
ФАКУЛЬТЕТ
КИВИНО ГНЕЗДО
ГИГАБАЙТЫ ВЛАСТИ
Бёрд Киви
МОСКВА

Киви Берд

Гигабайты власти

«Городские и музейные технологии»

2004

Берд К.

Гигабайты власти / К. Берд — «Городские и музейные технологии», 2004

Автор складывает причудливую мозаику из вдумчиво проанализированных фактов новейшей истории общества и технологий. Насквозь лживая иракская авантюра США, взломы сетей GSM и систем спутникового телевидения, нездоровый ажиотаж вокруг биометрии и методов тоталитарного контроля за гражданами во имя борьбы с международным терроризмом оказываются тесно связанными друг с другом. Современное общество стоит перед выбором: как использовать технологии для собственного развития.Для думающих людей.

Содержание

Берд Киви
Гигабайты власти. Информационные технологии между свободой и тоталитаризмом

Остальные, правда, предпочитали молчать, а коринфянин Сокл сказал вот что: «Поистине, скорее небо провалится под землю, а земля поднимется высоко на воздух над небом, скорее люди будут жить в море, а рыбы – там, где раньше жили люди, чем вы, лакедемоняне, решитесь уничтожить свободу, восстановив господство тиранов в городах. Нет ведь на свете никакой другой более несправедливой власти и более запятнанной кровавыми преступлениями, чем тирания».
Геродот. История

Все имена и события, упомянутые в книге, являются подлинными. Любое совпадение с вымышленными персонажами и сюжетами, надо полагать, неслучайно.

Глава 0
Вчера—сегодня—завтра

Страницы жизни героя, 1895
Самая знаменитая сточная яма США

Воскресным днем 1 января 1895 года в половине восьмого утра, в нескольких кварталах от вашингтонского Капитолия, в доме своих родителей на свет появился Джон Эдгар Гувер. Во всяком случае, так принято считать со слов самого Гувера, а он хорошо известен тем, что постоянно врал всю свою долгую жизнь.

Но, конечно же, это не самая главная особенность человека, вошедшего в мировую историю как самый знаменитый полицейский Соединенных Штатов Америки. Дж. Эдгар Гувер возглавил ФБР в возрасте 29 лет и умудрился сохранить свой пост на всю остальную жизнь. Его цепкие лапки, ухватившие кормило столь влиятельного в государстве органа, разжались лишь в результате естественной смерти, наступившей в возрасте 77 с лишним лет в мае 1972 года.

Несмотря на все демократические порядки «самой свободной страны мира», издавна практикующей профилактическую ротацию руководящих кадров, Гувер за почти полвека своего директорства в ФБР пересидел 8 президентов и 18 генеральных прокуроров. Достигнут же столь выдающийся результат был старым как мир способом – тщательным сбором и умелым использованием компромата на всех потенциальных противников, начиная с самых высших лиц государства и кончая любым мало-мальски известным журналистом.

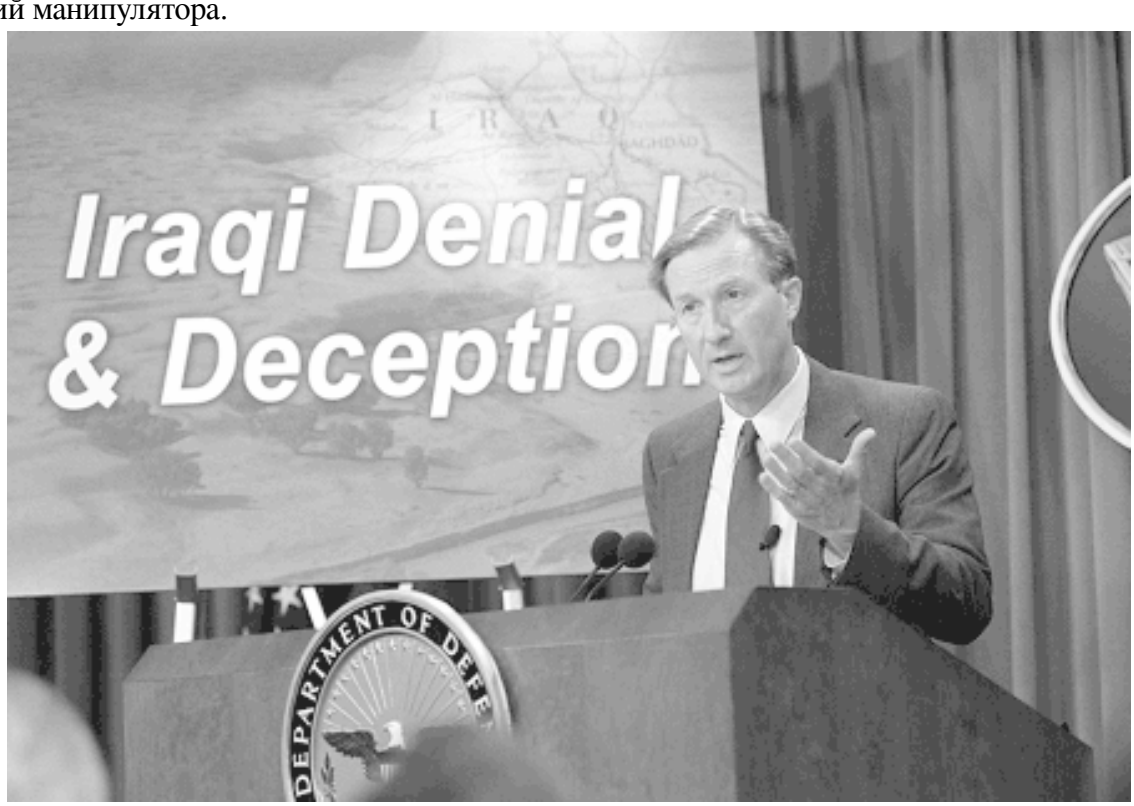
Когда в 1960-е годы президента Линдона Джонсона в очередной раз спросили, доколе страна будет все это терпеть, тогдашний хозяин Белого дома произнес бессмертную фразу: «Таких людей как Гувер предпочтительнее держать внутри палатки, чтобы он мочился наружу, а не снаружи, чтобы он писал внутрь»…

Тема испражнений, судя по всему, возникала в связи со специфической личностью Гувера регулярно и как бы сама собой. Так, уже после кончины непотопляемого директора ФБР, когда в 1974 году были обнаружены некоторые из его «секретных файлов» с компроматом, судья Лоуренс Зильберман, исполнявший в ту пору обязанности министра юстиции, высказался следующим образом: «Джон Эдгар Гувер был словно сточная яма, накапливающая грязь. Сейчас я полагаю, что он был самым худшим государственным деятелем за всю нашу историю».

Обман и Отрицание

В процессе пропагандистской подготовки военного вторжения США в Ирак, 8 октября 2002 года в американском Министерстве обороны было проведено на редкость интересное мероприятие. В этот день Пентагон устроил для прессы специальную презентацию, целиком посвященную методам «отрицания и обмана», практикуемым Ираком для сокрытия своего оружия массового поражения и баллистических ракет, как средств его доставки. Доклад-презентацию провел один из ответственных чинов РУМО, Разведывательного управления Министерства обороны США, доктор Джон Юречко. Личность докладчика здесь весьма показательна, поскольку Джон Юречко не является специалистом ни по баллистическим ракетам, ни по оружию массового уничтожения. Этот представитель разведслужбы, уже не в первый раз выступающий перед журналистами, является начальником отдела по методам ведения информационной войны или, говоря попросту, специалистом по дезинформации..[1]

Имеет смысл пояснить, что конкретно принято понимать под «ОиО», т. е. «отрицанием и обманом» (по-английски «D&D», или Deception and Denial). В сущности, ничего особого хитрого за данным термином не скрывается и, как заметил тот же Юречко, эти методы так же стары, как и вся зафиксированная история человечества. Вкратце, под «отрицанием» понимаются такие методы, которые используются страной для утаивания своих государственных и военных секретов, в частности, от устремлений зарубежных разведок. «Обман», в свою очередь, это манипуляция информацией и восприятием для того, чтобы вынудить обманываемые государства к определенным действиям или, наоборот, к бездействию, в зависимости от намерений манипулятора.



Джон Юречко

[1] [KR02], полное название источников см. по указателю в конце книги

Понятно, что обман и отрицание взаимосвязаны. Отрицание – это базис для успешных операций по обману. Невозможно манипулировать истиной и ложью до тех пор, пока истина предварительно как следует не замаскирована. Понятно и то, что спецслужбы США являются чрезвычайно искушенными в «ОиО», умудряясь в течение многих лет весьма успешно скрывать многомиллиардные разработки нового оружия или масштабные тайные операции в разных регионах планеты. Но доклад Джона Юречко, ясное дело, был посвящен не этой стороне его работы, а методам «ОиО», успешно применявшимся Ираком для обмана зарубежных разведслужб и инспекторов ООН.

