюдаемым и фиксируемым фактам находить скрытые и скрываемые закономерности, связи и отношения;

• в-третьих, буквально в последний год частично в результате преднамеренных утечек, спровоцированных разведывательными органами, частично в результате целенаправленной работы налоговых органов и органов финансового контроля основных стран мира, по сути, канула в лету банковская тайна и анонимность оффшорного и трастового владения. На волне разоблачений появились даже специализированные компьютерные сервисы, позволяющие отыскать скрываемые оффшорные компании у известных легальных юридических и физических лиц. С учетом того, что элитные группы активнейшим образом использовали оффшорные убежища, такое изменение ситуации резко повысило возможность реального анализа структуры финансово-экономических групп.

Однако, несмотря на единичные работы, по сути, документированных исследований структуры финансово-экономической элиты основных стран мира вот уже в течение более чем 15 лет не опубликовано в виде монографий, открытых докладов и т.п. В поисках ответа на этот вопрос автор статьи обратилась к одному из наиболее авторитетных и известных специалистов в области анализа элит, автору многократно переиздававшейся книги «Who Rules America Now?» профессору Уильяму Домхоффу. Господин Домхофф подтвердил, что, действительно, с начала века в Соединенных Штатах не вышло ни одной обобщающей работы по структуре финансово-экономической элиты США, где были бы подробно рассмотрены ее основные группы и связи между ними. Основную причину сложившегося положения профессор видит в том, что эта тема уже длительное вре-

мя не поддерживается грантами, которые являются в Соединенных Штатах основным инструментом научной деятельности. При этом можно предположить, что, тем не менее, такие исследования в Соединенных Штатах, Европе, Китае ведутся, но их результаты засекречиваются корпорациями или близкими к разведывательно-промышленному комплексу «думающими танками», которые их осуществляют.

К сожалению, весьма плачевная ситуация относительно документального анализа западных элит сложилась и в России. Между тем, востребованность темы возрастает, что называется не по дням, а по часам. Этому способствует целый ряд обстоятельств.

Прежде всего, вот уже длительное время происходят интенсивные процессы своеобразной приватизации ведущих западных государств. Этот процесс выражает себя в частности в том, что публичные представительные структуры власти все больше становятся лишь внешними формами по отношению к реальным структурам господства и принятия решения. Соответственно, для того, чтобы максимально эффективно взаимодействовать и противоборствовать с теми или иными акторами на политической арене надо точно понимать структуру финансово-экономической элиты и тенденции ее изменения. Кроме того, непростая, все более усложняющаяся геополитическая обстановка в мире предполагает максимальное использование несовпадения интересов различных элитных групп, а также выстраивание отношения с теми из них, чьи текущие или перспективные задачи совпадают с российскими интересами.

Справедливость оценки уровня исследований финансово-экономических элит как неудовлетворительного не сложно продемонстрировать на примере двух имеющих наиболее широкое хождение в экспертном сообществе подходов к структурированию элит.

Как это ни удивительно, немалая часть экспертного сообщества, например, В. Катасонов и В. Павленко продолжают сводить элитные противоречия к борьбе так называемых кланов Рокфеллеров и Ротшильдов. При этом, хотя подобные тексты претендуют на принадлежность не к публицистике, а к науке, в их подтверждение не приводится ни одного доказательства. Оно и понятно. Таких доказательств просто не существует в документированном виде. Что же касается ссылок на частные разговоры и недокументированные источники, подобная непроверяемая аргументация лежит за пределами науки и серьезной аналитики.

Другой популярный в экспертном сообществе подход был предложен известным колумнистом, спикером и исследователем М. Хазиным. В статьях, написанных в 2013 году, он высказал гипотезу раскола элит на три составных части, а именно: так называемых «менял», «процентщиков» и «региональных процентщиков». Анализ публикаций, где изложена подобная позиция, позволяет сделать вывод о том, что менялы от процентщиков отличаются источником дохода финансовых институтов, находящихся под контролем соответствующих групп. В случае менял эти доходы связаны с извлечением прибыли из валютных и финансовых рынков. В случае процентщиков главные источники прибыли лежат в традиционном кредитовании и близости к источникам эмиссии – ФРС и проч.

Принципиально исследователь может строить любые классификации, которые помогают изучать реальные экономические процессы, и задают своего рода исследовательскую картину мира. Однако представляется, что в данном случае такая классификация скорее затемняет, чем проясняет экономические процессы. Поскольку предложенная классификация претендует на анализ финансовой элиты, то естественным будет рассмотрение балансов основных банков. Благо, что таковых немного.

Нельзя не согласиться с названием мирового экономического бестселлера «13 банков, которые правят миром» Саймона Джонсона, Джеймса Квака. Даже если анализ расширить с 13 банков до 29 основных финансовых институтов планеты, найденных исследователями из Цюрихского технологического университета в упомянутом выше исследовании, то обнаружится, что серьезных расхождений в структуре балансов, позволяющих группировать эти институты на указанные группы, в реальности не существует. Доходные части балансов основных мировых банков весьма схожи между собой.

В то же время подход М. Хазина имеет определенный смысл, если перенести его из финансово-экономической сферы в политическую. Под таким углом зрения процентщики превратятся в политические элиты, делающие ставку на глобализацию, ориентированную не на какие-то конкретные страны, а, на мировое хозяйство и политическую структуру в целом. Менялы в этом смысле превращаются в часть элиты стран, так называемых региональных лидеров. Целью этих элитных групп становится поворот процессов глобализации вспять и членение единого мира на несколько зон, в которых может быть реализована автаркия, т.е. замкнутость зоны на саму себя при минимуме внешней торговли. И, наконец, региональные процентщики – это имперская политическая элита США, ставящая на глобальное и единоличное лидерство США в мире, либо поделенном на зоны, либо представляющим единое целое. Само по себе такое членение достаточно любопытно, однако не может выступить в качестве базисного. Ведь базисом, в конечном счете, всегда выступают технологии, организационные и финансово-экономические отношения, а не политические предпочтения.

В то же время, как показывает практика, наиболее эффективным способом осуществления исследовательских программ является, как убедительно доказал про-

фессор А. Брушлинский, является метод анализа через синтез. А синтез, как справедливо отмечает Ю. Овчинников в своей пионерной работе «О природе случайности», обязательно предполагает наличие концептуальной схемы, которая имеется у исследователя еще до анализа эмпирического материала. Указанная схема помогает организовать эмпирический материал и в ходе исследования либо находит свое подтверждение, либо должна быть отброшена как не отвечающая фактологической картине мира.

Чтобы сформировать предварительную гипотезу относительно структуры основных элитных групп необходимо опереться на наиболее сильные, действительно привносящие новое в элитный анализ, работы, вышедшие в последнее время. Речь идет в первую очередь о цикле работ знаменитого социолога М. Манна о сетях власти «The Sources of Social Power: Volume 1-4» и работах А. Фурсова «Колокола истории» и «Глобальные игроки – за исключением Китая – не государства, а устойчивые сетевые структуры». Также нельзя не включить в этот ряд работу профессора Принстонского университета М. Гиленса «Testing Theories of American Politics: Elites, Interest Groups and Average Citizens», и исследование С. Витали, Дж. Гладфелдера и С. Биттистона «The network of global corporate control». Краткая выжимка из этой работы под названием «147 корпораций, которые контролируют мир» была перепечатана всеми ведущими научными и популярными электронными и бумажными изданиями во всех странах мира, в том числе и в России.

Между тем, несмотря на всю сенсационность исследования, оно отражает лишь часть картины. Более того, в определенной степени его результаты показывают весьма искаженную картину. Дело в том, что, как эмпирически показал Э. Маршалл из Института Хэмптона, и неопровержимо математически доказал российский математик В. Подиновский, элиты, даже в условиях су-

ществования сети перекрестного владения акциями не представляют собой однородной системы.

Для выделения крупных структурных блоков в сложной системе мировых элит лучше всего подходит, по нашему мнению, критерий деятельности элитных групп. Именно деятельность определяет, какие технологии и ресурсы используются, какова структура активов и пассивов элит, на какие политэкономические отношения и функции они опираются, в чем особенности их взаимосвязи с другими элитными группами и слоями общества и т.п.

В современном глобальном мире потребительского финансизма по критерию деятельности четко выделяются три элитных группы. Естественно, что такое выделение не абсолютно, группы переплетаются между собой, имеют зачастую общих представителей в структурах политической власти и т.п. Однако, при этом, способ их существования, экономические интересы, механизмы политического доминирования и т.п. существенно различаются.

Первая группа – это, несомненно, хозяева сегодняшнего мира, финансисты, или, как их недружелюбно называют в СМИ – банкстеры. Они являются не только в значительной мере хозяевами эмиссионных центров, но и получают и контролируют львиную долю доходов глобальной экономики. Например, в Соединенных Штатах доля прибыли финансового сектора в общем объеме выросла с 10% до Второй мировой войны до более чем 50% в настоящее время. Полное господство финансистов окончательно установилось с перестройкой в Советском Союзе, и многократно упрочилось после его распада.

Вторая группа – это транснациональные компании традиционных отраслей экономики, порожденные второй производственной революцией, а также международные торговые компании. Эту группу еще часто называют корпоратократией. Ее расцвет приходится на годы

«холодной войны» с СССР, а конкретно со второй половины 50-х годов прошлого века до краха СССР в 1991 году. В последние 15-20 лет она перестала выступать конкурентом финансистов в борьбе элит и превратилась, по сути, в подчиненную им группу. Это, в частности, наглядно продемонстрировало упомянутое выше исследование «The network of global corporate control». В условиях перманентного снижения темпов экономического роста на протяжении последних десятилетий, падения нормы прибыли и действия мощных механизмов перераспределения прибылей, доходов и инвестиций из реального сектора в финансовую систему, у этого сектора фактически оказались исчерпаны внутренние драйверы и ресурсы развития. Его существование оказалось подчинено и с точки зрения формирования инвестиций, и с позиций владения капиталом, и по критерию обеспечения спроса на продукцию, финансовой элите глобального мира.

В последние 40 лет происходило постепенное формирование третьей группы мировой элиты, связанной с высокими технологиями, а в будущем, с разворачивающейся Третей производственной революцией. Фактором формирования третьей группы элиты стала «холодная война» между СССР и США – своеобразное преддверие Третьей производственной революции. Именно в тот период государства стали вкладывать огромные ресурсы в научные исследования и новые производственные технологии, которые могли использоваться как в военном, так и в гражданском секторах экономики. Например, в США, Европе и Японии именно государства сформировали высокотехнологичные сегменты, создали механизмы их финансирования, а также обеспечили трансферт технологии из государственного сектора в частный для их коммерциализации и использования для производства товаров и услуг в секторе конечного потребления домохозяйствами.

Об этом убедительно свидетельствуют написанные на основе обобщения огромных массивов достоверных эмпирических данных книги М. Маззукато «The Entrepreneurial State: Debunking Public vs. Private Sector Myths (Anthem Other Canon Economics)» и Ф. Блок, М. Келлер «State of Innovation: The U.S. Government's Role in Technology Development». Именно государство создало, по сути, Силиконовую долину, обеспечило стартовый капитал венчурных фондов, дало заказы университетам, сформировало устойчивые производственные программы гигантам американской высокотехнологичной индустрии. Американские высокотехнологичные компании в сфере информационных технологий, робототехники, биотехнологий и т.п. являются исходно в значительной мере порождением военно-разведывательного комплекса. В этом смысле третью группу элит можно назвать «силовиками», памятуя о знаменитом выражении Френсиса Бэкона «Знание – сила». Другое название для этой группы предложил известный криптограф, один из бывших руководителей компании Apple, отставной сотрудник АНБ Д. Райс в своей книге «Geekonomics». Он предложил называть эту третью группу «гикономиксами».

Однако, для того, чтобы вникнуть в ситуацию с сегодняшними элитами, недостаточно просто классифицировать их по принципу деятельности. Существует еще как минимум три тонких момента, без рассмотрения которых невозможно сколько-нибудь адекватно понять внутриэлитные процессы и соответственно отношения элит к новым процессам и явлениям, типа третьей производственной революции, слому Вестфальской мировой системы, деривативам, Биткойнам и т.п.

Прежде всего, нельзя не отметить происходящую в значительной части мира трансформацию государства, как важнейшего института человеческого общества. Среди самых разнообразных процессов в этой сфере типологически можно выделить три. Во-первых, все шире

происходит передача государственных функций на аутсорсинг частным компаниям. Например, число частных подрядчиков американского разведывательного сообщества перевалило за тысячу компаний. Во-вторых, все шире происходит своеобразная приватизация государства и отдельных его институтов, используемых как активы частными группами и группами влияния. Одним из примеров такой приватизации является деятельность ФРС, которая по законодательству выполняет функции государственного агентства Соединенных Штатов. Хорошо известно, как в разгар кризиса частным банкам было передано на длительный сроки беспроцентных кредитов на более чем 3 трлн. долларов. Наконец, в-третьих, все шире происходит передача функций от государства, где ключевую роль играет пусть декларируемая, но все-таки по факту представительная власть, к различного рода надгосударственным, никем, по сути, не контролируемым структурам, где все решают неподотчетные чиновники. Такие претензии предъявляются к формируемым в настоящее время Трансатлантическому инвестиционному и торговому партнерству и Транстихоокеанскому торговому партнерству. При ослаблении по факту роли представительного государства, увеличивается господство крупнейших компаний, корпораций, банков, а также неформальных групп и других образований самой разнообразной конфигурации.

Вторым аспектом, который нельзя не принимать во внимание, является все большее расхождение интересов различного рода институтов и организаций с одной стороны и действующих внутри них групп – с другой. В 80-х годах прошлого века А. Лазарчук и П. Лелик опубликовали эссе «Голем хочет жить». В нем они впервые показали, что крупные организации типа министерств, разведывательных агентств, транснациональных корпораций и т.п. демонстрируют квазиразумное поведение. Развивая идеи Р. Акоффа, они показали, что такие ор-

ганизации имеют собственные цели, которые могут не полностью совпадать с законодательными или другим образом нормативно установленными функциями. Причем, это целенаправленное поведение осуществляется в каком-то смысле независимо от конкретных лиц, возглавляющих указанные организации, и в большей мере определяется сложившимися внутренними процедурами и технологиями, а также различного рода неформальными правилам и ценностями, присущими конкретной организации или институту. В последующем эта гипотеза получила многочисленные эмпирические подтверждения на материалах самых различных стран мира. Такой подход хорошо объясняет известные всем факты, когда вновь назначенные руководители организации не могут изменить характер ее деятельности.

Уже в этом веке на Западе Дж. Ходжсон и Т. Кнудсен, а в России М. Мусин установили, что внутри крупных организаций с неизбежностью появляются группы с собственными интересами. При этом, чем больше организация, и чем строже в ней соблюдается внутренний режим секретности, тем с большей вероятностью эти группы могут конкурировать между собой, даже не зная о существовании друг друга. Каждая из указанных групп старается использовать квазиразумное поведение организации в собственных интересах.

Наконец, третий аспект связан с необходимостью демифологизации элитного анализа. Длительное время господствовало понимание элит как малоподвижных иерархий, в которых несколько групп ведут непримиримую борьбу между собой. Причем, как правило, эти иерархии относятся к числу жестких структур и существуют в неизменности длительное время, превышающее жизненные циклы нескольких поколений. Именно на данной посылке долгие годы было построено большинство работ по анализу элит.

Поскольку в условиях перехода после завершения «холодной войны» мировой системы в высокодинамичную, турбулентную фазу своего существования перестали обнаруживаться данные, подтверждающие наличие жестких иерархий, как основного принципа организации элит, то на их место пришла так называемая сетевая модель. Отношения внутри элит стали трактоваться как сети со всеми вытекающими из этого последствиями. С развитием интернета такая модель стала абсолютно господствующей. Из нее исходит подавляющее большинство современных исследований элит.

Комбинация указанных выше трех обстоятельств привела к появлению принципиально нового подхода. Суть его – в констатации необратимого упадка элит всех типов, и перехода власти к децентрализованным малоконтролируемым сетям, типа Аль-Каиды или группы активистов Дж. Ассанжа. Наиболее ярко этот подход выражен в международном политическом бестселлере 2013 года, книге М. Наима «End of Power». Ее главный тезис состоит в том, что власть теперь легко «взять», но она оказывается бессильной. Реальное господство перестало быть сосредоточено в руках элит, а оказалось как бы распределенным, «размазанным» по множеству слабосильных, и эффективных лишь на короткое время сетевых структур.

Однако представляется, что говорить о конце власти преждевременно. В случае элит действует универсальный принцип: в реальности все происходит не так, как кажется на первый взгляд. Еще в 30-40 годы прошлого века российско-германский биолог Н. Тимофеев-Ресовский установил, что наиболее успешно адаптируются к быстроизменяющейся ситуации те живые организмы, в которых наиболее четко проявляется блочный принцип организации. Если переводить это на привычный язык, то речь идет о иерархо-сетевых структурах. В 1945 году американский математик и биофизик У. Маккалок раз-

работал знаменитые нейронные сети, которые сегодня лежат в основе интеллектуального анализа Больших Данных. Занимаясь вопросами нейронных сетей, он вывел принцип организации живых организмов, который получил название гетерархии. В 2009 году профессор Корнуэльского университета Д. Старк выпустил книгу «The Sense of Dissonance: Accounts of Worth in Economic Life». Он обнаружил, что гетерархия является организующим принципом не только для живых организмов, но и в хозяйственной деятельности.

Мы полагаем, что этот же принцип лежит в основе формирования и функционирования современных элит. Гетерархия – это сложная адаптивная система, включающая сильные устойчивые сетевые (горизонтальные) связи и пластичные, динамичные организующие иерархии (вертикальные связи), чей конкретный состав зависит от внутренних факторов и изменений внешней среды. Т.е. в основе любой элиты лежат сетевые взаимодействия, обусловленные общим характером деятельности. Но в рамках этих сетевых связей образуются различные обособленные группы. Эти группы в зависимости от ситуации выстраиваются в иерархии, т.е. отношения господства-подчинения, которые и организуют эти самые гетерархии, обеспечивают их существование в мире. В качестве метафоры гетерархии можно предложить группу велогонщиков, которая уходит в отрыв от основного пелетона. По сути, все участники группы равны, но в зависимости от тактики всей группы, наличии сил у каждого из ее участников и других факторов, тот или иной участник группы отрыва берет на себя функцию лидера и старается, чтобы отрыв группы от пелетона не сокращался, а возрастал.

Современные элиты организованы по принципу гетерархии. Есть гетерархии финансистов, корпоратократов, силовиков или гикономиксов, в которых внутреннее сотрудничество сопровождается постоянной конкурен-

цией и переменчивым балансом сил внутри гетерархии в зависимости от изменения внешней среды и внутренних обстоятельств.

Важнейшей характеристикой всех элитных групп является их наднациональный характер. Наднациональные иерархо-сетевые структуры правящих элит сложились еще в последней четверти XIX и начале XX веков в период первой глобализации. С тех пор лишь менялись их конфигурация, иерархия, соподчиненность и состав групп. При этом мировая элита, т.е. правящий класс, слой никогда не была единой. Более того, она практически никогда в последнем столетии не делилась жестко по странам и регионам. Уже давно география осталась для школы, а в жизни стала господствовать метаполитика. Мета по-латыни означает «сверх». Когда мы говорим о метаполитике, то строго говоря, рассматриваем единство политики, экономики и культуры, реализуемые через власть.

Обычно складывание наднациональных групп мировой элиты относят к гораздо более позднему времени – к концу 60-х – началу 70-х гг. XX века, когда западная корпоратократия и фининтерн, или банкстеры наладили контакты с частью верхушки советской номенклатуры. Однако такая позиция является явным упрощением.

Давайте пристальнее присмотримся к периоду, когда, казалось бы, ни о каких наднациональных элитах речи идти не могло. А именно, времени, когда Советский Союз, возглавляемый И.В. Сталиным, находился в непримиримом противостоянии с капиталистическими странами.

Однако в этом случае придется ответить на один неудобный вопрос. А именно, об индустриализации СССР. Как это ни удивительно, ни в Советском Союзе, ни в современной России не издано ни одной монографии об участии Запада в сталинской индустриализации. Не слишком много таких работ и на Западе. К числу ред-

ких исключений, в частности, относится трехтомник Энтони Саттона «Western Technology and Soviet Economic Development».

А, между тем, материала на эту тему более чем достаточно. Сам И.В. Сталин никогда не скрывал роль сначала Германии, а затем США в советской индустриализации. Он, например, отмечал, что: «Мы многим обязаны Генри Форду. Он помогал нам строить автомобильные заводы... Советские люди многому научились у американцев. Американский опыт был использован при создании советской промышленности». Без участия американских и европейских фирм не появились бы в считанные годы ДнепроГЭС, Магнитогорский металлургический комбинат, Нижегородский автозавод, химическая, авиационная, электротехническая промышленность, военно-промышленный комплекс. 90% наиболее крупных объектов индустриализации были сооружены с участием американцев, как в части поставок комплектного оборудования (что называется, «завод под ключ»), так и собственно проектирования, организации строительства и т.п. Часто говорят о том, что на самом деле эти поставки были более выгодны для Запада, поскольку там был экономический кризис, так называемая «Великая депрессия», а Советский Союз представлял едва ли не единственную динамично развивающуюся страну. Но опять же в этом утверждении имеется очень большая доля лукавства. Весьма значительная, а в отдельные годы и преобладающая доля затрат, связанных с закупкой оборудования и оплатой проектов предприятий покрывалась за счет корпоративных и государственных западных долгосрочных кредитов. В 20-е гг. – прежде всего, из Германии, а в 30-е – из США и Британии.

Кстати, неслучайно, что еще в середине 20-х гг. Рокфеллеры активно пришли в Россию и реконструировали закавказские нефтепромыслы, нефтепроводы и танкерные стоянки. В то же время Ротшильды, через нефтяную

компанию Royal Dutch Shell, во главе с тогдашним ее руководителем Детеррингом, активно финансировали не только антисоветское белое подполье, но и троцкистскую оппозицию. Все это позволяет говорить о том, что даже в сталинские времена речь шла в каком-то смысле об наднациональных группах элит. В некоторой степени советская индустриализация была сознательным ответом западных корпоратократов на удар, нанесенный им еще в начале XX века принятым по инициативе банкиров антитрестовским законодательством, направленным в первую очередь против промышленников и последовавшим за созданием в 1913 г. Федеральной Резервной Системой США, выходом на первые роли финансистов.

Бытует мнение, что единственной национальной элитой в сегодняшнем мире является китайская элита. Однако и здесь все не так просто. Когда в 1971 г. Генри Киссинджер прилетел в Пекин восстанавливать политические, экономические и даже секретные военные отношения между США и Китаем, то по свидетельству одного из его близких советников, они с удивлением обнаружили в ближайшем окружении китайского руководства и, прежде всего, Чжоу Эньлая, британских советников. Кстати, и все нынешнее китайское экономическое чудо начиналось со свободных экономических зон в прибрежных южных районах Китая. В них и по сей день сосредоточена основная часть китайского промышленного потенциала.

Главным источником финансирования и трансферта технологий в свободные экономические зоны был Гонконг, ныне часть Китая с особым статусом, а тогда одна из последних британских колоний, управляемых генерал-губернатором. Но гораздо более важным являлось то, что Гонконг был не просто британской колонией, а подлинным форпостом, своего рода бастионом лондонского Сити в Азии. Именно в Гонконге были открыты филиалы всех крупнейших британских банков, а также основаны

собственно гонконгские банки, преимущественно с британским и, частично, голландским капиталом.

В конце 60-х гг. прошлого века под флагом теории конвергенции, т.е. сближения капитализма и социализма, часть российской номенклатуры пыталась влиться в мировую корпоратократию. Она полагала, что игра идет на равных, и в итоге ей удастся успешно интегрироваться в мировую корпоратократическую группу элиты в качестве равного полноправного партнера. Однако, как мы знаем, на деле получилось по-другому. Ирония истории заключалась в том, что от краха Советского Союза не слишком выиграли и западные корпоратократы. Если в годы холодной войны, с ее гонкой вооружений, борьбой за страны третьего мира, экономическим соревнованием двух систем, фининтерн был вынужден делить власть и партнерствовать с корпоратократами, то с крушением Советского Союза ситуация коренным образом изменилась.

Корпоратократы, которые исторически представляли собой стейкхолдеров, основных акционеров и верхушку топ-менеджмента в транснациональных промышленных, логистических и других корпорациях реального сектора экономики, оказались фактически в полном подчинении у финансистов. Достаточно внимательно проанализировать статистику, характеризующую основные показатели динамики западных стран и, особенно, Соединенных Штатов Америки, чтобы убедиться, что фактически с начала 90-х гг. мы имеем совершенно иной строй, нежели тот, который существовал до крушения Советского Союза.

Если говорить грубо, то можно сказать, что капитализм перешел в стадию финансизма. В этой стадии финансы окончательно перестали обслуживать экономику. Они превратились в самодостаточный, более того, главный сектор мирового хозяйства. Именно в 90-е гг. были отменены практически все ограничения на банковскую

деятельность, появились новые спекулятивные рынки капитала, родились деривативы. Начиная с этого же периода весь мир охватило безудержное потребительство, или, как говорят, консьюмеризация, означающая жизнь в кредит. Фактически суть финансизма можно выразить всего-навсего в трех цифрах. Вся мировая реальная экономика, включая в том числе и необыкновенно разросшуюся сферу услуг, сегодня составляет в год примерно 80 трлн. долларов. Мировой финансовый рынок в год оценивается примерно в 800 трлн. долларов, а с учетом деривативов – более чем в квадриллион. Таким образом, на реальную экономику приходится в лучшем случае не более 10% мирового денежного оборота.

Но вернемся от истории к реалиям сегодняшнего дня. Фактически в мировой наднациональной элите сложились три очевидных и хорошо распознаваемых группы.

Первая из них – это финансисты, фининтерн, или банкстеры. Господствующую позицию в этой группе занимают крупнейшие мировые банки, от которых в решающей степени зависит вся мировая экономика, прежде всего банки Лондонского Сити и Нью-Йоркской Уолл-стрит. Они в значительной степени контролируют Федеральную Резервную Систему США и Банк Англии. С ними вынужденные считаться Европейский Центральный Банк, национальные банки Японии и Швейцарии. Конечно, в состав финансовой элиты входят не только сами по себе крупнейшие банки, но и банки помельче, а также связанные с ними хедж-фонды, страховые компании, инвестиционные фонды и т.п.

Главной характеристикой этой части мировой элиты является то, что она способна наращивать капитал и делать деньги из воздуха практически в прямом смысле слова. До сих пор неизвестно, кто, в конечном счете, контролирует ФРС. Зато хорошо известно, кто получает триллионные кредиты на многие годы под 0,25% годо-

вых. Вот получатели этих по сути бесплатных, бесконечно пролонгируемых кредитов, которые и кредитами назвать трудно, и являются хозяевами сегодняшнего мира.