Хотя, по оценкам этого искушенного эксперта, действия Ирака в области «ОиО» зачастую выглядели довольно топорно, тем не менее Юречко вынужден признать, что они успешно помешали как международным инспекторам, так и западной разведке представить хоть сколько-нибудь серьезные свидетельства или фотографии, способные убедить скептиков в нарушении Саддамом Хусейном резолюций ООН, запретивших создание оружия массового поражения. По сути дела, с тех пор как предыдущая смена инспекторов ООН покинула Ирак в 1998 году, в этой стране так и не удалось выявить ничего по-настоящему компрометирующего. Тем не менее, специальный отчет ЦРУ, представленный политическому руководству США непосредственно накануне презентации Юречко, утверждал, что Багдад по-прежнему утаивает крупные программы по созданию ОМП.

В докладе Юречко эти выводы разведки были обоснованы весьма специфическим образом – длинным перечислением прошлых грехов режима Саддама Хуссейна, которых действительно было в достатке. После чего сделан элегантный переход к нынешним, как следует понимать, методам обмана, что надо процитировать дословно: «Вот один из типичных и относительно нехитрых методов „ОиО“, а именно маскировка. На этом слайде – пример предполагаемого иракского объекта, где создается биологическое оружие. Посмотрите внимательно на это фото. Одна из интересных особенностей объекта – его местоположение. Он замаскирован посреди жилого района. Здания ничем не выдают себя по внешнему виду. В объекте вообще нет ничего примечательного»…

На этом месте, казалось бы, Юречко должен был поведать о том, как доблестная разведка все же сумела выявить опаснейшую фабрику смертоносных вирусов в жилом квартале ни о чем не подозревающих мирных людей. Но вместо этого лектор многозначительно цитирует знаменитый афоризм покойного Амерона Кэппса, эксперта по контролю за вооружениями, который однажды изрек: «Мы никогда не находили ничего из того, что наши противники успешно скрывали». Из чего внимательный слушатель легко сделает вывод, что никакого биологического оружия разведка в действительности не выявила. Ни в этом жилом квартале, ни где-либо еще.

Но сам Юречко, конечно, ничего подобного не произносит, зато тут же приводит другую цитату, на этот раз из высказываний Тима Тревэна, бывшего инспектора ООН, который как-то изрек, что если в стране существуют недекларированные и невыявленные объекты оружия массового уничтожения, то их по определению невозможно инспектировать или отслеживать. А значит, делает вывод докладчик, практика инспекций не может дать никаких гарантий того, что страна не занимается запрещенной деятельностью.

Короче говоря, весь большой доклад доктора Юречко с убедительной демонстрацией спутниковых снимков, не доказывающих, по сути, абсолютно ничего, сам по себе стал классическим примером дезинформационной операции государства по обману и отрицанию. Обману собственного народа об истинных целях уже подготовленной иракской войны и отрицанию вполне очевидного факта – что у американских спецслужб нет ни одного убедительного доказательства нарушений Саддамом Хусейном резолюций ООН. А у США, соответственно, ни единой достойной причины для развязывания войны и убийства тысяч ни в чем не повинных людей.

Да и могут ли вообще существовать для этого достойные причины?

Одной ногой в будущем

Действие недавнего фильма Стивена Спилберга «Особое мнение» (Minority Report) происходит в 2054 году. Если кто почему-либо не в курсе, то это – фильм-предупреждение, фильм об обществе, тотально контролируемом органами безопасности. Об обществе, граждане которого практически полностью утратили тайну личной жизни. Режиссер вынашивал замысел этой картины не один год и, стремясь как можно более убедительно изобразить даже мелкие бытовые реалии сравнительно недалекого будущего, специально созывал в 1999 году на трехдневный коллоквиум две дюжины известных футурологов. В ходе того своеобразного «мозгового штурма» была сделана попытка набросать наиболее вероятные черты технологий грядущего.

Стивен Спилберг

Споры, как вспоминает Спилберг, были самые яростные, и все же в некоторых своих прогнозах футурологи оказались на редкость единодушны. Например, в том, что техника будущего непременно будет настраиваться индивидуально на каждого конкретного человека. Естественно, эта идея не могла не найти яркого отражения в кинокартине. А чтобы стало ясно, насколько быстро прогнозы визионеров воплощаются в жизнь, достаточно лишь взглянуть на небольшой тест, предложенный в 2002 году читателям одного из популярных изданий в связи с выходом на экраны фильма Minority Report. Спрашивается, какие технологии уже реализованы, а какие появятся в обозримом будущем:

• банкомат, предоставляющий клиенту банка доступ к его счетам путем сканирования радужки глаза;

• кассовый аппарат в супермаркете, позволяющий оплатить покупку бакалейных товаров простым прикосновением пальца к биометрическому сенсору;

• электронные журналы, мгновенно доставляющие читателям интересующие их новости по беспроводным сетям;

• голографические рекламные щиты, обращающиеся по имени к оказавшемуся поблизости прохожему.

Две первые технологии уже реализованы сегодня, две следующие показаны в MR, причем третья – уже на подходе, и лишь четвертая ожидает нас, вероятно, в грядущем. Тенденция все более глубокой «персонализации обслуживания» вполне отчетливо обозначена в нынешних высокотехнологичных продуктах. Например, персональные видеорекордеры (PVR) вроде тех, что изготовляют компании TiVo и SonicBlue, умеют по-тихому собирать данные об индивидуальных предпочтениях своих владельцев, предоставляя возможность рекламодателям более конкретно и целенаправленно адресовать свои обращения к зрителям. А следующее поколение сотовых телефонов оснащается функциями точного географического позиционирования, давая магазинам потенциальную возможность зазывать находящихся поблизости прохожих, суля им заманчивые, но краткосрочно действующие бонусы и скидки в течение ближайшего получаса. Текущие социологические исследования показывают, что ради какой-нибудь постоянной 10–15-процентной скидки большинство рядовых потребителей готово с радостью отказаться чуть ли не от всех своих прав на тайну личной жизни, предоставив торговцам любую интересующую их информацию – о вкусовых предпочтениях, ближайших планах, распорядке дня, кредитоспособности и так далее.[2]

Всякому, кто внимательно наблюдает за происходящим, достаточно очевидно, что благодаря технологиям тайна личной жизни размывается и исчезает не только для настырной коммерции. Жизнь людей становится все прозрачнее и для не менее (скорее, более) любопытных правоохранительных органов, понемногу обретающих возможность проконтролировать каждого человека практически в любом месте и в любой момент времени. Только в этом случае роль «морковки», обеспечивающей добровольный отказ от прав на свободу, играют уже не скидки-бонусы, а некая гипотетическая «всеобщая безопасность», гарантируемая пастырями от власти своему безразлично-согласному стаду.

У многих есть ощущение, что все мы одной ногой уже вступаем примерно в то будущее, которое изобразил Спилберг в MR. Сам режиссер не скрывает, что всерьез озабочен ходом реальных событий, и честно признается, что побаивается реальности нарисованных картин будущего: «Предсказания Джорджа Оруэлла сбываются, но не в XX, а в XXI веке. Большой Брат уже следит за нами, и та небольшая приватность, которая есть у нас сейчас, полностью испарится лет через 20-30, потому что технология позволит смотреть сквозь стены и крыши, заглядывать в самые сокровенные тайны нашей личной жизни, в святая святых семьи».[3]

Никто, наверное, не станет сегодня утверждать, что страхи Спилберга абсолютно безосновательны. И картины-предупреждения, подобные Minority Report, время от времени создавать необходимо уже затем, чтобы люди наглядно видели, куда способен увести общество неудержимый прогресс технологий.

Однако, имеет смысл всегда помнить, что никакой консенсус даже самых авторитетных футурологов планеты не в силах предсказать реальное будущее человечества. Ведь самая главная особенность нашей истории – это ее полнейшая непредсказуемость. Достаточно вспомнить события бурного XX века. Столь радужные надежды на торжество прогресса, науки и просвещения в самом начале столетия, а вместо этого – чудовищная по масштабам жертв и разрухи мировая война. Через пару десятков лет – еще одна, даже более страшная глобальная бойня. В середине века – мир, расколовшийся на два непримиримых враждующих лагеря и подготовка к третьей, теперь уже ядерной мировой войне. А вместо этого – еще через полстолетия – фактически полный, никем не предсказанный коллапс коммунистической системы, глобализация экономики и единое информационное пространство планеты.

---

[2] [FS02]

[3] [BW02]

В данной книге не дается никаких предсказаний на будущее. Но здесь достаточно тщательно собраны факты о реальных возможностях, недостатках и перспективах современных информационных технологий, столь серьезно влияющих ныне на развитие человеческого общества. И среди этих фактов время от времени непременно мелькают и такие, что окажут очень серьезное воздействие на мир, каким он станет еще через 50 лет.

Глава 1
Матрица, ее мутанты и хакеры

СЖГ, 1917
Лучше бы он остался библиотекарем

В июле 1917 года Эдгар Гувер закончил юридический факультет Университета Джорджа Вашингтона и в том же месяце по протекции дяди-судьи начал работу в Министерстве юстиции США. Все четыре года в университете Гувер учился по вечерам, а днем должен был работать – курьером в Библиотеке Конгресса, – поскольку семья постоянно испытывала серьезные денежные затруднения из-за плохого здоровья отца, Дикерсона Гувера.