С 70-х гг. прошлого века фактически составной, хотя и наиболее слабой, подчиненной частью финансовой элиты стала элита нефтяников и газовиков. Доллар не смог бы выжить как мировая валюта, если бы с конца 60-х гг. прошлого века все расчеты по нефти и энергетическим ресурсам в целом не осуществлялись бы исключительно в долларах. В этом смысле крах Советского Союза, одной из крупнейших, если не крупнейшей энергодобывающей державы мира, являлся обязательным условием выживания доллара, как главной мировой валюты и условием установления абсолютного доминирования фининтерна в мировом правящем классе. А соответственно и торжества финансизма, как нового глобального общественного строя.

Вторая – некогда равная по силам фининтерну, а теперь явно подчиненная группа мировой элиты, корпоратократия. В сегодняшнем мире к ней относятся топменеджеры и ключевые акционеры транснациональных монополий, нефинансовых и невысокотехнологичных секторов мировой экономики. Другой составляющей корпоратократии является высший уровень мирового чиновничества, особенно, наднациональных государственных, финансовых, экономических структур, типа МВФ, Всемирного Банка, структур Европейского Союза и т.п. По сути, корпоратократы являются той частью мировой элиты, которая контролирует традиционную производящую экономику. Т.е. то, чем люди и компании пользуются каждый день, начиная от производства поездов и автомобилей и заканчивая одеждой и бытовой техникой.

Третья часть мировой элиты начала складываться еще в 70-80-е гг., но в полный голос заявила о себе и своих претензиях на лидерство уже после кризиса 2008 г.

Она сложилась в первую очередь вокруг ведущих университетов таких стран, как США, Япония, Великобритания, Франция и др. Ведущие университеты мира, в отличие от российских учебных заведений, давно представляют собой не просто образовательные центры, а исследовательско- производственно- кадрово-коммерческие структуры с миллиардными оборотами. Именно здесь впервые появились и были доведены до коммерческого уровня все основные информационные технологии, позволившие осуществить интернет-революцию. Но информационными технологиями дело не исчерпывается. Здесь же уже долгие годы ведутся успешные исследования в сферах биотехнологий, поведенческих наук, разработки принципиально новых видов материалов и методов их обработки, роботизации и т.п.

На базе университетов появилась новая экономика, которая изначально подпитывалась не банковскими деньгами, а дотациями государств, так называемым рисковым, или венчурным капиталом и механизмами коммерциализации интеллектуальной собственности через фондовый рынок. Естественно, что эта экономика в первую очередь была связана с военно-разведывательным сегментом власти. Именно военные и разведка выступали основными заказчиками, а соответственно и своего рода спонсорами новой экономики.

Нельзя не отметить, что этот сектор сложился в немалой степени под воздействием опыта Советского Союза, где роль университетов выполняли крупнейшие научно-исследовательские институты, успешно работавшие буквально до последних дней существования Советского Союза по означенным выше направлениям. Американцы это и не скрывают. Нынешний главный советник Б. Обамы по науке Дж. Холдрен недавно сказал, что передовая американская наука и индустрия в значительной степени появились на свет благодаря масштабным инициативам Джона Кеннеди, который прямо в своих речах говорил о

том, что Америка должна ответить на технологический и научный вызов Советов.

Сегодня можно говорить, что ранее разрозненные исследовательские и коммерческие кластеры, относящиеся к различным сегментам новых технологий, а также властные, и прежде всего военные и разведывательные структуры, срослись в единое целое, организованное на иерархо-сетевой основе и ставшее отдельной обособленной и в значительной мере независимой частью мировой элиты. Вслед за шведскими исследователями Зондерквистом и Бердом, многие их называют нетократами. Другие – гикономиксами. На наш взгляд, исходя из отечественных традиций, их можно назвать «силовиками». С одной стороны такое название прямо отсылает к знаменитому высказыванию Ф. Бэкона: «Знание – сила», а с другой, подчеркивает, что главной организующей и финансирующей силой этой группы были военно-промышленный комплекс и разведывательные сообщества разных стран.

Почему именно сегодня разгорелась схватка между финансистами, или как их еще называют, банкстерами, и силовиками, при участии корпоратократов на той и другой стороне?

Подавляющее большинство аналитиков считает, что единственный шанс для Соединенных Штатов, Японии и, в значительной мере, Западной Европы выйти из кризиса, состоит в том, чтобы сделать упор на новую экономику, осуществить в широких масштабах третью производственную революцию.

В начале этого года MTI, RAND, Токийский университет и Европейский Центр оценки технологий выпустили доклад «Технологическое развитие 2025». Они предложили заменить наименование NBIC на NIBEP (neyrosciens, information technology, bio-technology, energy revolution, production. Новая производственная революция базиру-

ется на робототехнике, 3D-печати, композиционных материалах и т.п.).

В докладе сделан вывод, что существуют 24 критические технологии. Те, кто обладает всеми этими технологиями смогут осуществить новую технологическую революцию, запустить новую экономику. Согласно докладу у американцев есть готовые 21 технология, у японцев – 17, у Европейского Сообщества – 14, у Израиля – 9, у Южной Кореи – 8, у Китая – 7. И 4 – у России.

Наиболее авторитетные «фабрики мысли» приходят к выводу, что выживание американского, японского и западноевропейского социумов в решающей степени зависит от того, удастся ли им запустить на полные обороты новую экономику, или нет. Соответственно, запуск новой экономики предусматривает несомненное доминирование гикономиксов, или силовиков, и той части корпоратократов, которая сумеет приспособиться к новым реалиям.

Как отмечают практически все исследователи новой экономики финансовая система, в том виде, в котором она существует без малого три века, оказывается просто ненужной. Банкстеры, располагая огромными ресурсами, и естественно, квалифицированными мозговыми трестами, прекрасно понимают тенденции развития технологий и отдают себе отчет в тех коренных изменениях в балансе мировых элит, которые эти технологии с собой принесут. Поэтому фининтерн не остановится ни перед чем, чтобы не допустить утраты своего доминирующего положения в наднациональной элите, включая организацию рукотворного нового экономического кризиса, или даже большой, но не тотальной войны. Банкстеры сегодня находятся в ситуации, когда отступать им просто некуда.

Борьба между различными частями элит ведется сегодня практически во всех сферах – и в сфере технологий, и в экономике, и в политике, и в культуре. Чаще всего она

происходит «под ковром», невидимо, и остается малозаметной, а главное, совершенно недокументированной для сторонних, не входящих в элиту наблюдателей. Однако, в последнее время, борьба достигла такого накала, что все чаще выплескивается на поверхность. Лучшие примеры это – непрерывные утечки по оффшорам, эпопея Дж. Ассанжа, дело Э. Сноудена, расследование картельных сговоров крупнейших банков на всех основных финансовых рынках – от ставок кредитования до рынков нефти и металлов и т.п.

Борьбу банкстеров и традиционных корпоратократов с одной стороны, и гикономиксов в связке с наиболее продвинутыми в технологичном плане корпоратократами – с другой, очень часто сводят к борьбе между технологическими укладами. Т.е. грубо говоря, между старыми технологиями индустриальной эпохи и новыми технологиями постиндустриальной производственной экономики. Однако, представляется, что дело здесь гораздо глубже. По сути, мы стоим на пороге такого же переворота в жизни всего человечества, какой произошел в результате промышленной революции конца XVIII – начала XIX веков. Возможно, речь идет еще о более масштабном сдвиге, сравнимом с неолитической революцией. Некоторые, например, один из руководителей Google Эрик Шмидт говорит даже о возможности изменения в антропологическом типе человека. И принципиально важно, чтобы Россия не просто нашла свое место в этом процессе, но и выступила одним из лидеров. Этому способствуют многие обстоятельства нашей давней и совсем недавней истории, а также события, происходящие в настоящее время.

# Глава 8
# РУССКОЕ ЧУДО XXI ВЕКА

## 8.1. Украденное чудо

Более 50 лет назад, в июне 1963 года в Кремлевском Дворце съездов состоялась премьера фильма, на которой присутствовало не только руководство Советского Союза, но и весь дипломатический корпус. Это был двухсерийный художественно-документальный фильм «Русское чудо», снятый кинематографистами уже не существующей теперь страны – ГДР – о другой, канувшей в Лету стране – СССР. Съемки фильма были приурочены к запуску первого советского спутника, а завершились после полета Юрия Гагарина в космос. Как раз в этот период Джон Кеннеди произнес свою хрестоматийную фразу: «Если не хотите учить русский, учите физику».

Фильм рассказывал о том, как страна с разрушенной до основания экономикой и инфраструктурой, лишившаяся каких-либо технологий и организационной культуры, поголовно безграмотная, погрязшая в идеологических словопрениях и политических дрязгах, за короткий срок превратилась не только в мощную индустриальную и военную державу, одержавшую победу в Великой Отечественной войне, но и успешно соревнующуюся за мировое господство с Соединенными Штатами Америки.

Как это ни кажется сегодня удивительным, если открыть подшивки ведущих западных газет того времени, книги крупных экономистов и политологов, отнюдь не просоветски, а скорее антикоммунистически настроенных, в них обсуждался лишь один вопрос. И заключался он не в том, победит ли СССР в соревновании двух систем Соединенные Штаты Америки, а в том, за какой период

времени это конкретно случится. Это не преувеличение, а проверяемый факт. Благо сегодня, во времена интернета, оцифровано вся бумажная пресса, начиная с XVIII века.

История рассудила по-другому. Сегодня в силу конъюнктурных соображений можно рассказывать сказки о том, как агенты вражеских разведок развалили Советский Союз и привели его к гибели. Это злостная и вредная неправда. Причины крупнейшей геополитической и человеческой катастрофы эпохи лежали главным образом внутри самого Советского Союза. Они были связаны с безграмотностью и эгоизмом его партийно-хозяйственной элиты. Деятельностью военного лобби по неоправданному раздуванию военных расходов на традиционные, и к тому времени уже отсталые вооружения, чье производство изнуряло и лишало ресурсов все остальные сектора советской экономики. Свою лепту внесло слабоволие и потребительские устремления широких слоев населения. А заграница, как всегда, помогла России разрушить саму себя.

Поэтому неудивительно, что уже в 70-е – 80-е годы многократные попытки вновь показать по центральному телевидению фильм «Русское чудо» наталкивались на отказы высших телевизионных начальников, действующих по указке тогдашнего ЦК КПСС. «Русское чудо» в тот период было уже не нужно подавляющей части правящего партийно-бюрократического слоя. Ведь главный смысл фильма состоял в том, что потенциал страны Советов был таков, что в конце XX века вполне вероятным является еще одно «Русское чудо».

На протяжении четверти века после выхода фильма на экраны советская наука и техника успешно подтверждала вывод восточногерманских кинематографистов. Практически во всех ключевых сферах – от космоса до исследований морского дна, от биотехнологий до энергетики, от вычислительной техники до новых типов вооружений, были совершены прорывы, которые при их

инженерном и промышленном подкреплении могли бы произвести переворот в мировом хозяйстве.

Это не преувеличение. Сразу же после прихода на пост президента США Рональда Рейгана на самом высоком уровне был запущен проект «Сократос» под руководством физика, полковника М. Секоры. Наиболее детальный, документированный и ориентированный на сегодняшний день отчет о проекте «Сократос» опубликован в книге Эрвина Экмана «President Reagan's Program to Secure U.S. Leadership Indefinitely: Project Socrates». Главная цель проекта состояла в объективном анализе уровня конкурентоспособности критических отраслей промышленности США, выявлении сфер науки и техники, где США отставали от СССР, Европы, Японии и осуществлении экстраординарных мер по преодолению отставания и обеспечению лидирующих позиций во всех критических технологиях уже в течение 80-х годов. Проект реализовывался во всех ключевых отраслях науки, промышленности и технологий Соединенных Штатов с вовлечением в него всех крупнейших высокотехнологичных корпораций, университетов, исследовательских центров и т.п.

В СССР в это время случилась перестройка. Технологии были забыты. Научно-технические направления прикрывались и лишались финансирования буквально ежемесячно. В какой-то мере научно-технологический погром эпохи перестройки стал продолжением падения научно-технического фактора в экономическом развитии СССР, которое началось еще со второй половины 70-х годов. Тогда науку и технику подменили открытые в Тюмени месторождения, и высшее партийное руководство подсадило страну на нефтяную иглу. Именно в 70-е годы были посеяны семена развала, которые в полной мере проявились в 1991 году. В общем, пока американское государство занималось ликвидацией технологического отставания, массированным вливанием средств в науку

и технику, Советский Союз предпочел тупиковую модель нефтепотребительского социализма. Тогда же в стране приняли к руководству к действию слова заокеанского президента Д. Кеннеди с точностью до наоборот. Бросили учить физику и принялись осваивать английский по Rolling Stones и Led Zeppelin.

Несмотря на все неблагоприятные обстоятельства, внутри различных сегментов российской экономики и, прежде всего, военно-промышленного сектора продолжали развиваться островки высоких технологий. Как это ни удивительно, наибольших успехов практически в большинстве сфер науки и техники Советский Союз достиг на технологическом уровне в самом конце 80-х годов, когда в полной мере начал действовать ранее созданный научный задел. Символом триумфа советской технологической мощи стал до сих пор не воспроизведенный в мире вывод на орбиту крупнотоннажного непилотируемого возвращаемого орбитального комплекса «Буран» с его успешным возвращением на Землю. Другой поразительной иллюстрацией этих достижений является недавняя публикация одного из крупнейших американских журналов Nature, где выделялись семь наиболее перспективных энергетических технологий на ближайшие 15 лет в сфере ядерной энергетики. Пять из них к 1991 году уже существовали в Советском Союзе либо в виде опытных образцов, либо доведены до стадии инженерных расчетов и стендовых испытаний.

В постсоветской, так называемой «демократической, рыночной России» о фильме «Русское чудо» никто не вспоминал. На глобальном уровне стояли другие задачи: признать советскую действительность преступной, забыть о ней и никогда к ней не возвращаться. Эти цели во многом были реализованы. А главное – в общественное сознание была вбита устойчивая установка на то, что никакого нового русского чуда уже быть не может, что новая Россия должна быть просто встроена в общемиро-

вой процесс и пользоваться благами западной цивилизации, не претендуя ни на какое первенство и тем более чудеса в развитии.

### 8.2. На пороге Третьей производственной революции

Тем не менее, случилось то, что случилось. После краха СССР в мире окончательно восторжествовала мутация капитализма – потребительский финансизм. В 90-е – нулевые годы показалось, что научно-технический прогресс остановлен навсегда и все разработки сводятся к выпуску новой модели iPad или других гаджетов.

Возможно, так бы и продолжалось, если бы не глобальный финансово-экономический кризис, начавшийся в 2008 году. Под угрозой тотальной крупномасштабной катастрофы на Западе и на Востоке пришли в действие ослабленные и подавленные крахом СССР научно-технологические силы, которые соединились с государственными, венчурными и рисковыми капиталами, вставшими на ноги в ходе интернет-революции и накопившими огромные ресурсы всех типов информационными гигантами, и определенными политическими силами, заинтересованными в выживании глобальной мировой системы.

Параллельно с проведением частично целенаправленных, а частично – стихийных мер по ограничению всевластия спекулятивно-финансового и банковского капитала, произошло усиление корпоративных, государственных и социальных сил, делающих ставку на высокие технологии, как гарантию выживания современного социума и обеспечение его развития.

Любопытно, что даже сейчас, когда страна вырвалась из хаоса 90-х годов, идеологическая машина и левых, и правых в основном говорит о тяжелых перспективах экономического, финансового развития, стращает тяжелыми социальными последствиями. При этом

в современном российском обществе практически не обсуждаются проблемы, связанные с технологическим прогрессом XXI века, которые активнейшим образом обсуждаются на Западе и на Востоке, и не в среде профессоров и исследователей, а политическими, технологическими и экономическими элитами, субъектами действия и других групп и слоев населения.

Доступная информация свидетельствует о том, что при всех несомненных острых проблемах, противоречиях и трудностях, которые имеются в США, Западной Европе и Японии, буквально на наших глазах разворачивается и набирает темпы Третья производственная, или промышленная революция.

Своим названием она обязана международному бестселлеру Джереми Рифкина «The Third Industrial Revolution: How Lateral Power Is Transforming Energy, the Economy, and the World», которая стала настольной книгой многих политиков и Востока, и Запада. Ее автор признан одним из наиболее влиятельных экономистов современности. Он является советником Еврокомиссии. Среди его поклонников – Барак Обама, Политбюро Коммунистической партии Китая, правительство Бразилии, а на постсоветском пространстве – руководство Казахстана. На основе идей Рифкина разработан план дальнейшего экономического развития Евросоюза, который уже принят Европарламентом.

Наряду с книгой Дж. Рифкина о Третьей производственной революции возвестили еще две работы. Они стали настольными книгами не только в высоких государственных кабинетах, но и, прежде всего, в бизнесе, среди новой генерации научно-технического и программистского сословий. В их число входят книги Питера Марша «Новая индустриальная революция: потребители, глобализация и конец массового производства» (The New Industrial Revolution: Consumers, Globalization and the End of Mass Production), редактора одного из

наиболее авторитетных в мире журналов Economist, постоянного автора Financial Times, и бестселлер Криса Андерсона «Производители: Новая промышленная революция» (Makers: The New Industrial Revolution), редактора знаменитого журнала и интернет-портала Wired. К сожалению, ни одна из этих трех обсуждаемых, а сегодня уже и реализуемых во многих странах мира работ не переведена на русский язык.

### 8.3. Кластеры и технологические пакеты Третьей производственной революции

При всем различии позиций авторы упомянутых выше книг едины в том, что производственная революция означает глубокие, быстрые в исторической перспективе, скачкообразные (фазовые) изменения в самих основах техники и технологий, используемых в ключевых отраслях хозяйства. Эти изменения ведут к необратимым и качественным сдвигам в организации труда и производства, системах логистики, маркетинга и продаж. Производственная революция изменяет базовые структуры экономической жизни. Полностью перестраивает социум и привычные способы его регулирования. Преобразует политические институты. Любая производственная революция имеет неоспоримые положительные эффекты и неизбежно связана с целым рядом негативных социальных последствий и проблем для широких масс населения.

Третья производственная революция по своим масштабам, последствиям и сдвигам стоит не только наравне, а возможно и превосходит Первую и Вторую производственные революции. Первая производственная революция конца XVIII – начала XIX века была связана с текстильной отраслью, энергией пара, углем, железными дорогами и т.п. Вторая производственная революция конца XIX – первой половины XX века стала детищем электричества, двигателей внутреннего сгорания, триум-

фом машиностроения и конвейера, как метода организации производства.

Уже на начальных стадиях Третьей производственной революции можно выделить несколько определяющих ее черт:

• во-первых, одновременное широкое производственное применение различных независимых кластеров технологий. Прежде всего, робототехники, 3D-печати, новых материалов со спроектированными свойствами, биотехнологии, новых информационных технологий и, конечно же, диверсификация энергетического потенциала производства и общества;

• во-вторых, постоянно возрастающее взаимодействие между отдельными технологическими кластерами, их своеобразное «слипание», взаимное коммулятивное и резонансное воздействие друга на друга;

• в-третьих, появление на границах технологических кластеров принципиально новых, не существовавших ранее технологий и семейств технологий, в которых кластеры взаимодействуют между собой.

Основой основ превращения отдельных технологических кластеров или паттернов в единый технологический пакет играют информационные технологии, которые проникают буквально во все стороны технологической, производственной и социальной жизни, связывая между собой отдельные технологические блоки. Наиболее яркими примерами этого являются такие технологические паттерны, как биотехнологии, робототехника, управляемая на основе больших данных и т.п. По сути, уже на начальном этапе индустриальной революции можно говорить о формировании единого технологического пакета Третьей производственной революции.

В сфере организации производства и труда отличительной чертой Третьей производственной революции является миниатюризация производства в сочетании с сетевой логистикой и персонификацией потребления

продукции. Как отмечал в своей работе К. Андерсон: «Если раньше эффективные производства и действенные сети маркетинга и продаж были под силу только большим заводам, крупным ритейловым сетям и транснациональным корпорациям, то в самое ближайшее время это будет доступно всем». Правда, при всей миниатюризации и демократизации производства одновременно будет возрастать зависимость мелкого производителя от поставщиков Больших Данных, программных продуктов и интеллектуальных услуг, которыми останутся, по мнению Дж. Рифкина, крупнейшие информационные компании, типа IBM, Google, Amazon и проч.

Иными словами, децентрализация производства, переход к прямым связям в сфере распределения и персонификации потребления будет происходить в условиях сохранения господства цифровых гигантов, контролирующих ключевую технологию Третьей производственной революции – системы сбора, хранения, интеллектуальной обработки и распределенной доставки цифровых данных и знаний, а также компьютерных программ и сервисов всех типов и конфигураций.

Первым ключевым направлением Третьей производственной революции является стремительная автоматизация и роботизация производства. Как отмечают эксперты, принципиально многие элементы автоматизации и роботизации могли быть внедрены в промышленное производство еще в 80-90-е годы. Однако в те времена экономически выгоднее оказалось использовать вместо роботов практически дармовой труд рабочих из Китая и других азиатских стран. Но по прошествии почти четверти века ситуация изменилась. С одной стороны труд в Азии заметно подорожал. С другой стороны деиндустриализация Америки, многих стран Европы и частично Японии нанесла сильнейший удар по экономике этих стран. Наконец, за этот период появились принципиально новые программные и микроэлектронные

решения, позволяющие в разы повысить эффективность и функционал роботов при снижении себестоимости их производства. Сегодня, например, типовой американский робот на конвейере окупается в течение полутора, максимум двух лет.

Уже сейчас в Америке действует или готовится к пуску в ближайшие годы более 9 тыс. полностью автоматизированных производств. И это только начало. В Соединенных Штатах на 10 000 рабочих мест в производстве приходится 870 комплексно-автоматизированных рабочих мест, в Японии – 400, в Корее – 270, Китае – 32. Не менее впечатляющая статистика имеется по так называемым человекоподобным индустриальным роботам всех типов. В 2012 году по данным Международной федерации робототехники шире всего применялись человекоподобные роботы в Южной Корее. Там на 10 000 занятых приходилось 400 таких роботов, в Японии – примерно 320, в Германии – 250, в США – 150.

В настоящее время безусловным лидером по производству промышленных, высокотехнологичных роботов являются Соединенные Штаты Америки. В 2013 году на предприятия США поставлено чуть менее 20 тыс. единиц высокотехнологичных антропоморфных роботов. В нашей стране в 2012 году имелось всего 307 роботов. Из них 65 поступило из-за рубежа. Для сравнения в крошечной Чехии подобных роботов тысяча.

Ради справедливости надо сказать, что США не являются лидером по уже установленным промышленным роботам. Первое место уверенно держит Япония. Второе место занимает Китай. И лишь на третьем месте – Соединенные Штаты. Лидирующую пятерку замыкают Южная Корея и Германия. При этом по оценкам специалистов китайские роботы менее технологичны и применяются в основном на элементарных сборочных работах, связанных с выпуском традиционных гаджетов и бытовой техники.

Вторым направлением Третьей производственной революции, а по мнению, Криса Андерсона, даже главной ее движущей силой является 3D-печать. В основе 3D-печати лежит технология под названием Additive Manufacturing, то есть аддитивное (впору сказать «поэтапное») изготовление. Метод подразумевает, что принтер послойно формирует изделие, пока оно не примет окончательный вид. 3D-принтеры не наносят на бумагу краску, а «выращивают» объект из пластмассы, металла или других материалов.

Методы трехмерной печати также заметно разнятся. 3D-принтер может слой за слоем наносить жидкий материал (например, керамику или пластик), который сразу же застывает. Широко используется более технологичный метод, где сырьем служит порошковый металл (например, сталь, титан, алюминий). В этом случае лазерный луч скользит по отдельным слоям и, согласно заданной программе, плавит и склеивает те или иные крупицы друг с другом. Существует еще множество различных типов 3D-печати. На конец 2013 года выпущено уже более тысячи моделей различных 3D-принтеров, рассчитанных как на принципиально различные методы печати и используемого материала, так и на совершенно различный бюджет. В настоящее время ряд крупных производителей 3D-принтеров выступили вместе с интернет-гигантами, типа Google и Amazon с предложением к правительству США бесплатно поставить 3D-принтеры сначала в подавляющее большинство, а затем и во все школы. А в последующем наладить обязательное обучение на уроках труда работе с 3D-принтерами.

Если на первом этапе 3D-принтеры в основном использовали гики и продвинутые дизайнеры, то затем наступила очередь инженеров и конструкторов. Ведущие компании стали активно использовать 3D-печать для моделирования. Затем 3D-печать пошла в массы. Например, выпускник Принстона Марчин Якубовски

создал целую социальную сеть, объединяющую инженеров, конструкторов, энтузиастов 3D-печати, которые совместными усилиями разрабатывают Global Village Construction Set – все, что вам нужно в «глобальной деревне». В сети публикуются в открытом доступе 3D-чертежи, схемы, видеоинструкции, бюджеты и пользовательские инструкции. В результате появляется то, что К. Андерсон называет «индустрией облака» или «облачным производством». По его словам: «Вы загружаете в глобальное сетевое облако заказ на продукт, который вас интересует, где дальше это задание находит своего оптимального исполнителя, который может произвести это максимально быстро, качественно и дешево».

В текущем году произошел прорыв в области промышленного использования 3D-печати крупнейшими корпорациями. Линии 3D-печати в настоящее время строят Boing, Samsung, Siemens, Canon, General Electric и т.п. Из стадий опытных образцов и экспериментов на уровень массовой строительной технологии постепенно выходит использование 3D-печати для строительства коттеджей, небольших домов и других сооружений. В настоящее время мировой рынок продажи 3D-принтеров оценивался от 3 до 3,5 млрд. долларов и в среднем удваивается в течение полутора лет, т.е. следует знаменитому компьютерному Закону Мура.

Бесспорным лидером как в производстве 3D-принтеров, так и в их использовании являются Соединенные Штаты. На них приходится почти 40% мирового производства 3D-принтеров. Около 10% – доля Японии. Практически столько же приходится на Германию и Китай. Пятерку лидеров с 6% замыкает Великобритания. Россия в сфере промышленного применения 3D-принтеров занимает десятое место. Что же касается применения 3D-принтеров, как основы минифабрик, то в России вместе с Африкой таких производств, по данным ведущего мирового эксперта в сфере 3D-печати, нет вообще, за исключением нескольких учебных лабораторий.

Третьим направлением новой производственной революции является производство новых материалов, включая материалы с заранее спроектированными свойствами, композитные материалы и т.п. Необходимость появления широчайшей гаммы новых материалов диктуется с одной стороны требованиями широкого внедрения экономичной, эффективной 3D-печати, а с другой – развитием микроэлектроники, биотехнологий и т.п.