Карьера Гувера в министерстве развивалась стремительно. Всего через два года тогдашний генеральный прокурор Александр Палмер сделал смышленого молодого человека своим помощником по особым поручениям. В этой должности Гувер стал отвечать за новое подразделение, Отделение общей разведки, сформированное для сбора информации на «революционные и ультрареволюционные группы». Эта работа, по сути дела, идеально подошла Гуверу, поскольку тот всегда получал огромное удовольствие от составления картотеки на книги личной библиотеки и от работы с каталогами огромного книгохранилища Библиотеки Конгресса. Теперь он получил возможность использовать свой большой опыт для составления огромной картотеки на коммунистов, анархистов и прочих левацких «подрывных элементов».

В течение нескольких лет под руководством Гувера была составлена гигантская проиндексированная картотека почти на полмиллиона (450 тысяч) имен людей предположительно левых убеждений. Примерно на 60 000 из них, расцененных Гувером в качестве наиболее опасных, были собраны подробные биографические данные. С юных лет напуганный красной угрозой, Гувер убедил Палмера, что всех подобных людей необходимо хватать и высылать из США. В день второй годовщины русской Октябрьской революции, 7 ноября 1919 года, полиция одновременно арестовала в 23 городах свыше 10 000 человек, подозревавшихся в большевистских, анархистских и прочих леворадикальных взглядах. Аресты сопровождались побоями и чрезвычайно жестоким обращением, войдя в историю как один из наиболее, вероятно, чудовищных прецедентов нарушения гражданских прав в США в XX веке. Подавляющее большинство арестованных были американскими гражданами, выслать их из страны не было никаких оснований, так что в конечном итоге власти были вынуждены их отпустить. Но Эдгар Гувер в результате получил в свое распоряжение имена сотен адвокатов, вызвавшихся представлять интересы арестованных в суде. Всех этих адвокатов, так же как и журналистов, и всех прочих, подавших голос сочувствия в адрес репрессированных, также занесли в постоянно растущую базу данных.

Когда в 1921 году Отделение общей разведки вошло в состав Бюро расследований Министерства юстиции, Гувера произвели в заместители директора Бюро. В 1924 году он уже сам стал директором, постоянно озабоченным улучшением информационного обеспечения расследований. В 1926 году Эдгар Гувер создал в Бюро базу отпечатков пальцев, которая со временем стала самым большим в мире хранилищем подобного рода.

В 1975 году, три года спустя после смерти Гувера, американский Конгресс отдал распоряжение произвести тщательную проверку всех досье по тематике «внутренняя безопасность», хранящихся в десяти основных управлениях ФБР. В результате этой проверки выяснилось, что свыше двадцати процентов всех усилий Бюро было направлено на охоту за предположительно «подрывными элементами». Причем реальный криминал был обнаружен лишь в четырех из

девятнадцати тысяч семисот расследований, да и выявленные четыре случая не имели ничего общего с национальной безопасностью, шпионажем или терроризмом.

Похоже, для США было бы гораздо лучше, если бы Эдгар Гувер так и остался библиотекарем.

Матрица – перезагрузка TIA

Явление TIA

В ноябре 2002 года мир узнал о новой, чрезвычайно амбициозной инфотехнологической программе Пентагона, получившей название «Тотальная информационная осведомленность» или кратко TIA, от Total Information Awareness. Целью этой программы, запущенной в Агентстве передовых военных исследований (DARPA), виделось создание гигантской компьютерной системы для наблюдения за многими миллионами граждан США и других стран мира – для предотвращения, как объявлено, будущих террористических актов на этапе их подготовки. Под «наблюдением» здесь понимаются постоянные анализ и оценка данных из множества сведенных воедино информационных баз, правительственных и коммерческих, содержащих самые разные сведения о личной жизни граждан по всему миру.

Для общего руководства проектом в DARPA было создано специальное Управление информационной осведомленности, возглавил которое адмирал Джон Пойндекстер, в свое время получивший очень громкую скандальную известность в качестве советника по национальной безопасности президента Рейгана. По словам Пойндекстера, его задача – создать новую технологию для эффективного просеивания информации, накапливаемой в «сверхбольших» хранилищах данных и в объединенных сетью компьютерах. Такая технология позволит отыскивать характерные следы назревающих угроз среди множества ежедневных транзакций – покупок литературы или химикатов, бронирования билетов или мест в гостинице, обращения к врачам или консультантам. Власти уже достаточно давно имеют доступ к массе всевозможной информации о деятельности конкретных установленных террористов, но для этого, говорит Пойндекстер, каждый раз приходится либо получать ордер в суде (на территории США), либо предпринимать достаточно утомительные усилия по дипломатическим или разведывательным каналам (за рубежом). Новая же система TIA, как виделось ее создателям, позволила бы достигать нужных целей намного более эффективным способом.[4]

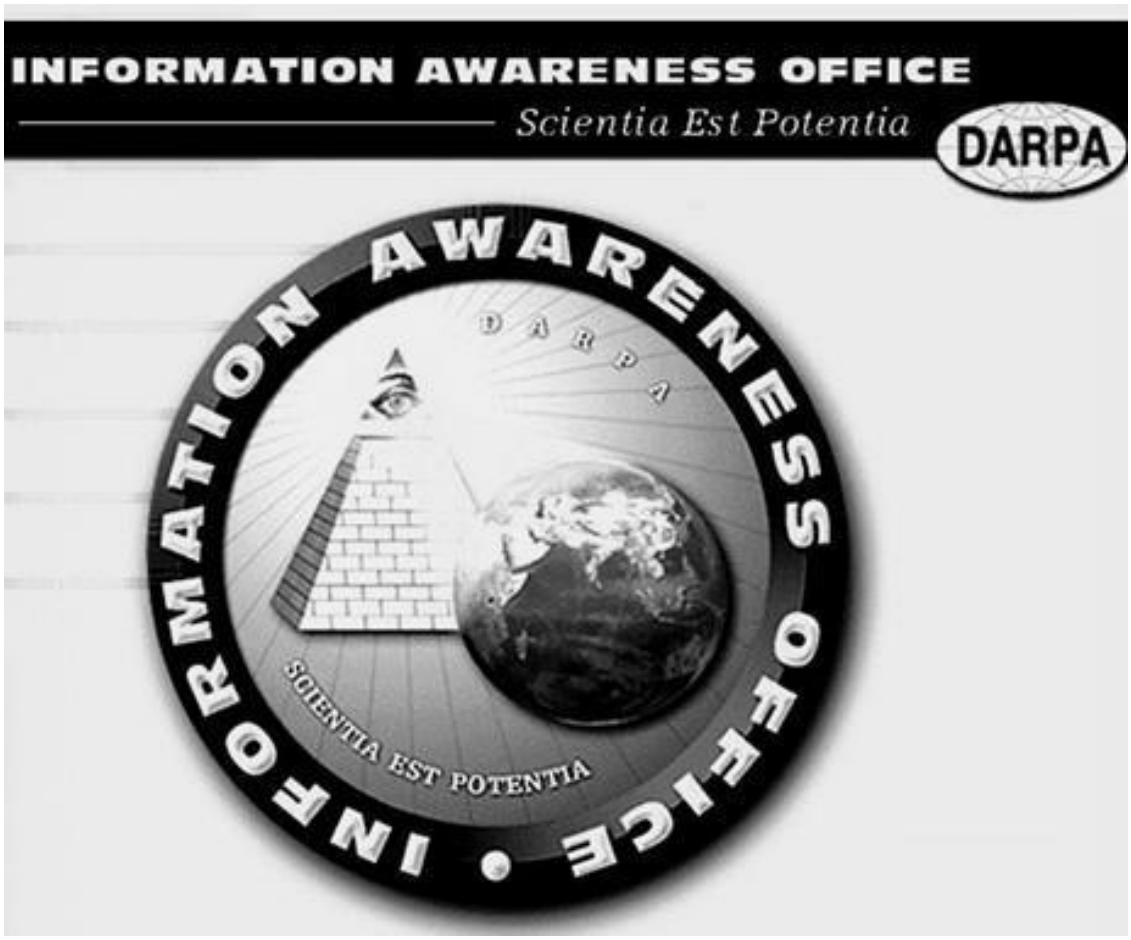
Суть новой технологии не столько в отслеживании уже известных людей, догадывающихся, возможно, что за ними следят, сколько в выявлении «подозрительных» структур в поведении всех людей вообще. Иначе говоря, всякий заказ по кредитной карте, всякая подписка на журнал или газету, всякий выписанный рецепт на медикаменты, всякий веб-сайт, посещаемый в Интернете, всякая электронная почта, входящая или исходящая, всякий взнос в банк или съем денег, всякая запланированная поездка – все эти данные, фиксируемые в каких-то базах данных, становятся предметом пристального интереса спецслужб и объектом обработки для их специального аналитического инструментария.

Вдохновленные грандиозностью задачи, создатели TIA украсили, как смогли, свой вебсайт богатой и многозначительной символикой. В качестве эмблемы проекта был выбран древний масонский знак «всевидящего ока» – глаз в вершине пирамиды, пристальным взором осматривающий земной шар. Девиз тоже подобрали подходящий – латинское изречение Scientia Est Potentia (Знание – сила), обычно приписываемое Фрэнсису Бэкону.