В свое время новое материаловедение связывали исключительно с наноматериалами, т.е. с новыми материалами, производимыми на основе миниатюризации. Однако действительность оказалась несколько иной. При всей важности нанотехнологий на сегодняшний день ключевое место заняло производство материалов с наперед заданными характеристиками, требуемыми с одной стороны для наилучшего выполнения изделием своих функций, а с другой – возможности использования для производства изделий новых технологических методов типа 3D-печати. Лидерами в новом материаловедении и производстве принципиально новых материалов являются опять же Соединенные Штаты, Япония и Германия. Россия, несмотря на колоссальный научный, и частично технический задел, созданный еще в советские годы, благодаря достижениям институтов АН СССР и деятельности композитной промышленности, в настоящий момент не входит в число лидеров. Хотя отдельные разработки у российских ученых имеются. Ярким подтверждением этого стал факт присуждения Нобелевской премии по физике за 2010 год А. Гейму и К. Новоселову за новаторские эксперименты с графеном. Нобелевскую премию они получили, будучи уже гражданами Нидерландов и Великобритании, но работу проводили еще как сотрудники Научного центра РАН в Черноголовке.

Ключевым направлением Третьей производственной революции являются без сомнения биотехнологии в широком смысле этого слова. По сути, сюда входит инду-

стрия индивидуализированных лекарств, на которые делают ставку и фармацевтические гиганты, и новые, молодые, быстроразвивающиеся компании в этой сфере. Сюда же относятся различные виды регенеративной медицины. Широко используются возможности 3D-печати для производства донорских органов. Сегодня это уже не фантастика, а прошедшая клинические испытания обыденность, которую взяли на вооружение, например, медицинские учреждения Франции, Германии, Соединенных Штатов и т.п.

Особым направлением является биоинформатика. Четыре года назад группе исследователей во главе с Джоном Крейгом Вентерем удалось впервые в истории создать искусственную жизнь, используя ДНК одного из вирусов. Теперь эта команда может, что называется, производить новые виды бактерий и живых организмов прямо из компьютера. Дж. Вентер так и заявил, что им удалось сделать «первый самовоспроизводящийся биологический вид на планете, родителем которого является компьютер». В 2009 году, после приема у Б. Обамы исследования хотели засекретить. Но в итоге приняли решение открыть разработки миру. Сегодня, по мнению Дж. Вентера, синтетическая биология – это «мощнейший набор инструментов, который в ближайшие годы приведет к созданию эффективных вакцин против самых различных заболеваний, начиная от гриппа, заканчивая СПИДом». Правда, он же предупредил о страшной опасности, попади эти инструменты в руки террористов и экстремистов.

Нельзя не отметить, что вплоть до 1991 года советская микробиология и биоинженерия занимали лидирующие позиции в мире. По оценкам американских экспертов, благодаря существованию специализированного российского комитета – Главмикробиопрома, с большой сетью подведомственных научно-исследовательских и производственных центров и учебных институтов, Со-

ветский Союз заметно опережал другие страны мира по многим направлениям биотехнологий и генной инженерии. Однако затем, под флагом борьбы с биологическим оружием и в условиях погрома высокотехнологичных отраслей отечественной промышленности, значительная доля потенциала оказалась утерянной. Хотя, по оценкам зарубежных экспертов, при должной мобилизации сил Россия может, базируясь на имеющихся разработках и достижениях действующих научных школах, диаспоре российских биотехнологов, работающих за рубежом, наверстать упущенное.

Первая и Вторая производственные революции в корне меняли основной энергетический источник. Если первая промышленная революция была реализована на угле, то вторая производственная революция стала детищем нефти и электричества. В отличие от других направлений, относительно энергетического базиса Третьей производственной революции единодушия среди специалистов нет. В частности, автор первой и самой популярной в свое время книги о Третьей производственной революции, Дж. Рифкин являлся убежденным сторонником «зеленой», возобновляемой энергетики. Более того, он стал одним из инициаторов разработки принятого в ЕС плана, связанного с закрытием АЭС, сокращением использования, по его мнению, экологически вредных электростанций на угле, нефти и т.п. Сегодня европейские промышленники, отдавая должное Дж. Рифкину в других областях, часто и недобрым словом поминают его в части «озеленения» энергетики, а также продвижения бредовых идей замены газа ветряками и подобными шалостями «зеленых».

Без излишнего шума большинство теоретиков, а главное – практиков на высоких правительственных постах, отвечающих на Третью производственную революцию, считают, что будущее принадлежит не возобновляемым источникам энергии, а принципиально новым

видам ядерной энергетики, прогрессивным технологиям добычи газа и нефтесодержащих элементов, а также совершенно новым типам энергетики.

Стержневой составляющей, пронизывающей все технологические кластеры Третьей производственной революции и превращающей их в единый технологический пакет, являются без сомнения, информационные технологии. Применительно к теме Третьей производственной революции в структуре информационных технологий выделяются три ключевые составляющие.

*Первая.* Это – Большие Данные. Большие Данные – это сбор, хранение, оцифровка, обработка и предоставление в удобном для пользователя виде в любое время и в любой точке всей совокупности сведений о тех или иных событиях, процессах, явлениях и т.п. Ключевым в Больших Данных является то, что они позволяют работать именно со всей информацией в режиме онлайн. Главным является слово «всей». У пользователя Больших Данных имеется вся картина, не зависящая как раньше от каких-либо выборок, ограничений по источникам, времени предоставления данных и т.п. Большие Данные могут включать в себя любые форматы – от таблиц до потокового видео, от оцифровки старых отчетов, до текстовой записи, сделанной теми или иными источниками. Никогда раньше в истории человечества у лиц, занимающихся анализом, прогнозированием, конструкторско-инженерной деятельностью, принятием решений не было возможности оперировать со всей информацией. Причем, не просто оперировать, а получать эту информацию в удобном и доступном для восприятия виде. Сегодня безусловными лидерами в сфере Больших Данных являются США, Великобритания, Япония и Китай. В этих странах имеется большое количество платформ, обеспечивающих работу с Большими Данными, специальные курсы подготовки, множество центров, где компании могут получить консультации или услуги, связаннее с Большими Данными.

В России, надо прямо сказать, ситуация плачевная. Притом, что в нашей стране разработана мощнейшая алгоритмическая и математическая база для интеллектуального анализа Больших Данных, самих Данных по большому счету нет. То, что у нас называют Большими Данными в подавляющей части – это уже много лет применяемая за рубежом традиционная бизнес-аналитика. Специалисты по Большим Данным в стране пока не готовятся. Нет ускоренных центров переподготовки. У нас издана на сегодняшний день единственная книга, посвященная этой теме, которая носит скорее не учебный, а научно-популярный характер ( В. Майер-Шенбергер и К. Кукьер «Большие Данные. Революция, которая изменит то, как мы живем, работаем и мыслим»).

Сами по себе Большие Данные являются важнейшим государственным и корпоративным активом, который при должном использовании обеспечивает их владельцам устрашающее интеллектуальное превосходство и деловое доминирование.

*Вторая.* Это – когнитивные вычисления и экспертные системы. За последние два-три года Соединенным Штатам и частично Великобритании удалось осуществить подлинный прорыв в области создания экспертных систем, базирующихся на так называемых когнитивных вычислениях. В основу когнитивных вычислений заложены программы, в определенной степени моделирующие и имитирующие некоторые известные психофизиологические процессы. За счет этого созданы программы, которые облают возможностями самодописываться и совершенствоваться, учитывая допущенные ими при решении тех или иных задач ошибки. Наиболее известной экспертной системой, базирующейся на когнитивных вычислениях, стал знаменитый компьютер Watson корпорации IBM, победивший во вполне человеческой игре «Своя игра». После победы на игровом поле Watson показал высокие результаты как экспертная система в ме-

дицинской онкологии, фармацевтике, полицейских расследованиях, биржевом деле. По оценкам различных экспертов в ближайшие 7–12 лет он может вытеснить до 70% работников, занимающихся рутинным умственным трудом в самых различных сферах деятельности. Главное даже не в этом. Экспертные системы дают их обладателям и пользователям огромную интеллектуальную мощь, ставя на службу богатство человеческого знания, помноженного на мощь вычислительных алгоритмов. При этом надо отметить, что IBM уже не является монополистом. Об активной работе в этом направлении объявили Google, Facebook, Amazon.com и проч.

*Третья.* Это – облачные и распределенные вычисления. Как нетрудно заметить, огромные мощности и программные ресурсы, потребные для работы с Большими Данными, когнитивными вычислениями, созданием мощных экспертных систем класса Watson по карману только крупнейшим корпорациям. В этих условиях развитие облачных распределенных вычислений, т.е. создание платформ, которыми одновременно могут пользоваться десятки, сотни, а то и миллионы пользователей, делает Большие Данные, когнитивные вычисления и мощнейшие экспертные системы доступными для самого маленького бизнеса и отдельных граждан. Уже сегодня компания IBM открыла для сторонних разработчиков облачный Watson, и они делают программы под заказ для небольшого бизнеса.

Иными словами, три составляющих информационных технологий позволяют наделить децентрализованные маленькие и сверхмаленькие производства на основе робототехники, 3D-печати, биотехнологий и проч. мощнейшими интеллектуальными ресурсами, которыми сегодня располагают только крупнейшие корпорации.

Правда, ценой такого наделения и вообще широкого использования интеллектуальных облачных технологий является отказ от прокламируемой рядом пионеров

Третьей индустриальной революции, типа Дж. Рифкина и К. Андерсона, исключительно демократического, полностью сетевого характера Третьей индустриальной революции, где не будет места иерархии. Это, конечно же, иллюзия. Но она ни в коей мере не отменяет будущее, которое наступает в странах, где разворачивается Третья индустриальная революция буквально не по дням, а по часам.

В настоящее время информационные технологии являются своего рода платформой технологического развития, точно так же как во время Второй производственной революции такой платформой выступало машиностроение. Наступает эра цифрового производства.

Цифровое производство приобретает самые неожиданные формы. В настоящее время несколько американских компаний, занятых производством роботов и 3D-принтеров, включая Google, заняты реализацией проекта Factory-in-a-Day. Первые такого рода минизаводы предполагается запустить уже в 2015 году. Проект должен позволить разворачивать автоматизированное производство не только на крупных предприятиях, но и на средних, мелких и сверхмелких не более чем за 24 часа. Эти заводы комплектуются гибкими многофункциональными роботами, 3D-принтерами, лазерными резаками и т.п. Роботы, принтеры и другое оборудование поставляются с уже загруженными в них наиболее популярными программами, обеспечивающими их эффективную работу. Т.е. завод поставляется примерно так, как сегодня продается смартфон или планшетник с предустановленным ПО. Все необходимое в течение дня можно получить из облака. Заблаговременно, до поставки предприятия, его владельцы и персонал получают учебный курс работы на предприятии с компьютерной игрой, эмулирующей и обучающей реальной деятельности. В ходе эксплуатации завода 24 часа в сутки его пользователям обеспечивается техническая поддержка

и консультации со стороны изготовителя оборудования и софта. Плюс из облака имеется возможность подгружать необходимые дополнительные программы, получать экспертные советы, обрабатывать Большие Данные.

Еще дальше пошли производители фаблабов. Эти производственные лаборатории оснащаются многофункциональными станками, 3D-принтерами, другими необходимыми приспособлениями. Особенность этих лабораторий состоит в том, что они не только позволяют произвести в натуре ту или иную разработку или изобретение, но и обладают потенциалом для собственного расширенного производства. Т.е. фаблаб спроектирован таким образом, что, используя имеющееся оборудование, способен достраивать и расширять имеющийся функционал. Никогда раньше такого не предусматривалось. Хорошо известно, что всегда существовали предприятия по производству средств производства для производства средств производства и т.п. Теперь же в рамках одного предприятия можно расширять и само предприятие и производить средства производства, и предметы для конечного персонифицированного пользователя.

Идеолог фаблабов – преподаватель Массачусетского технологического института Нил Гершенфельд доказывал, что производственная революция уже произошла, только она находится в латентной стадии: «Охват сети интернет каждый год удваивался в течение примерно десяти лет. Казалось, что интернет возник из ниоткуда, но на самом деле он просто долгое время развивался и мало кто его замечал. То же сейчас происходит с фаблабами. Или другая параллель: когда только стали появляться персональные компьютеры, почти все производители больших компьютеров решили, что это игрушки, что-то несерьезное. И все они потерпели крах, кроме IBM. То же и с новыми машинами для цифрового производства: они замещают привычную промышленность и создают новую, подрывая сложившийся порядок».

В мире насчитываются уже сотни, а в следующем году будут созданы и тысячи фаблабов. В 2013 году первый фаблаб в России был открыт в Москве на базе МИСИС Н. Гершенфельдом.

Одним из первых плодов ранней стадии Третьей производственной революции становится возврат производства в Америку и Европу. В 2013 году более половины компаний с оборотом миллиард долларов, объявило, что в ближайшие несколько лет полностью вернет производство из Китая и других азиатских стран в Соединенные Штаты. В США за последнее время темпы роста промышленности превышают динамику многих других секторов экономики. Создано более 500 тыс. несезонных рабочих мест. Это, конечно, не идет ни в какое сравнение с 6 млн. рабочих мест, потерянных промышленностью США. Но это места в своей массе, отвечающие требованиям Третьей производственной революции с соответствующими показателями производительности и эффективности.

Следует также иметь в виду, что 75% новых разработок и технологий и почти 90% новых, зарегистрированных патентов создаются в США именно в сфере промышленного производства. Нельзя также не отметить, что в настоящее время Соединенные Штаты контролируют более 65% высокотехнологичных разработок и 55% высокотехнологичных патентов в мире.

Подобные процессы активно разворачивается в Южной Корее, Японии. Началась реиндустриализация Великобритании. Спохватилась Германия, длительное время почивавшая на лаврах самой успешной высокоиндустриальной экономики XXI века. Пытается развернуть у себя Третью производственную революцию и Китай. Хотя именно в Китае в силу чрезвычайно высокой избыточной доли сельского работоспособного населения, и занятости традиционным индустриальным трудом основной части городского населения реализовать до-

стижения Третьей индустриальной революции очень и очень тяжело. А что же Россия?