Чего же не удалось предусмотреть искателям «тотального знания-силы», так это в высшей степени негативной реакции общественности на программу TIA. Мало того, что создается технология для грандиозного вторжения государства в частную жизнь граждан, так еще во главе проекта поставили отъявленного прохиндея и лжеца Пойндекстера. Тут же всплыли все известные нелицеприятные факты из биографии отставного адмирала. Как бывший глава

[4] [RO02]

совета национальной безопасности в рейгановской администрации, Джон Пойндекстер в 1990 году был осужден федеральным судом по пяти уголовным преступлениям, включая ложь в показаниях Конгрессу, уничтожение компрометирующих официальных документов и препятствование парламентскому расследованию в деле «Иран-Контрас». Пойндекстер был одной из центральных фигур в этом самом громком политическом скандале США 1980-х годов, включавшем тайную продажу оружия Ирану с переводом полученных денег на помощь контрреволюционному движению в Никарагуа, активное участие ЦРУ в подпольном наркобизнесе и другие нелегальные формы деятельности спецслужб для тайного финансирования своих операций. Покидая Белый дом, президент Джордж Буш-папа, сам в прошлом директор ЦРУ, амнистировал всех, кто был осужден по этому громкому делу, а многие шокирующие подробности этой истории так и не стали достоянием широкой общественности.



Исходный вид оформления веб-сайта TIA

В TIA достаточно быстро поняли, что затеянная работа была подана неудачно – и уже в декабре интернет-публика стала отмечать заметные косметические коррективы в оформлении веб-сайта проекта. Сначала исчезли биографии главных создателей программы, затем существенно сократился перечень конкретных типов данных, просеиваемых фильтрами TIA. Наконец, к концу декабря, вместе с другими содержательными деталями исчезла и «тайно-масонская» эмблема с пирамидой и земным шаром. Сам же проект, тем не менее, продолжал развиваться своим ходом, но теперь в менее доступной взору общественности форме.[5]

[5] [DM02]

Подозреваются все

В апреле 2003 года стали известны некоторые подробности о том, как происходит наполнение централизованной базы данных файлами со списками потенциально «неблагонадежных» граждан. В Нью-Йорке забили тревогу правозащитники, установившие, что полиция, в массовых количествах арестовывавшая участников демонстраций против войны в Ираке, задерживала людей в участке, если те отказывались помимо обычных имени и адреса сообщать о себе массу дополнительных сведений: где они учились, членами каких организаций состоят, участвовали в акциях протеста прежде и так далее. Здесь уместно вспомнить, что согласно официальным статистическим данным в 2002 году в тюрьмах США содержалось свыше 2 миллионов граждан страны, что при населении 286 миллионов составляет около 0,7 % от общего числа. Для сравнения в Китае, который многими расценивается как авторитарное полицейское государство, насчитывается 1,4 миллиона заключенных при населении 1,3 миллиарда, т. е. около 0,1 %.[6]

Для повышения эффективности «поиска врагов» в марте 2003 г. Министерство юстиции США существенно понизило планку достоверности информации, вносимой в национальную базу данных о преступности NCIC (National Crime Information Center). До введения новых правил там содержалось 39 миллионов записей о зарегистрированных преступлениях и преступниках, теперь же туда вносится не только абсолютно достоверная информация, но и непроверенные сигналы, расценивающиеся как серьезные. Помимо этого, в ФБР составлен совершенно необозримый список «подозреваемых в терроризме», состоящий из 13 миллионов человек, т. е. почти 5 % от всего населения США. Сведущие люди, умеющие считать, тут же несложными арифметическими калькуляциями наглядно продемонстрировали, сколь нелепы попытки пристально следить за 1/20 долей страны и к сколь чудовищным ошибкам это будет постоянно приводить.[7]

Подобные расчеты, однако, убеждают кого угодно, но только не тех, кто формирует тотальную супербазу. Весной 2003 года стало известно, что едва ли не за год до объявления инициативы TIA по заказу правительства американские частные компании интенсивно, тайно и в массовых объемах начали скупку информации о гражданах иностранных государств. В частности, фирма из Атланты ChoicePoint продала «заинтересованным правительственным ведомствам» США свыше сотни миллионов собранных ею записей о гражданах Бразилии, Мексики, Колумбии, Венесуэлы, Коста-Рики, Гватемалы, Гондураса, Сальвадора, Никарагуа. Понятно, что ChoicePoint специализируется на государствах Латинской Америки, но наверняка есть и другие фирмы, специализирующиеся на прочих регионах планеты. Ведь теперь фактически вся заграница – это потенциальная угроза Америке.[8]

Больной скорее жив, чем умер

Трудно сказать, чем именно система TIA не понравилась американским конгрессменам, но летом 2003 года стало понятно, что будущее программы далеко не столь радужно, как виделось ее идеологам. Пытаясь спасти ситуацию, они и название сменили на менее вызывающее – теперь уже не тотальная, а «Информационная осведомленность о терроризме» (Terrorism Information Awareness). И начальника программы сменили, вновь убрав в тень одиозную фигуру адмирала Пойндекстера. Ничего не помогло – система TIA так и не смогла стяжать

[6] [NY03],[PS02]

[7] [BS03],[JM03]

[8] [FC03]

ничего, кроме чрезвычайно негативной прессы и критических отзывов конгрессменов, усмотревших в гипер-базе данных чистую оруэлловщину и отчетливые контуры тоталитарного Большого Брата.

Официальная смерть TIA наступила 24 сентября 2003 года. В этот день на совместном заседании обеих палат американского Конгресса большинством голосов было принято решение о полном лишении финансирования в 2004 году как программы TIA, так и ее организующей структуры – Управления информационной осведомленности. Правда, в действительности столь эффектное решение вовсе не означало прекращение разработки комплекса исследовательских проектов, входивших в состав TIA. Просто их раскидали по другим управлениям и агентствам. В результате ситуация стала скорее даже хуже, чем была, поскольку работы государства, сосредоточенные на копании в личной жизни граждан и попавшие под огонь критики, теперь стали практически невидимыми для публики. А значит, и намного меньше доступными для контроля со стороны общества.

Отныне известно лишь то, что восемь самостоятельных программ, входивших в состав TIA, будут продолжены в других подразделениях DARPA, т. е. их финансирование просто будет осуществляться по другим каналам. Кроме того, родственные исследования будут осуществляться в рамках значительно более скрытной программы спецслужб, известной под названием NFIP или National Foreign Intelligence Program. Эту программу совместно ведет целая группа таких агентств, как Центральное разведывательное управление, Федеральное бюро расследований и Агентство национальной безопасности. Бюджет программы полностью засекречен, также как и подробное раскрытие целей совместной работы, скрываемой за набором примерно таких слов – «инструментарий для обработки, анализа и совместных действий в контртеррористической внешней разведке». В соответствии с новыми законами США, следует напомнить, теперь ничто не мешает использовать любые инструменты NFIP и внутри страны.[9]

MATRIX сегодня – это TIA вчера

Случайно или нет, но ровно через год после явления народу TIA, в ноябре 2003 стало известно о новой реинкарнации той же самой, в сущности, идеи, но теперь уже под видом не государственной, а коммерческой программы. Программа носит на редкость подходящее название MATRIX, как акроним полного названия – **M**ultistate **A**nti-**Ter**rorist **I**nformation e**x**change, т. е. «Антитеррористический информационный обмен множества штатов». Согласно ее создателю, флоридской компании Seisint, MATRIX представляет собой крупнейшую на этой планете базу данных, содержащую на тот момент свыше 20 миллиардов записей. Работая совместно с Департаментом правоохранительных органов Флориды (FDLE) и получив 12 миллионов долларов из федерального бюджета, фирма Seisint разрабатывала MATRIX так, чтобы система могла накапливать досье на каждого отдельно взятого гражданина страны. Естественно, вся работа затеяна лишь для того, чтобы помочь стране в борьбе с терроризмом. Ну а попутно, как приятный бонус, эта же система поможет эффективно выявлять бандитов, рэкетиров, мошенников и прочих педофилов.