### 8.4. Из жизни рентополучателей

Россия за последние 25 лет из «страны мечтателей и ученых», военных и рабочих превратилась в территорию миллиардеров, менеджеров и продажников. С Россией стали связывать не триумфы в космосе и пуск новых энергетических гигантов, а покупку «Челси», «Арсенала» и очередные киберпреступления русских хакеров.

Модель, победившая в декабре 1991 и октябре 1993 годов, с ветшающим технологическим базисом, дистрофичной воспроизводственной инфраструктурой, распадающейся тканью социальных взаимоотношений сотрудничества и взаимодействия уже прошла точку своего невозврата. Долгие годы политики, экономисты постоянно употребляли дежурные слова о том, что «еще немного, и мы пройдем точку невозврата». Сегодня понятно, что то, что было создано в 90-е и сохранилось в нулевые, точку своего невозврата прошло и впереди только перспективы жизни слабоструктурированного населения, проживающего на территории, на которой может быть все, что угодно.

Метафорой реформистской России, неудачливой наследнице СССР, стал алкоголик. Как известно, для того, чтобы купить желаемый горячительный напиток, он сначала продает унаследованные от родителей картины и другие ценные вещи. Потом приходит очередь кухонной утвари, мебели, наконец, в дело идет снятый с пола паркет, а после этого разгневанные жильцы дома просто выкидывают его из квартиры на улицу. И становится он бомжом.

Буквально на нескольких цифрах можно показать, что приведенная выше метафора не является преувеличением.

В одном из отчетов правительству министр финансов РФ А. Силуанов сообщил, что и в 2013 году, как и в прошлые годы, более половины доходов бюджета составило поступление из нефтегазового сектора. На него же приходится более 70% экспорта и более 30% внутреннего валового дохода. Однако, по факту роль этого сектора еще выше. Дело в том, что такие развитые сектора, как торговля, финансовый сектор и т.п., вносящие значительный вклад и в объем ВВП, и в формирование бюджетной базы в существенной мере порождены и зависят от положения дел в энергетическом секторе.

Фактически, как показывают многочисленные исследования, так или иначе от этого сектора зависит практически все, даже столь, казалось бы, далекая сфера, как информационные технологии. Если бы не нефтегазовые деньги, в нашей стране не могли бы существовать десятки съедающих миллионы долларов стартапов, совершенно не рассчитанных на какую-либо экономическую окупаемость, в которых трудятся лучшие программисты и разработчики, вполне способные при других обстоятельствах создавать экспертные системы и заниматься когнитивными вычислениями.

Порождением нефтегазовых потоков, а также проведенной после невиданного в мире обесценивания национального богатства, бесчестной приватизации, стали 130 миллиардеров и некоторая часть из 180 тыс. долларовых миллионеров, которые имеются в нашей стране. Однако не стояли в стороне от нефтегазового пирога и широкие народные массы. В то время как во всем мире в этом веке население, и особенно средний класс, затягивали пояса, у нас длился просто праздник жизни.

Институт глобализации и социальных движений на основе данных Роскомстата подсчитал: с 2000 по 2013 год средняя зарплата в России выросла на 900%. При этом, реально зарплата за этот период с учетом индекса потребительских цен увеличилась в 4,7 раза. А реальный

размер назначенных пенсий (по всем видам пенсий) – в 4,9 раза. Ничего подобного не происходило ни в одной развитой стране мира, за исключением Китая, где зарплаты и доходы росли в меру роста национального продукта, а главное – повышения производительности труда и эффективности производства. У нас никакой связи между зарплатой и доходами, и производительностью и эффективностью в этом веке не было. Тратились возросшие доходы, пенсии и другие денежные поступления либо на импорт, либо на отечественную продукцию народного потребления. Следует отметить, что согласно данным журнала «Эксперт», в продукции, произведенной для потребления домохозяйствами, предприятиями-резидентами РФ по большинству позиций, до 60–70% себестоимости составляют затраты на покупку импортных комплектующий, компонентов и т.п. И потребительский импорт, и закупка этих компонентов осуществляется в подавляющей части опять же за счет экспорта сырья и продуктов первого передела.

Главным фактором нашего благосостояния являлся рост цен на нефть и связанные с ней другие энергоносители. Если в 1998 году за баррель нефти давали 14 долларов, то сегодня – более 100 долларов.

Здесь напрашивается вопрос. Почему же руководство, в начале нулевых осуществившее решительные меры по наведению порядка, обузданию олигархических кланов, пресечению сепаратистских тенденций, не увидело эту опасность, и в каком-то смысле потеряло целое десятилетие для решительной модернизации? Ответ, как ни странно, по нашему мнению, можно найти в многочисленных работах психологов, социологов и клиницистов из России и других стран мира, занимавшихся обследованиями фобий и других патологий у людей, переживших техногенные, природные катастрофы, и оказавшихся в районах чрезвычайных событий. Работы практически всех, даже не знакомых друг с другом авторов, говорят примерно об одном и том же.

Люди, пережившие закритичный уровень стресса в результате катастрофических событий в значительной степени утрачивают навыки самостоятельных действий, отказываются осуществлять какие-либо дополнительные усилия, полностью теряют склонность к волевым действиям, предрасположенность к риску и стремятся к спокойной, упорядоченной, что называется «сытой» жизни, по возможности, перекладывая ответственность за любые решения на какие-то другие инстанции. Зачастую эти инстанции они воспринимают как своего рода «магического спасателя», который должен решить за них все их проблемы. Такая компенсаторная реакция и тип поведения имеют место вне зависимости от уровня развитости общества, профессионального, квалификационного или имущественного состава обследованных групп. Сходные результаты были получены и после Чернобыля и Спитака, и на Гаити, и, казалось бы, в продвинутых Соединенных Штатах, в Новом Орлеане после урагана «Катрин».

Представляется, что вторая половина 80-х – 90-е годы в России как раз и стали длительным периодом закритичного стресса для основной части населения Российской Федерации. Соответственно в послестрессовой ситуации оно могло действовать только в соответствии с выявленными закономерностями. Власть же в данном случае просто подстраивалась под объективную ситуацию и действовала исходя из жестких поведенческих стереотипов основной части российского социума. При этом, кстати, надо иметь в виду, что и сама власть является частью этого социума.

Иными словами, вся страна – и богатые, и бедные, и миллиардеры, и малообеспеченные слои населения, чьи доходы росли опережающими темпами, превратились в большой и дружный коллектив рентополучателей, живших на то, что завоевали и построили предки. При этом нынешнее поколение россиян бездумно отнимало буду-

щее у своих детей и внуков. Если бы рост доходов хоть както был увязан с заботой о наращивании технологического потенциала, обновлением основных фондов, то это было бы полбеды. Но у нас случилась беда в полный рост.

Если в период модернизации норма накопления в структуре ВВП составляла, например, в Германии и Японии 40-60%, в Китае – более 30%, то в России она не поднималась выше 20%. Да и то значительная часть этих накоплений оказалась потрачена на новые версии «проектов века».

По мнению помощника Президента РФ А. Белоусова: «В российской экономике накопился колоссальный инвестиционный долг. И не только в инфраструктуре. Средний срок службы оборудования в ряде важных отраслей российской промышленности составляет 20 лет. А в реальности эта «средняя температура по больнице» означает, что российская экономика состоит из двух разных частей. Одна работает на относительно новом оборудовании, другая – на оборудовании в лучшем случае 70-х годов. Нередко на заводах, имеющих госзаказ, то есть работающих и достаточно успешных на общем фоне, можно встретить вот такой своеобразный набор оборудования: в литейке – импортная американская машина 1935 г., сварка ведется на советском оборудовании 60-х годов, при этом может быть внедрена какаянибудь специальная компьютерная система на одной из финальных стадий производства». Общий уровень износа производственного оборудования в России достиг в 2013 году ужасающей величины – 80%.

Выдающийся и всемирно известный российский экономист Г. Ханин считает: «Самое опасное: за 20 лет произошло беспрецедентное, большее, чем во время Великой Отечественной войны, сокращение основных фондов, то есть материальной базы экономики. Часть этих фондов разрушена и растащена, сдана на металлолом, часть крайне изношена… При этом почти на 30%

(и это тоже беспрецедентно) сократилась реальная производительность труда».

Впрочем, значительная часть нашего экономического истеблишмента считает, что ничего страшного не происходит. Например, главный советник руководителя Аналитического центра при Правительстве РФ Леонид Григорьев полагает: «Катастрофы никакой нет, пока цены на нефть остаются в районе сотни. Потребление «кормится» за счет импорта. Получили деньги, вывезли что смогли, на остальное купили потребительские товары и живем. Медленно, спокойно окончательно превращаемся в нефтеэкспортирующую страну латиноамериканского толка». Ничего, что доля российского высокотехнологического экспорта в общемировом объеме равна размерам статистической погрешности, порядка 0,6%.

Однако жить по Л. Григорьеву вряд ли получится. Дело здесь заключается в особенностях ценообразования на нефть и другие энергоносители, а также ситуации на этих рынках. Известно, что в последние годы темпы экономического роста в России падают даже при сохраняющихся высоких ценах на энергоносители. Сегодня уже правительство обсуждает вопрос, насколько длительным будет период сверхнизких темпов экономического роста, и вступила или нет российская экономика в период рецессии, которая на академическом языке скрывает простое и понятное слово «кризис». При этом понемногу уменьшается и экспорт нефти. Возможно в будущем такое же может произойти и с газом в силу ужесточающейся конкуренции на мировых рынках. Но главное не в этом.

Взлет цен в текущем веке на энергоносители лишь в небольшой части связан с резко возросшим потреблением Китая, Индии, Бразилии и других новых индустриальных стран, на которые приходится не более 10% общего мирового потребления. Главным стало то, что в 90-е годы помимо физической нефти на рынке во все возрастаю-

щих объемах появилась так называемая «бумажная нефть». Это – торгуемые на биржевых площадках фьючерсы на поставку нефти, а затем газа, а также другие производные, имеющие общее название «деривативы». Сегодня объем сделок с бумажными энергоносителями значительно превышает объем сделок с реальной нефтью. Соответственно, спекулятивная составляющая в цене нефти и привязанных к ней ценах на другие энергоносители постоянно растет, и составляет по различным оценкам от 40 до 60% в общей цене.

В конце прошлого века в Соединенных Штатах и Западной Европе был принят целый ряд нормативных актов, стимулирующих спекуляции на рынке бумажных энергоносителей. Был отменен закон Стиголла-Гласса. Это дало поистине необозримые возможности банкам и другим инвестиционным институтам для разного рода финансовых спекуляций, включая создание и использование разнообразных производных финансовых инструментов, так называемых деривативов.

Затем, на самом рубеже тысячелетий, практически были сняты все барьеры на пути развития рынка деривативов и отменено их жесткое регулирование. Кроме того, в этот же период, как показывает реальная статистика, происходила значительная эмиссия денежных средств, по размерам сопоставимая с объемами эмиссии после кризиса. Огромные спекулятивные капиталы, ринувшиеся на рынок бумажных энергоносителей, в значительной мере и спровоцировали фантастический рост цен на нефть.

В 2014 г. начало реализовываться суровое правило Волкера, которое значительно ограничивает возможности банков спекулировать на фондовых и товарных рынках. В Европе открыт ряд серьезных расследований против крупнейших мировых банков, связанных с их сговором для извлечения незаконной прибыли на спекуляциях с золотом, нефтью и металлами. С учетом того,

что 95% контрактов на спекулятивную бумажную нефть и другие энергоносители принадлежат крупнейшим семи американским банкам, против которых собственно и направлены все указанные меры, в теме «бумажная нефть» можно ожидать самых неожиданных поворотов.

Никто не отважится делать точные прогнозы относительно цены на нефть и газ даже на ближайшие годы. Понятно, что ряд факторов, в том числе связанных с Третьей производственной революцией и диверсификацией энергетики, будут требовать сохранения относительно высоких цен. Но вряд ли это продлится долго. Более того, проведение отмеченных выше финансовых репрессивных мер против банковских спекуляций в сочетании с ограничением эмиссии центральными банками, несомненно, будут действовать понижательно на рост цен на энергоносители. Кроме того, в условиях обострения финансово-экономического кризиса, как показывает практика, первой реакцией становится бегство со спекулятивных рынков, приводящее к обвальному падению цен на энергоносители, металлы и т.п. В общем, по любому мы окончательно перестаем быть хозяевами собственной судьбы и становимся заложниками зыбкой и манипулируемой финансовой конъюнктуры.

### 8.5. Русский прорыв

Понятно, что в новых условиях старая экономика, базирующаяся на всенародном присвоении ренты и выжимании последних остатков из накопленного технологического потенциала, больше не работает. Точка невозврата действительно пройдена. Единственный выход в сложившемся положении – это осуществление Третьей производственной революции, причем в варианте гораздо более решительном и бескомпромиссном, чем за рубежом.

По сути, если мы в ближайшее время не начнем Третью производственную революцию, то перед страной

замаячит неприятный призрак социальных потрясений. На многие языки мира переведена знаменитая работа российских исследователей А.В. Коротаева, Д.А. Халтуриной, С.В. Кобзевой, Ю.В. Зинькиной «Ловушка на выходе из ловушки? О некоторых особенностях политико-демографической динамики модернизирующихся систем». Широко известны доклады Г.Г. Малинецкого о социальной динамике и не имеющие аналогов в мире методы моделирования политических и социальных потрясений И.Д. Колесина. Все эти работы, построенные на анализе огромного массива эмпирического материала с применением самых современных математических и содержательных методов анализа, показывают, что наибольшие угрозы возникают не там и не тогда, где и когда население длительное время живет плохо, а там, где после достаточно длительного периода неуклонного роста благосостояния и перехода к новым потребительским стандартам, происходит некое, зачастую весьма незначительное снижение доходов и уровня жизни. Несложно заметить, что это, к сожалению, может стать описанием нашего будущего.

В каком-то смысле, как говорил великий русский актер Ролан Быков: «Это очень хорошо, что пока нам плохо». В Соединенных Штатах, Европе, Японии и Китае существует достаточно большое число предприятий и владеющих ими мощных транснациональных групп, относящихся к традиционной, понемногу уходящей экономике. В свое время экономический рывок ФРГ и Японии, а в последующем Китая был связан во многом с тем, что они создавали свой производственный потенциал по сути с нуля. Старого потенциала либо не существовало, либо он был разрушен в ходе военных действий. У нас вместо военных действий были бездумные рыночные реформы и структуроразрушающая приватизация. Поэтому поле для Третьей производственной революции у нас на сегодняшний день в значительной степени рас-

чищено. Ослаблены и группы, которые связывают свое существование с традиционными уходящими технологическими укладами. Вместо этих групп у нас имеются группы рентополучателей различного типа. Но, как показывает история, противодействовать рентополучателям легче, чем монополистическим группам с особыми интересами.

Наконец, у нас, в отличие от большинства стран мира, в силу длительного пренебрежения к образованию и квалификационной подготовке, нет мощных профессиональных групп, которые будут препятствовать Третьей производственной революции. Например, сегодня в Соединенных Штатах в этом направлении уже активно действуют юристы, психоаналитики, офисные работники среднего звена и т.п.

Трудно препятствовать тому, что непонятно, неизвестно и, главное, не воспринимается серьезно на данный момент. А эффект неожиданности, опять же как свидетельствует мировой опыт, при должной воле и последовательности позволяет пройти первую, наиболее критичную фазу технологических преобразований. Что же касается навыков и знаний, необходимых для уверенной работы в рамках Третьей производственной революции, то сегодня уже существует целая гамма соответствующих учебных курсов, практических платформ, методов получения не столько знаний, сколько умений. Ими можно спокойно воспользоваться, и не изобретать велосипед. В крайнем случае, перевести ключевые курсы на русский язык и договориться о возможности проведения практических занятий, опять же на русском. Такая работа в настоящее время активно проводится. Как показывает опыт, ведущие мировые университеты, а также компании-производители роботов, 3D-принтеров, облачных платформ и т.п. охотно идут на это и поддерживают соответствующие инициативы.

Третья производственная революция в России не только возможна, но и весьма вероятна. Более того,

осмелимся высказать точку зрения, что она не является каким-то «русским чудом», а представляет собой своего рода производственную необходимость, которую нужно реализовать спокойно, трезво, систематично и дисциплинированно.

Прежде всего нельзя допустить идеологизаци и забалтывания Третьей производственной революции. Необходимо сразу расставить точки над i, и четко отделить ее от различного рода фантазмов, типа создания СССР 2.0 и подобных проектов. Еще совсем древним грекам было известно, что в одну и ту же реку нельзя войти дважды, и лозунги, подобные приведенному выше, имеют чисто пропагандистский характер, и лишь отвлекают работоспособную, умную и способную к действию часть российского населения от реального дела.

Практический подход к осуществлении Третьей производственной революции требует покончить в первую очередь с «разрухой в головах». Допустимо принятие любых мер, которые заставят людей повернуться лицом к реальности и начать мыслить технологически, а не политически. В конечном счете, отнимающие уйму времени, сил и ресурсов бесплодные дискуссии между левыми и правыми, патриотами и космополитами, либералами и коммунистами, государственниками и анархистами и т.п. носят в России преимущественно чисто политический характер. В обществе же рентополучателей политика сводится к тому, кто и как будет делить ренту, и кто сколько ее получит. При технологическом подходе идеологические ориентации и личностные взгляды на те или иные вопросы истории, философии и других увлекательных наук становятся не более чем личным делом. Единственно важным оказывается вопрос, можешь ли ты что-то сделать практическое, либо способен только получать деньги, как боец идеологического фронта.

Наконец, Третья производственная революция не имеет ничего общего со сверхмобилизационными

проектами 30-х годов прошлого века, различного рода «чрезвычайками» или загоном всех в гигантские высокоинтегрированные корпорации, которые будут создавать по единому плану десятки миллионов рабочих мест. Несмотря на то, что подобные проекты заполнили не только Рунет, но и страницы серьезных изданий, надо отдавать себе отчет, что то, что работало когда-то, не сможет работать сегодня. Более того, сам характер Третьей производственной революции предусматривает сочетание максимальной децентрализации, минипроизводств с выходом на гигантские централизованные платформы, носящие преимущественно не организационный, а технологический характер. В рамках Третьей производственной революции, единственным критерием для выбора тех или иных организационных форм или имущественных отношений становится технологическая целесообразность. Политика и идеология в России должны вернуться на свойственное им место, и из королев бала превратиться в служанок технологии и экономики.

### 8.6. Направления русского прорыва

Перво-наперво рачительный хозяин эффективно и заботливо использует то, что уже есть. Делает ставку на свои сильные стороны. В каждой стране и регионе Третья производственная революция должна осуществляться и осуществляется исходя из национальных задач, с учетом региональных и страновых особенностей и текущей ситуации.

Для русской производственной революции непреложным законом должен стать отказ от ломки чего-либо эффективного и работающего. Принцип «до основания, а затем» был многократно использован в истории нашей страны и в общем и целом показал свою крайнюю неэффективность.

Когда говорится и пишется, что экономика нашей страны не должна зависеть исключительно от топливно-

энергетического комплекса – это ни в коей мере не означает, что этот комплекс не является, по сути, единственно работающим сектором экономики, реально обеспечивающим ее текущую жизнедеятельность. Поэтому, Третья производственная революция должна развернуться именно в этом комплексе. Этому способствуют, по меньшей мере, три обстоятельства.

*Первое*. В 2013 году Президент Российской Федерации В.В. Путин сказал: «Все без исключения недропользователи обязаны соблюдать существующие условия разработки месторождений, полностью извлекать полезные ископаемые на всем предоставленном участке, а не работать по принципу «снятия сливок». Здесь имеется в виду, прежде всего, конечно, использование соответствующих технологий...» Подавляющее большинство таких технологий хорошо известно, и прошло практическую апробацию. Многие из них имеют отечественное происхождение. Другими располагают зарубежные партнеры крупнейших российских корпораций. В нынешних непростых, напряженных геополитических условиях важно любой ценой сохранить технологическое и экономическое взаимодействие на корпоративном уровне. Поэтому дело за малым – прекратить говорильню и начать делать дело. Тем более что конъюнктура нефтегазового рынка к этому принуждает.

Общим принципом в отношении новых технологий, и не только в нефтегазовом секторе, должно стать так называемое правило Лазаря Кагановича: «У каждой аварии есть имя, отчество и фамилия». Поставьте вместо слова «авария» слово «ошибка» и получите искомое. Причем, речь должна идти не о какой-то чрезвычайщине, а о систематической ежедневной работе по отслеживанию ответственности и применению мер к тем, кому даны права, и кто получает немалые вознаграждения.

*Второе.* Как блистательно доказали в своей работе «История. Кризисы. Перспективы. Новый взгляд на

прошлое и будущее» В. Криворотов и Л. Бадалян, наиболее глубокие и комплексные научно-технические прорывы происходят тогда, когда человечество осваивает новую среду обитания, либо по-научному «ценоз». Россия в последние годы, прежде всего, в лице топливно-энергетического комплекса, и в первую очередь, «Газпрома» и «Роснефти», возвращается в Арктику. Причем, делает это на долговременной системной основе. Буквально в самые последние месяцы запущена уникальная нефтедобывающая платформа «Газпрома» на Приразломном месторождении на арктическом шельфе. Наращивает объемы добычи и обустраивается гигантский международный проект «Ямал СПГ». Набирает мощность расположенное на Таймыре Ванкорское месторождение «Роснефти». Завершаются подготовительные работы к разворачиванию проекта по освоению крупнейшего месторождения редкоземельных металлов в Якутии, где свои возможности объединили новосибирские ученые, частный бизнес, власти Якутии и федеральный центр. Приход в Арктику, и вообще на Север, означает не только создание новых платформ добычи, но и целые инфраструктуры жизнеобитания, транспортировки и логистики.

В отличие от безумных проектов Е. Гайдара и его команды, предложивших просто бросить европейский и азиатский Север России, крупнейшие российские нефтегазовые компании с преобладающим государственным участием, вместе со своими зарубежными партнерами фактически занимаются созданием нового Арктического ценоза. Этот ценоз включает в себя и самые передовые технологические кластеры, складывающиеся в целостный технологический пакет Третьей арктической индустриальной революции, сложные системы постоянной человеческой жизнедеятельности в этих районах, самые передовые природосберегающие технологии, охраняющие экологию региона, гарантирующие его от повторе-

ния судьбы Мексиканского залива. Совершенно очевидно, что при тщательном продуманном подходе создание Арктического индустриального ценоза может стать одним из главных локомотивов Третьей российской производственной революции. Здесь, конечно, важно, преодолеть свойственное любой крупной корпорации во всем мире стремление внутренней бюрократии использовать освоение ценоза для получения бюрократической ренты, и отсечь от освоения ценоза передовые решения и технологии, напрямую не связанные с корпорациями. Это не чисто российская, а мировая задача, и решать ее можно только за счет обеспечения прозрачности, дисциплины и взаимного перекрестного контроля всех участников проекта.

Национальная задача освоении Арктического ценоза и реализация там технологического пакета Третьей индустриальной революции не должна быть поставлена под сомнения в случае неблагоприятного изменения цен на энергоносители. Существенный риск такого оборота событий есть. Однако задача освоения Арктического ценоза – это не задача года или даже десятилетия. Поэтому, на каком-то этапе надо быть готовым к тому, что освоение Арктического ценоза будет затратной задачей, когда государственные корпорации должны будут целевым образом датироваться. В этом смысле чрезвычайно важным и дальновидным является привлечение в качестве младших партнеров иностранных участников, которые заинтересованы в долговременном доступе к арктическим ресурсам, и которые могут разделить с нашей стороной бремя создания техноценоза в годы неблагоприятной рыночной конъюнктуры.

*Третье.* В ходе развертывания Третьей производственной революции в мире происходит отрезвление в отношении различного рода передовых технологий атомной энергетики. Целый ряд таких технологий, зачастую абсолютно без рекламы, а иногда и по возможности

скрытно, запущены в последние несколько лет в Соединенных Штатах, Франции, Великобритании, Китае. Речь идет в частности о ториевой энергетике, сверхмалых атомных реакторах и т.п. Здесь нельзя не отметить, что в отличие от других отраслей, в атомной промышленности удалось сохранить традиции знаменитого министерства среднего машиностроения под руководством Е.П. Славского. Нынешний Росатом без сомнения является мировым лидером и уверенно контролирует не только внутренний рынок, но и высококонкурентен за рубежом. В то же время, как в любой большой корпорации, текущие успехи и повседневная деятельность не всегда дают возможность развернуть передовые решения, за которые хватаются отстающие. Но здесь мы имеем дело не с технологическими, а с организационно-дисциплинарными вопросами. В России в атомной и близких к ней энергетических отраслях накоплен огромный потенциал принципиально новых проектов, которые находятся в высокой степени готовности, и при должной политической воле и неусыпном контроле, а также целевом выделении ресурсов на подобные проекты, они могут быть запущены и реализованы даже быстрее и лучше, чем их зарубежные аналоги. Поскольку за рубежом в значительной степени приходится начинать в этой сфере либо с нуля, либо использовать старые российские лекала.

Отдельная, принципиально новая задача связана с разворачиванием Третьей индустриальной революции по тем направлениям, в рамках тех кластеров и технопакетов, которые формируются в настоящее время на Западе и Востоке. Нашим большим преимуществом является то, что первоначальную работу, что называется, нулевой цикл осуществили за нас другие. Сегодня уже ясны магистральные направления Третьей производственной революции, ее основные кластеры, базовые технологии, квалификационные навыки, нужные для работы в новых условиях и т.п.

Для того чтобы максимально быстро и решительно начать эту работу в нашей стране нужны, прежде всего, организационные меры, а также изменения некоторых наших привычных поведенческих установок и взглядов.

Как отмечают практически все эксперты, всерьез занимающиеся как на государственном, так и на корпоративном уровне Третьей производственной революцией, ее основные кластеры начали формироваться еще в 70-е годы прошлого века и под воздействием стремительного развития информационных технологий на наших глазах превратились в единый технологический пакет.

Несмотря на все перипетии и неприятности, которые подстерегали российскую науку и технику, она не представляет абсолютно выжженной земли. Более того, в сфере информационных технологий нам есть чем похвастать. В этой связи нужно провести само собой разумеющееся мероприятие. Тем более что условия для него после ликвидации автономии РАН сложились благоприятные. Нет больше местничества, обособленности и стремления принизить внеакадемические научно-технические достижения. Нужно как можно скорее провести полную и детальную инвентаризацию действующих разработок и технологий, входящих в кластеры Третьей технологической революции, с определением по каждой технологии уровня ее готовности для практического использования и т.п.