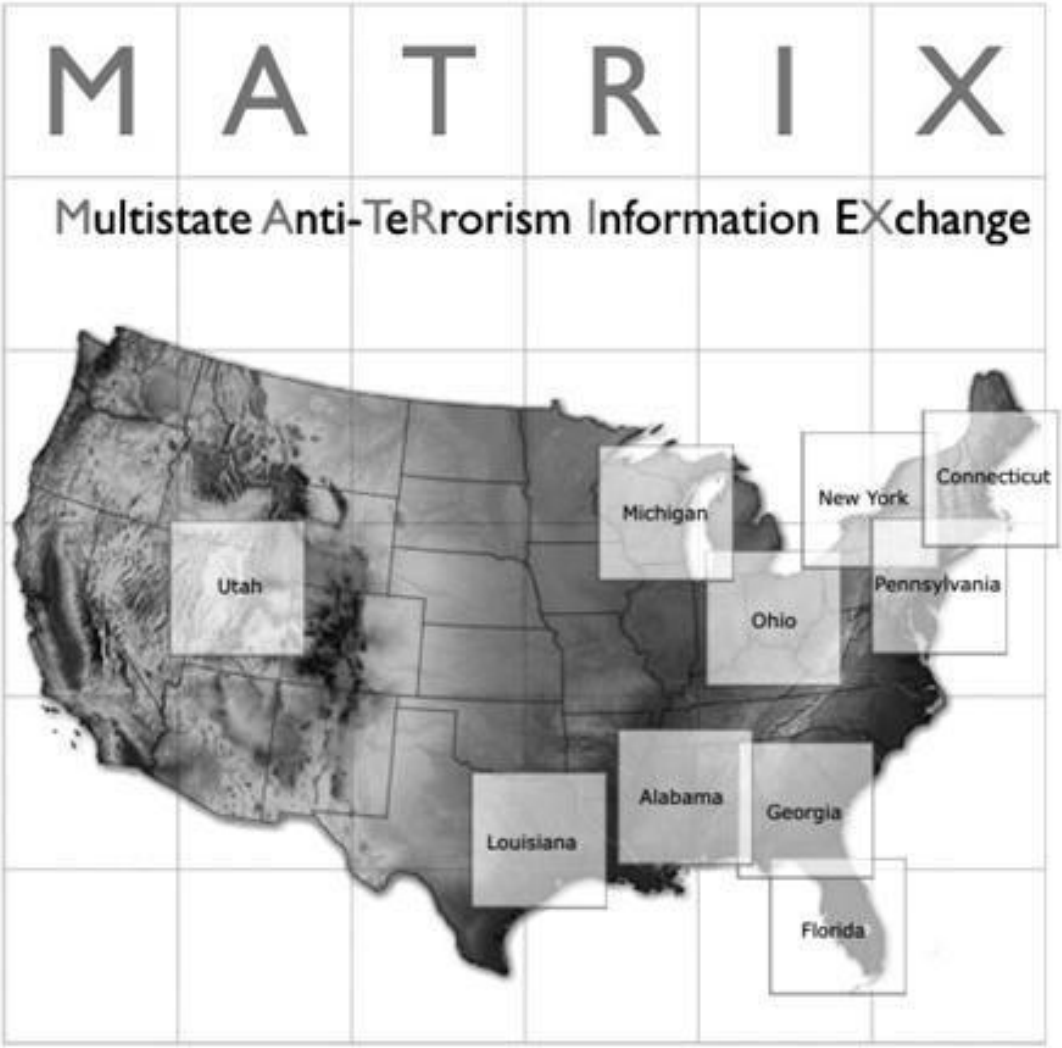
Небезынтересно отметить, что MATRIX имеет большое сходство с TIA не только в функциональной части, но и в крайне сомнительном моральном облике главного инициатора проекта. Человек, стоящий за MATRIX – это весьма состоятельный флоридский предприниматель Хэнк Эшер, щедрый спонсор нынешнего политического руководства штата (губернатор Флориды Джеб Буш – брат 43-го и сын 41-го президентов США) и большой друг недавно ушедшего на пенсию главы FDLE. А кроме того, как недавно выяснилось, в начале 1980-х годов – актив-

[9] [SC03]

ный наркодилер, лично доставивший в США из Колумбии несколько самолетов, загруженных кокаином (этим бизнесом, напомним, активно занималось в ту пору ЦРУ).

Общенациональное расширение флоридской компьютерной базы Seisint, поначалу созданной для FDLE, происходило примерно по следующей схеме. Администрациям других штатов предлагалось за свой счет прислать имеющиеся у них файлы с данными обо всех выданных водительских лицензиях, обо всех зарегистрированных машинах, а также имеющие архивы о криминальной деятельности. В Seisint смешивают их с аналогичными данными других штатов и со всеми «коммерческими» базами данных, которые компания уже успела приобрести и скомпилировать. После чего вновь подключившийся штат получает доступ ко всему хранилищу, но не бесплатно, а, скажем, за полтора миллиона долларов в год.

В результате, как обещают в Seisint и FDLE, пользователь MATRIX элементарным нажатием кнопки получает доступ к самой разнообразной информации на интересующих людей: номера социального страхования, фотографии, даты рождения, нынешние адреса и старые адреса за последние 30 лет, телефонные номера и имена других людей, живущих по тому же адресу и по соседству. А также: заявления на получение кредита и отчеты по выплатам, описание принадлежащей собственности, когда и где она куплена, сколько и кому уплачено вместе с суммами выплаченных налогов, история нарушения правил при вождении транспортных средств с полной информацией о правах и зарегистрированных на это имя машинах. Ну, и так далее, включая всю перечисленную информацию о родственниках, близких и соседях.



География «Матрицы»

Трудно сказать, как далеко в другие штаты успела бы распространить свои сети система MATRIX, если бы информация о ней не начала появляться в прессе, породив журналистские расследования. Именно одна из флоридских газет раскопала материал о криминальном прошлом Хэнка Эшера, после чего тот резко разорвал все связи с компанией Seisint. Но волна уже пошла, и местные власти ряда штатов начали забирать обратное данное поначалу согласие. Так, после поднятого журналистами шума генеральный прокурор Джорджии постановил, что передача на сторону информации о водительских лицензиях и зарегистрированных машинах нарушает законы штата. Дальше – больше. Из 14 штатов, успевших присоединиться к МАТРИЦЕ, за несколько месяцев отвалились Орегон, Алабама, Южная Каролина, Кентукки и Луизиана, найдя для этого в каждом случае свои причины.[10]

Эта история чрезвычайно наглядно продемонстрировала, насколько охотно власти идут на нарушение собственных законов и вторжение в частную жизнь граждан, но только при единственном важном условии – чтобы об этом ни в коем случае не узнали ни пресса, ни публика, приходящая на избирательные участки.

[10] [CM03]

Радиочастотное число зверя

RFID многоликая

В ноябре 2003 года почти одновременно в разных точках планеты прошли два независимых друг от друга мероприятия, тесно связанных, тем не менее, единым предметом обсуждения. Сначала, 15 ноября в Массачусетском технологическом институте, Кембридж, прошел семинар «RFID и приватность» (от RadioFrequency IDentification – технология радиочастотной идентификации), в дискуссиях которого приняли участие ученые-разработчики, представители продвигающих технологию компаний, правозащитники и журналисты. Подобный научно-практический семинар организован впервые, однако актуальность его очевидна практически для всех, кто понимает, сколь серьезную угрозу тайне личной жизни представляют новейшие технологии бесконтактной идентификации и базы данных на этой основе.

Всего несколькими днями позже, 20–21 ноября, по другую сторону Атлантики, в парижском отеле «Шарль де Голль» состоялся большой международный конгресс ID World 2003. Под общим девизом «Революция идентификации в реальном и цифровом мирах» участники форума обсуждали достижения и перспективы бурно развивающихся ныне технологий RFID, биометрии, смарт-карт, а также в целом сбор информации на основе этих технологий.

Поскольку оба форума прошли практически в одно время, прежде всего бросилось в глаза то, сколь по-разному оценивают технологию бизнес-круги в зависимости от места, где она обсуждается. На семинаре в МТИ много выступали правозащитники, рассказывавшие о лицемерии, двуличности и лжи, сопровождающих внедрение новых технологий идентификации. А представители бизнеса, в свою очередь, напирали на то, сколь сильно преувеличивают неспециалисты опасности чипов идентификации, сколь слабым и подверженным помехам является излучение RFID, как много способов сделать чип бездействующим и сколь легко его блокируют всякие материалы – от жидкостей и человеческого тела до пластмасс и фольги.[11]

Зато на парижском конгрессе ID World доклады рисовали захватывающую картину победного шествия новаций едва ли не во всех мыслимых сферах – от торговли и учета производства до охраны объектов. Вообще говоря, впервые технологию радиочастотной идентификации в задачах отслеживания перемещений и контроля доступа начали применять еще в 1980-е годы. Основу систем RFID составляют устройства-считыватели (ридеры) и «умные метки», т. е. микрочипы с подсоединенной антенной. Когда такая метка приближается к ридеру, она активизируется и радиоволнами выдает считывателю информацию, хранящуюся в памяти чипа. К концу 1990-х годов технология RFID достигла такой степени миниатюризации, что чипами-ярлыками в принципе можно помечать уже что угодно – от людей и одежды до денежных знаков и насекомых.[12]

Например, Европейский центральный банк (ECB) активно сотрудничает с ведущими европейскими изготовителями микросхем, создающими RFID, намереваясь в ближайшем будущем с помощью этой технологии защитить от подделки единую европейскую валюту, запрессовывая чипы непосредственно в банкноты евро. Все работы по принципиально новой защите бумажных денег ведутся в обстановке повышенной секретности, поэтому представители ECB крайне неохотно соглашаются на комментарии, дают уклончивые ответы и предпочитают говорить сразу о множестве современных мер защиты банкнот, включая рельефную печать и голографические полосы. Что же касается микрочипов, то, согласно информации

[11] [MA03]

[12] [SI03]

специализированных изданий по микроэлектронике, над этой задачей по заказу Европейского центробанка работают германская фирма Infineon Technologies AG и голландская Philips Semiconductors NV. Что же касается конкретных сроков, то анонимные источники в ECB в качестве ориентировочной даты выпуска евроденег с встроенными чипами называют 2005 год.[13]

Одна из самых многообещающих сфер приложения RFID – это автоматизация материального учета. В 1999 году в результате совместной договоренности множества крупных компаний при Массачусетском технологическом институте была сформирована исследовательская группа Auto-ID Center. В качестве главных задач перед этим центром были поставлены разработка и полевые испытания новой разновидности компьютерных сетей, способных при помощи чипов и считывателей RFID отслеживать расположение и перемещение по складам или магазинам огромной массы штучных объектов, таких как бритвы, бутылки или ботинки. Главными спонсорами Auto-ID-центра стали такие фирмы и торговые сети, как Coca-Cola, Gillette, Target, Home Depot и Wal-Mart, которые вложили в проект свыше 20 миллионов долларов. В октябре 2003 разработанная в Auto-ID Center технология сочтена настолько зрелой, что ее решено перевести на следующую ступень развития. Все разработанные в МТИ стандарты и прочие обязанности по поддержке RFID переданы фирме EPCglobal, совместному предприятию организаций Uniform Code Council и EAN International, ведающих стандартами штрих-кодов.[14]

Грандиозные перспективы для RFID видятся в самых разных областях индустрии. Так, в январе 2003 г. автошинный гигант Michelin объявил о начале испытаний чипов-идентификаторов, вулканизируемых непосредственно в резину покрышек. Радиочастотная микросхема-идентификатор изготовляется компаниями Fairchild Semiconductor International и Philips, имеет размер со спичечную головку и специально предназначена для отслеживания индивидуальной судьбы каждой из автопокрышек. Для этого в чипе хранится уникальный номер шины, который можно привязать к номеру автомобиля; данные о том, где и когда покрышка сделана; максимально допустимое давление; размеры и так далее. Всю эту информацию можно считывать и обновлять дистанционно с помощью ручного прибора. Кроме того, компании Philips и Texas Instruments разработали для шин специальные чипы RFID с датчиками температуры и давления, по радио связанные с бортовым компьютером автомобиля, чтобы водитель мог по приборной панели отслеживать состояние каждой из шин индивидуально. Правда, в мишленовскую резину такие датчики пока встраивать не планируется, поскольку для начала компания хочет убедиться, найдут ли спрос шины с простыми чипами-идентификаторами. Пока что упрочненные микросхемы RFID для шин – удовольствие довольно дорогое, добавляющее к стоимости покрышки несколько долларов. Точно еще неизвестно, захотят ли автомобильные компании платить дополнительные деньги за новые возможности, однако в Michelin уверены, что цена существенно упадет, если дело дойдет до массового производства (ежедневно здесь выпускается 800 000 шин).[15]

Периодически поступают известия и о весьма экзотических приложениях RFID. Вроде, к примеру, оригинальной системы iGlassware, наделяющей зачатками интеллекта самые обыкновенные стаканы и фужеры. Благодаря этому изобретению американца Пола Дитца из научно-исследовательского центра MERL, бармены и официанты в ресторанах смогут теперь мгновенно узнать, у кого из посетителей опустело в бокале, мгновенно подскочить, вновь наполнить посуду и продемонстрировать тем самым высочайший класс обслуживания клиентов в заведении. В системе iGlassware микрочип с крошечной катушкой антенны крепятся к дну стакана в упаковке, защищающей электронику от посудомоечной машины. Специальное про-

[13] [JY01]
[14] [GI03]
[15] [RF03]

зрачное покрытие стакана играет роль электродов конденсатора, а жидкость, заполняющая посуду, в данном случае выполняет функцию диэлектрика, перетекание которого в желудок клиента изменяет емкость конденсатора. Поскольку реагирующий на эти перемены микрочип каждого стакана имеет индивидуальный идентификатор, а в каждый стол встроен транслятор-радиопередатчик, то на пульте у бармена или метрдотеля ведется постоянный учет степени наполненности посуды клиентов. И как только емкость конденсатора в одном из стаканов уменьшается до критической, официант получает сигнал с координатами стола и места, требующего, возможно, налить «еще по одной». Электропитание чипов в стаканах осуществляется за счет радиочастотного сигнала, излучаемого передатчиком в столе. Эксперты по менеджменту ресторанов и отелей проявили к новинке самый горячий интерес, назвав ее «долгожданным и весьма многообещающим приложением».[16]

Ну и, конечно же, нельзя не сказать о масштабном распространении RFID за последние годы в торговле и системах оплаты. Так, компания ExxonMobil с большим успехом внедрила систему Speedpass на более чем 7500 своих автозаправочных станций. Благодаря этому водители мгновенно расплачиваются за бензин, просто проведя брелоком или карточкой с RFID-чипом вблизи считывателя – соответствующая сумма через компьютер автоматически снимается с банковского счета клиента. Эту же систему Speedpass недавно реализовали в более чем 400 закусочных McDonald's в Чикаго, где теперь клиентам предоставлена возможность моментально расплачиваться за свои гамбургеры и картошку-фри.

Весьма похожую систему под названием PayPass начала внедрять сеть MasterCard, встраивая RFID непосредственно в кредитную карточку. Благодаря чипу-идентификатору владелец освобождается от необходимости вводить код PIN, подписывать чек или как-либо еще взаимодействовать с персоналом – если в точке расчета, конечно, уже имеется соответствующий считыватель. Поскольку при таком подходе нужды в пластиковой карточке, как таковой, в общем-то уже нет, в MasterCard рассматривают и иные варианты реализации RFID, вроде встраивания микрочипов в авторучку (для солидных мужчин) или же, к примеру, в серьги (для дам). Все эти предметы, правда, несложно потерять, поэтому в конечном счете банковские институты очень устроил бы вариант с имплантацией RFID непосредственно в тело человека.

И вот тут в центре внимания оказывается американская фирма Applied Digital Solutions (ADS), на сегодняшний день единственная, кто уже занимается подкожными инъекциями RFID-микросхем не только животным, но и людям. Глава ADS Скот Силвермен тоже выступал на парижском конгрессе ID World, где сообщил, что его фирма уже готовится к запуску в обозримом будущем специального сервиса VeriPay, который позволит людям расплачиваться за товары и услуги с помощью чипа, имплантированного в руку.[17]

Время двойных стандартов

Флоридская компания Applied Digital Solutions регулярно привлекает внимание прессы и общественности начиная с начала 2000-х годов, когда впервые стали появляться известия о ее технологии Digital Angel, позволяющей с помощью чипа-импланта дистанционно идентифицировать человека, следить за его географическим местоположением и физическим состоянием. Особый же резонанс инициативы ADS получили в феврале 2002, с появлением торговой марки «Чипсоны». Эту торговую марку – The Chipsons – компания Applied Digital зарегистрировала для своеобразного увековечения флоридской семьи Джекобсов – дантиста Джефри, его жены Лесли и их сына-подростка Дерека, – вызвавшихся быть первой семьей с имплантированными

[16] [YB02]
[17] [JU03]

в руку устройствами VeriChip, капсулами размером 11x2 мм, содержащими внутри катушку антенны и RFID-микросхему, подпитывающимися от тепла человеческого организма.[18]

Эта акция наглядно продемонстрировала, насколько быстро стала меняться ситуация в Америке после 11 сентября 2001. Когда в 2000 году только-только появились сообщения о технологии Digital Angel, то американская общественность буквально вскипела от негодования. Очень громко зазвучали голоса не только правозащитников, усмотревших в технологии посягательство на приватность граждан, но и христиан-ортодоксов, сразу вспомнивших знаменитое библейское пророчество об Антихристе из книги Апокалипсис апостола Иоанна: «И он сделал так, что всем – малым и великим, богатым и нищим, свободным и рабам – положено будет начертание на правую руку или на чело их; и что никому нельзя будет ни покупать, ни продавать, кроме того, кто имеет это начертание (число имени его) или знак зверя»… Интересно, что слова о «числе зверя» в данном случае подходили на редкость точно, поскольку патенты на свой чип-имплант Applied Digital Solutions приобрела вместе с покупкой фирмы Destron Fearing, специализировавшейся на чипах-метках для скота и других животных. Волна протестов в обществе оказалась тогда настолько мощной, что руководство ADS поспешило дать задний ход и заверить публику, что решила отказаться от технологии имплантации и переключиться на сенсоры, встраиваемые в браслеты или пейджеры.[19]

VeriChip, подкожная капсула с микросхемой RFID

Но затем случились известные события 11 сентября 2001, и уже через пять дней на волне национальной истерии хирург из Нью-Джерси Ричард Силиг самостоятельно имплантировал себе сразу две капсулы с устройством VeriChip – в правое предплечье и бедро, – дабы на собственном организме продемонстрировать полезность новой технологии в деле обеспечения личной безопасности. После этого пошли сообщения об интенсивных контактах Applied Digital Solutions с латиноамериканскими странами, где технологию якобы чрезвычайно активно востребовала общественность, озабоченная ростом количества похищений людей. А в феврале во флоридскую штаб-квартиру компании нанес личный визит бразильский сенатор Антонио де Кунха Лима, вызвавшийся стать «первым политиком с чипом-имплантом»…[20]

Дело это, конечно, сугубо личное и каждый, как известно, сходит с ума по-своему. Но в свете чрезвычайной озабоченности американской госадминистрации проблемами тотального

[18] [JU02a],[JM02]
[19] [LD03]
[20] [JU02b]

контроля, в стране стали рождаться опасения, как бы наиболее лояльная к власти часть общества не потребовала всеобщей поголовной имплантации. Подобные опасения не так-то просто назвать полностью безосновательными, поскольку в прессе и Интернете уже неоднократно выдвигались предположения, что у флоридской фирмы ADS явно имеются какие-то очень влиятельные покровители на самой вершине политической власти США. Уж слишком уверенно держится ADS на плаву и продолжает продвигать свои сомнительные инициативы, несмотря на очевидно негативное отношение к ее технологии со стороны подавляющего большинства общества. Событие, произошедшее в октябре 2002, весьма убедительно подтвердили, что дело тут действительно нечистое.