Конечно, тонким моментом является всегда сама процедура оценки. Но в общем плане можно не мудрствуя лукаво, использовать мировой опыт. Главным оценщиком с точки зрения коммерциализации или практического применения должен стать конечный пользователь. В одних случаях им являются соответствующие государственные структуры, в других – заинтересованные представители бизнес-сообщества, в третьих – специалисты по коммерциализации технологий на внешних рынках. Конечно, никакая инвентаризация не проходит

без привлечения экспертов. Но здесь важно опираться не на различного рода охотников за грантами из российской юрисдикции, а в тех случаях, где нет ограничений по режиму секретности, широко привлекать практиков Третьей производственной революции из-за рубежа. Огромная фактография убедительно свидетельствует, что такие эксперты в подавляющем большинстве случаев не выступают в качестве промышленных шпионов, а напротив, выполняют функции менторов и консультантов. Примеры Сингапура, Малайзии, Бразилии – лучшие тому подтверждения.

Есть основания ожидать, что по целому ряду направлений Третьей производственной революции итоги инвентаризации внутренних научно-технических разработок окажутся неутешительными. Несмотря на несомненную печальность подобной констатации, в ней, вообще говоря, нет ничего страшного. Не так давно известный исследователь Эми Чуа опубликовала книгу «День империи», которая сразу же после выхода получила большую популярность в высоких политических и деловых кругах различных стран мира, включая Америку. Книга посвящена источникам мощи так называемых мировых «гипердержав». Американка китайского происхождения, профессор Йельского университета, установила, что одним из главных источников процветания империй является их открытость миру, терпимость и доброжелательность к иностранцам, готовность привлекать их на службу, брать из мира все лучшее, что в нем накоплено.

Собственно, для знатоков российской истории в выводах Эми Чуа нет ничего нового. Хорошо известно, что в Российской империи та же Екатерина Вторая активно привлекала в Российскую Академию наук лучших ученых мира, а для освоения богатых почв Новороссии и Поволжья всячески стимулировала крестьянскую миграцию из Германии. В годы российского экономического чуда 90-х годов XIX века в России трудилось много специалистов из стран Европы.

Есть и более близкие примеры. Уже долгие годы старательно скрывается роль зарубежного участия в советской индустриализации. Не то что книг, но и исторических публикаций, либо диссертаций на эту тему найти невозможно. Между тем, на стройках индустриализации трудились в общей сложности десятки тысяч инженеров, конструкторов, высококвалифицированных рабочих из многих стран мира. Десятки заводов были спроектированы в архитектурно-проектных фирмах Соединенных Штатов Америки. Сотни крупнейших советских предприятий были оснащены по последнему слову техники оборудованием ведущих американских, германских, британских и др. фирм.

Поэтому при решительном проведении в России Третьей производственной революции надо максимально широко использовать даже в нынешней сложной геополитической обстановке зарубежный опыт и возможности в самых различных формах. При этом, создание дочерних структур западных гигантов в России в сложившихся условиях является отнюдь не лучшей формой трансферта технологий Третьей производственной революции. Хорошо известно, что разработчиками этой технологической волны являются университеты, а также небольшие быстро развивающиеся компании, которые затем зачастую покупают гиганты, начиная от Google, заканчивая Lockheed Martin.

Никто не мешает российским структурам участвовать в скупке подобных компаний. Беспристрастный анализ публикаций о сделках на высокотехнологическом рынке Америки показывает, что в последние месяцы все чаще покупателями выступают, например, китайские, южнокорейские, бразильские компании. Вполне очевидно, что одним из магистральных направлений антироссийской политики США, и в значительной мере ЕЭС и Японии является ее необъявленная технологическая блокада. Но следует помнить, что даже в период наибо-

лее острой конфронтации США и СССР в годы «холодной войны» советской разведке удавалось вполне успешно быть в курсе последних технических достижений американских и европейских корпораций. В нынешнем, гораздо более распределенном и неоднородном мире идея полной технологической блокады России выглядит полной утопией. Вполне очевидно, что многие страны, с которыми Россия в настоящее время поддерживает добрососедские либо дружеские отношения, достаточно эффективно осуществляют трансферт технологий. Соответственно, это может быть использовано и для получения необходимых технологий или приобретения соответствующих компаний Россией. Кроме того, Третья производственная революция в значительной степени завязана не на фактор капитала, а на человеческий фактор, т.е. знания, умения, профессиональные навыки конкретных людей. А как известно из мировой истории, с людьми и их коллективами всегда проще договориться, чем с государствами и корпорациями. Поэтому в любых условиях важно сполна использовать мировой научно-технический потенциал, применив для этого методы, адекватные конкретной геополитической ситуации.

Разумное соединение внутреннего и внешнего потенциала Третьей производственной революции в условиях слабости препятствующих ей институциональных барьеров и групп особых интересов, позволит развернуть эту революцию в России более быстрыми темпами, чем во многих иных странах.

### 8.7. Третья производственная революция. Необходимые и достаточные условия

Необходимым условием решительного, а главное, результативного развертывания Третьей производственной революции в России является скорейшее освоение и практическое использование ее технологического пакета в экономики страны в целом, и особенно

в рамках Арктического ценоза. Дополнительным условием, своего рода неоценимым бонусом, может стать использование «закрывающих» технологий и реализация на их основе «русского технологического чуда».

Однако, при всей важности технологических аспектов, остается проза жизни, связанная с финансами, организационным обеспечением Третьей производственной революции.

В отличие от гиперрасходов, связанных с фантастическими планами создания в короткие сроки 25 млн. высокоавтоматизированных рабочих мест, которые заставляют задуматься о бессмертном творении Н. Гоголя, сама по себе Третья производственная революция – предмет экономически рентабельный и в относительно короткой перспективе самоокупаемый.

Однако в любом случае для старта технологических нововведений, особенно учитывая отсутствие развитой частной венчурной инфраструктуры, неизбежно потребуются немалые деньги. Причем вряд ли можно ожидать сколько-нибудь значительных отвлечений средств из государственного бюджета, который на долгие годы, вероятно, будет весьма напряженным в силу непредсказуемых цен на энергоносители.

В этой связи вряд ли стоит изобретать мудреные схемы, а лучше воспользоваться уже имеющимся отечественным и зарубежным опытом мобилизации ресурсов на высокотехнологичные проекты.

В течение текущего года будет принят пакет законов, предусмотренный в выступлении Президента РФ В.В. Путина, связанный с решительной деофшоризацией российской экономики. Цель законов, как известно, состоит в том, чтобы вывести бизнес из оффшоров и, помимо прочего, пополнить государственную казну.

На опыте борьбы с оффшорами государство наработало необходимый комплекс процедур, методов и нормативных подходов к исправлению ранее имевшихся

законодательных недочетов и порожденных ими различного рода злоупотреблений. Дело осталось за малым – распространить этот опыт на сферу финансирования технологического прорыва. Причем сделать это таким образом, чтобы не залезать в казну, не использовать дополнительные средства государственного бюджета.

Возможно ли это? Вполне. В России несколько структур прямо отвечают за технологическое развитие. Речь идет в первую очередь о «Роснано» и Сколково. Известно, что в ходе проведенного в 2013 году аудита Счетной Палаты выявлены огромные масштабы нецелевого использования средств крупнейшей государственной компанией «Роснано». Общий объем финансирования «Роснано» в 2007–2012 годах составил 259 млрд. рублей. Из них 227 млрд. – из госбюджета и под государственные гарантии. Результаты деятельности корпорации на сегодняшний день убыточны. Более 1,5 млрд. долларов было отправлено в различного рода зарубежные дочки, не имеющие никакого отношения к передовым технологиям. Из 22 проектов, проверенных аудиторами, которые составляют пятую часть от всех проектов компании, лишь один имел какое-либо отношение к передовым технологиям. Т.е. львиная доля средств, которые должны были пойти как раз на Третью производственную революцию, была использована на финансовые операции и проекты, никак не связанные с высокими технологиями. В том же прошлом году проверка Генпрокуратурой Сколково обнаружила нецелевое использование и хищение бюджетных средств в сумме более 125 млрд. рублей.

Очевидно, что проверки Генпрокуратуры и Счетной Палаты вскрыли только вершину айсберга. Но даже отмеченных выше средств вполне достаточно для успешного решительного и мощного запуска Третьей производственной революции.

Осталось только применить к «Роснано», Сколково и подобным структурам подход, опробованный на офф-

шорах. В конце концов, когда на кону стоит существование и процветание страны, главным является даже не наказание, а возврат средств и их целевое использование. В экономике, также как и в физике, действует закон сохранения. Только сохраняется не энергия, а деньги. И если с одного счета они «ушли», то на другой счет они обязательно «пришли». Поэтому главное в финансовом обеспечении Третьей производственной революции это – не наказание виновных, а деятельное исправление ими собственных ошибок путем возврата средств на исходные счета с последующим их перечислением в структуры, которые могут использовать эти средства подконтрольно и строго целевым образом.

Всему миру известно, что в Европе гремят футбольные клубы, купленные бывшими или нынешними российскими гражданами за счет продажи приватизационных активов или освоения государственных контрактов. Также не укрылись от российского населения многочисленные яхты, бороздящие просторы мирового океана, а также рекорды, которые бьют наши соотечественники на рынках недвижимости Лондона, Флориды и Лазурного Берега во Франции.

В то же время, когда в 2008 году Уоррен Баффет и Б. Гейтс выступили с инициативой пожертвовать как минимум половину своего состояния на благотворительные цели, немалая часть российских, даже серьезных экспертов разразилась статьями о том, что создается общемировой общак с тем, чтобы либо поработить человечество, либо истребить его на корню, либо заменить киборгами.

Между тем, не слишком сложно, обратившись опять же не к собственным домыслам и конъюнктурным фантазиям, а к фактическим материалам, установить, куда расходуются указанные деньги, какие проекты они финансируют. Кстати, среди участников этого фонда, деньги которого тратятся на благотворительные проекты ис-

ключительно за рубежом, есть и российские миллиардеры – В. Потанин и Б. Мильнер.

Надо сказать, что не всё с российскими миллионерами так плохо, как может показаться. Например, основатель знаменитого «Вымпелкома» Д. Зимин уже долгие годы значительную часть своих средств тратит на научные гранты, проведение бесплатных лекций и семинаров, издание научной литературы и т.п. В этой связи учитывая широко распространившееся в мире среди миллиардеров и миллионеров веяние благотворительности, представляется, что можно найти очень серьезных и влиятельных, чрезвычайно богатых людей, которым их коллегам было бы сложно отказать в просьбе создать российский благотворительный технологический фонд. При этом ключевым моментом должно стать то, что средства в этот фонд должны вносить все, кто получил сверхдоходы на приватизации и на работе с государством. Причем, распоряжаться этим фондом вероятно должно не государство, а какие-то другие структуры. Подобный опыт можно посмотреть в Америке в эпоху создания университетов. Помимо огромных средств для Третьей производственной революции это значительно улучшит социальный климат в России и преодолеет свойственную русской ментальности ненависть к богатым.

Конечно, важным является вопросы налогообложения компаний Третьей технологической волны, работающих в рамках Третьей производственной революции, включая «закрывающие» технологии. Принципиально, с некоторыми доработками для этих целей, вполне может подойти режим Сколково. В этом случае проекты, несомненно, послужат во благо России.

При желании можно найти и еще немалое количество вполне легитимных, строго соответствующих общепринятой мировой практике принципов и способов финансирования «русского чуда XXI века».

# ОГЛАВЛЕНИЕ

Елена Ларина, Владимир Овчинский

# КИБЕРВОЙНЫ XXI ВЕКА

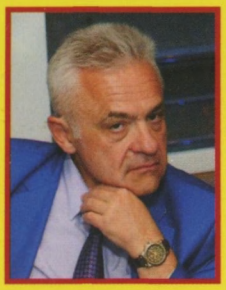
## О ЧЕМ УМОЛЧАЛ ЭДВАРД СНОУДЕН


Знак информационной продукции согласно
Федеральному закону от 29.12.2010 г. №436-ФЗ

Формат 84x108 1/32. Печать офсетная.
Бумага офсетная. Усл.печ.л. 11.
Заказ А-2097. Тираж 1500 экз.

ЗАО «Книжный мир».
Тел.: (495) 720-62-02 www.kmbook.ru

Отпечатано в полном соответствии с качеством
предоставленного электронного оригинал-макета
в типографии филиала ОАО «ТАТМЕДИА»
«ПИК «Идеал-Пресс».
420066, г. Казань, ул. Декабристов, 2.
E-mail: idelpress@mail.ru



**Овчинский Владимир Семенович** – советник Министра внутренних дел РФ, начальник Российского бюро Интерпола (1997–1999), доктор юридических наук, генерал-майор милиции в отставке. Постоянный член Изборского клуба. Автор книг – «Стратегия борьбы с мафией», «Основы борьбы с организованной преступностью», «Интерпол в вопросах и ответах», «Криминология и биотехнологии», «Криминология кризиса» и др.

**Ларина Елена Сергеевна** – предприниматель в сфере информационных технологий, член сообщества практиков конкурентной разведки, преподаватель Академии информационных систем, автор многочисленных статей в печатных и электронных СМИ. Эксперт Изборского клуба.

Мир на пороге великих перемен, имя которым – Третья производственная революция. И как любая другая революция, эта сопровождается войнами, переделом собственности и сменой господствующих элит. Только это – кибервойны, которые ведутся в Сети кибероружием за господство в будущем кибермире. Сможет ли Россия осуществить прорыв и сотворив «Русское чудо XXI века», занять достойное место в новом, цифровом мироустройстве или потерпит сокрушительное поражение на виртуальных полях сражений незримой Третьей мировой кибервойны и канет в Лету? Будущее покажет.

Каким это будущее может быть, читатель узнает из новой книги эксперта по конкурентной разведке Елены Лариной и известного российского криминолога, генерал-майора милиции в отставке, доктора юридических наук Владимира Овчинского.

www.kmbook.ru

ISBN 978-5-8041-0723-0

9 785804 107230

Изборский клуб