Тогда, ко всеобщему удивлению народа, национальное Управление по надзору за качеством пищевых продуктов и медикаментов (Food and Drug Administration, FDA), еще совсем недавно заявлявшее, что будет тщательно разбираться с продукцией ADS, вдруг издало официальный документ, вообще освобождающий VeriChip от исследований и сертификации в FDA, если устройство используется в целях «безопасности, финансовой и персональной идентификации». Для формального объяснения такого шага заявлено, что FDA занимается лишь имплантами медицинского назначения. Однако хорошо известно, что до этого в США ничего нельзя было вживлять человеку под кожу без достаточно длительной процедуры сертификации в FDA. Даже косметические импланты, включая средства увеличения размеров бюста или пениса, хотя и не имеют никакого медицинского назначения, проходят тщательное исследование экспертов FDA на предмет побочного воздействия на человеческий организм. Известно и то, что ADS при рекламе VeriChip всегда напирает именно на медицинскую полезность своего устройства, потенциально обещающего спасать жизни попавшим в беду людям.[21]

Поскольку и управление санитарного надзора, и Applied Digital Solutions отказались передать в печать документы, сопровождающие выдачу разрешения на VeriChip, правозащитная организация EPIC запустила официальный запрос на получение этой документации на основании закона о праве граждан на доступ к информации (FOIA). У правозащитников нет сомнений, что всякий человек имеет право вживлять в собственный организм что угодно – хоть хвост или рога. Но нынешние совместные маневры бизнеса и власти легко могут привести к тому, что однажды частные работодатели или государственные учреждения в качестве приема на работу начнут требовать у людей согласия на вживление под кожу чипа идентификации. Совершенно добровольного согласия, естественно…[22]

Учет и контроль

То, что технология RFID чрезвычайно нравится американской госадминистрации, особенно спецслужбам и военным, не подлежит никакому сомнению. Имеются сведения, что Министерство обороны США впервые начало применять радиочастотные метки еще в 1991 году, во время войны в Персидском заливе, для отслеживания перемещений крупных грузов и транспортных средств. К концу 2003 года высшее руководство Пентагона сочло технологию «умных ярлыков» настолько развитой, что решило радикально перестроить всю неповоротливую, «византийскую» систему закупок и инвентаризации в гигантском военном ведомстве. В конце октября 2003 Пентагон официально объявил о выработке «Политики радиочастотной идентификации», которая потребует от каждого поставщика Министерства обороны снабдить к январю 2005 года все свои товары пассивными (с питанием от антенны) чипами RFID. Исключение сделано только для таких «массовых товаров», как песок, гравий и вода.[23]

---

[21] [JU02c]

[22] [EA02]

[23] [GL03]

Другая весьма привлекательная для военных область применения технологии RFID и близко ей родственных бесконтактных смарт-карт – это контроль доступа. Широкомасштабные эксперименты с «умными баджами» начались в Пентагоне в 2000 году, вместе с постепенным вводом личных «карт общего доступа» для идентификации военного и гражданского персонала на основе смарт-карт.[24]

Но, вообще говоря, к технологиям смарт-карт в Министерстве обороны США начали примеряться по крайней мере года с 1993. Тщательно знакомились с опытом правительственных органов стран поменьше, таких как Испания или Финляндия, где подобные вещи уже введены достаточно широко. Изучали и готовили технологический фундамент в национальной промышленности. Приблизительное представление о том, что представляет собой система автоматизированного контроля доступа в режимных ведомствах, можно получить на следующем примере. На рубеже 1998-99 гг. американская фирма 3-G International (3GI) объявила о выпуске «смарт-картной системы широкого применения Passage Government», предназначенной для решения задач по обеспечению безопасности в правительственных агентствах и организациях. В системе 3GI предусмотрено шесть базовых приложений, куча дополнительных, а также технология управления картами, позволяющая правительственным организациям выпускать «персонализированные» многоцелевые смарт-карты. Каковы же основные приложения Passage Government?

• Мониторинг физического доступа и определение местонахождения персонала – обеспечивает контроль и регистрацию прихода и ухода сотрудников с работы. Для идентификации сотрудников используются цифровые фотографии, и в реальном масштабе времени поддерживается база данных о персональном местонахождении людей. По запросу администрации генерируются соответствующие сообщения и отчеты.

• Учет посетителей – работает совместно с предыдущим приложением. Приложение поддерживает базы данных о посетителях, о временных картах-пропусках, о выдающих эти карты и о принимающих посетителей.

• Контроль за оборудованием – обеспечивает усовершенствованный учет и контроль за имуществом и оборудованием на объекте. Доступ к оборудованию контролируется соответствующей базой данных о владельцах смарт-карт.

• Учет посещаемости – использует возможности смарт-картной технологии для оперативного документирования посещений сотрудниками учебных занятий, встреч, конференций и прочих служебных сборов. Это клиентское приложение «снимает» персональную/административную информацию со смарт-карты посетителя мероприятия и формирует отчеты заседаний.

В 2001 году фирму 3GI поглотила более крупная RSA Security, включив Passage Government в более широкий пакет приложений RSA SecurID Passage.[25]

Одно из главных «неудобств» традиционных смарт-карт – для считывания информации их надо непременно проводить через щель прибора считывателя. Другое дело – новые бесконтактные смарт-карты, обменивающиеся информацией с ридером или программатором дистанционно через радиочастотный интерфейс. Метка RFID, по сути своей, та же самая бесконтактная смарт-карта, но с меньшей функциональностью из-за крошечных размеров. С начала 2000-х годов именно RFID и бесконтактные смарт-карты выступают в качестве основы современных систем «умных баджей», внедряемых повсеместно – в госучреждениях и корпорациях, учебных заведениях и тюрьмах.[26]

---

[24] [RE00]

[25] [FA01]

[26] [PE03],[JS03]

По секрету всему свету

Мало кому (кроме государства и корпораций) нравится идея крупных баз данных, централизованно хранящих персональную информацию о гражданах. Во-первых, это сверхпривлекательный объект устремлений для злоумышленников, использующих реквизиты чужой личности в своих гнусных целях. Во-вторых, это мощная потенциальная угроза злоупотреблений со стороны владельцев базы и обслуживающего персонала. И в-третьих, коль скоро здесь так глубоко замешан человеческий фактор, надежно защитить подобные хранилища практически невозможно. В таких условиях можно гарантировать, что известия о компрометации очередной крупной базы как появлялись часто прежде, так и будут регулярно появляться впредь. Широкое же внедрение микрочипов радиоидентификации, которые индустрия в ближайшем будущем намерена встраивать чуть ли не во все потребительские товары, непременно увеличит и масштабы компрометации. Потому что RFID, облегчающие корпорациям и торговым сетям учет производства и сбыта, для покупателей означают ведение соответствующих гигантских баз данных о приобретенных ими товарах.

Эта тенденция очень не нравится той части общества, что обеспокоена вторжением корпораций и властей в личную жизнь граждан. Для сопротивления бесконтрольному насаждению RFID создана специальная общественная организация CASPIAN или «Потребители против вторжения супермаркетов в частную жизнь» (Consumers Against Supermarket Privacy Invasion and Numbering). Летом 2003 г. активисты этой организации и решили проверить, как радетели RFID, заверяющие всех в надежной защите накапливаемой информации, в действительности способны хранить секреты. Для этого был проведен нехитрый тест на сайте Auto-ID Center (**www.autoidcenter.org**) – исследовательского центра консорциума, объединяющего около 100 компаний и 5 университетских лабораторий, разрабатывающих инфраструктуру для широкомасштабного внедрения чипов идентификации. Абсолютно без всяких хакерских ухищрений, просто введя в окошке поиска волшебное слово «confidential», правозащитники получили свободный доступ к целой библиотеке (около 70) конфиденциальных документов, не предназначенных для посторонних глаз.[27]

Среди этих материалов оказался, в частности, доклад о мерах по «умиротворению» противников RFID, в котором приводятся цифры внутреннего социологического исследования, показавшего, что около 78 % опрошенных граждан «встревожены» посягательством чипов-меток на частную жизнь, а 61 % обеспокоены влиянием повсеместно встроенных микросхем на здоровье. В другом документе вносятся предложения по смене отпугивающего названия RFID-чипов на более дружелюбное типа «зеленые ярлыки». О документах с подробным расписанием рабочих встреч и детальной контактной информацией функционеров консорциума и говорить не приходится.

Естественно, это дало повод активистам CASPIAN громко заявить о неспособности консорциума обеспечить надежное хранение чувствительной к разглашению информации. В Auto-ID Center, в свою очередь, воздержались от комментариев, однако усилия для более надежного закрытия документов все же приложили. Впрочем, птичка уже выпорхнула из клетки, и конфиденциальные документы можно найти в Сети на множестве сайтов-зеркал (см. **www.cryptome.org/rfid-docs.htm**).

[27] [AM03]

Интересно также, что буквально на следующий день после скандала крупнейшая в мире сеть универмагов Wal-Mart (порядка 4700 магазинов по всему миру) неожиданно объявила о сворачивании торгового эксперимента с RFID-чипами в бритвах Gillette. Руководство Wal-Mart не пожелало комментировать прекращение этого проекта, получившего название «умные полки» и уже практически подготовленного к запуску в универмаге Броктона, одного из пригородов Бостона. Но можно предполагать, что скандал в Auto-ID Center был сочтен слишком неблагоприятным фоном для представления публике новой технологии.[28]

[28] [GS03]

Охота на ведьм XXI века

[В Древнем Египте] термином «хэка» обозначалась магия, то есть «слова власти» – магические слова, заклинания.
Уоллис Бадж. Египетская магия

Имеется некоторое сообщество, некая общая культура, состоящая из опытных программистов и сетевых чародеев, которая ведет свою историю от многолетней давности первых миникомпьютеров и от самых ранних экспериментов с сетью ARPAnet. Члены этой культуры и дали рождение термину «hacker»[хэка]. Хэкеры построили Интернет.
Эрик Рэймонд. Как стать хэкером

Во все времена власти с опаской относились к компетентным людям, хорошо знающим свое дело, а потому имеющим тенденцию к самостоятельному мышлению и независимым суждениям. В древнейшие времена такой репутацией пользовались маги, с наступлением эры высоких технологий обостренное раздражение властей стали вызывать так называемые «хакеры». Сейчас уже никто, наверное, и не скажет, в какой момент к термину «хакер» прирос криминальный смысл. Обычно в этом принято винить поверхностных журналистов и киношников, не способных провести грань между пытливым исследователем-профессионалом и каким-нибудь безответственным или злонамеренным негодяем (кракером, т. е. криминальным хакером), использующим чужие результаты в собственных корыстных целях.

Откуда исходит угроза миру?

В последний день 1999 года на страницах популярного сайта **www.Slashdot.org** была опубликовано интервью с членами известной хакерской организации L0pht,[29] признанное читателями как один из лучших материалов такого рода за всю историю Slashdot. Интервью было коллективным, то есть ответы давал как бы просто L0pht, без конкретизации отвечавшихличностей. И один из самых первых вопросов звучал примерно так: «Чьи угрозы следует рассматривать более опасными для личных свобод, со стороны правительства или со стороны транснациональных корпораций?»

Вот что, в несколько вольном пересказе, ответили на это хакеры из L0pht.[30]

Хотя и правительства, и транснациональные корпорации в значительной степени несут угрозу личным свободам человека (в частности, в Интернете), но существует опасность, значительно превосходящая первые две. Имя ей – неинформированные граждане. И как это ни парадоксально звучит, эта опасность многократно реальнее именно в условиях демократических режимов, где правительства стараются следовать общественному мнению. Потому что уже абсолютно четко видно, как большинство граждан вполне согласны и готовы поступиться своими личными свободами в обмен на ощущение некой безопасности. Обычно это укладывается в формулу типа «ради безопасности наших детей».

Уже сейчас многие люди полагают, что анонимный доступ к Интернету – это признак криминального поведения. Тем, кто управляет рычагами власти, обычно очень хочется, чтобы стремление воспользоваться правом на личную тайну воспринимали как «антисоциальное»

[29] В 2000 году на базе L0pht была создана консалтинговая компания @Stake, специализирующаяся на проблемах компьютерной безопасности

[30] [BR99]

поведение. Ведь добропорядочному гражданину нечего скрывать, не так ли? Это только террористам, наркодельцам и педофилам нужно скрывать свои темные замыслы.

На правительство надавливают неинформированные граждане, либо те, кому уже промыли мозги до стадии панического ужаса от угроз современных технологий и от тех людей, которые бесконтрольно могут технологии использовать (хакеров, одним словом). В этом процессе лоббирования активно участвуют и транснациональные корпорации, финансируя деятельность «озабоченных» общественных групп или принимая участие в деятельности ассоциаций, оказывающих консультативную помощь правительственным структурам в технических вопросах. И весьма часто эти рекомендации приводят к очередному урезанию священного права граждан на личные свободы.

Весьма проблематичным является и то, что мир деятельности транснациональных корпораций – это мир частной собственности. И когда какая-либо внешняя группа начинает заниматься тщательным анализом технологических продуктов или коммуникационных услуг корпораций, то возникают конфликты принципиального характера. Если эта группа обнаруживает существенный изъян, скажем, в безопасности и публикует информацию о дыре в защите, то корпорация в свою очередь нередко объявляет, что этим нанесен сильнейший ущерб ее деятельности и затевает судебное преследование в отношении опубликовавших компромат, а то и добивается изменений в законодательстве.

Одна из наиболее известных историй такого рода – судебная тяжба индустрии сотовой связи в США. Клонирование сотовых телефонов было острейшей занозой в наиболее нежных местах индустрии мобильной связи. В конце концов к решению проблемы привлекли американское правительство, дабы подобного рода мошенничество было запрещено специальным законом. В итоге же определенный участок спектра радиочастот стал в США запрещенным для прослушивания и сканирования. А обладание «оборудованием для клонирования» стало преступлением, хотя это просто компьютер, программатор перезаписываемых микросхем и сотовый телефон. Любому, кто понимает техническую суть проблемы, очевидно, что это явная глупость. Но имеющие большие деньги имеют и большое влияние на власть. И именно государственная власть принимает такого рода законы.

Правительство подталкивает людей, люди подталкивают правительство. Уже и не найдешь, кто первым высадил это семя… Те же, кто смыслят что-то в технологиях, страсть как все заняты разработкой какой-нибудь очередной крутой штуковины. Ну, а погруженный в эти технические чудеса мир тем временем все больше сползает к глобальной диктатуре, пока население понемногу привыкает к ней под видом «безопасности».

Конец цитаты, как говорится.

Когда законы готовит полиция

В ноябре 2003 года президент США Джордж Буш обратился с просьбой к американскому Сенату ратифицировать первый международный закон о компьютерных преступлениях или Конвенцию о киберпреступности (Convention on Cybercrime). В своем письме к Сенату Буш назвал этот весьма спорный в своем содержании договор, официально подготовленный Советом Европы, «эффективным инструментом в глобальных усилиях по противодействию преступлениям, связанным с компьютерами» и «единственным многосторонним договором, направленным на компьютерные преступления и электронный сбор улик».

Хотя США не являются членом Евросовета с правом голоса, достаточно хорошо известно, что именно американские правоохранительные органы были главной силой, стоявшей за подготовкой международного договора о киберпреступности. В этом законе они видят путь к выработке интернациональных стандартов в оценке криминальной деятельности, имеющей отношение к посягательствам на авторские права, к онлайновому мошенничеству, детской

порнографии и несанкционированным сетевым вторжениям. Как заявляют в Министерстве юстиции США, эта конвенция устранит «процедурные и юридические препятствия, которые могут задерживать или мешать международным расследованиям».[31]

Поскольку столь благородному, на первый взгляд, делу яростно и который уже год подряд сопротивляются правозащитники многих стран, имеет смысл рассмотреть историю рождения данной конвенции в некоторых содержательных подробностях.

Для компьютерных специалистов, уважающих термин «хакер», под «хакингом» обычно понимается процесс проникновения в суть той или иной вещи. Конечный результат – понимание того, «как это работает», зачастую сопровождаемое предложениями по улучшению работы. У властей же понимание «хакинга» сложилось совсем иное. Поскольку политическое руководство государств – народ занятой, то им некогда разбираться во всех этих терминологических тонкостях. Для этого есть эксперты и консультанты. Раз кругом говорят, что хакеры взламывают защиту компьютерных сетей, значит это дело экспертов из полиции и прочих правоохранительных органов. Логика же полиции свелась примерно к следующему умозаключению: раз хакерская публика мнит себя дюже умной и пишет всякие-разные программы, плодящие киберпреступность и лишающие корпорации доходов, то надо это дело запретить. Причем на корню.

Впервые о подготовке закона стало известно в октябре 2000 года, когда был рассекречен весьма важный и любопытный документ, подготовленный под эгидой Совета Европы и носивший название «22-я версия Проекта договора о киберпреступлениях» (Draft Convention on Cybercrime, № 22 rev). Этот документ, подготовленный в условиях необычной для европейского сообщества секретности, был представлен как «первый международный договор, посвященный уголовному праву и процедурным аспектам разного рода преступного поведения, направленного против компьютерных систем, сетей и данных».

В 22-й версии проекта обнаружилось много чего интересного: и намерение заставить всех интернет-провайдеров хранить подробные отчеты о деятельности своих клиентов (нечто подобное уже реализовал у себя Китай, поскольку это крайне полезный инструмент в борьбе с инакомыслием); и намерение привлекать к уголовной ответственности за посягательство на копирайт (для множества европейский стран это весьма спорный с правовой точки зрения вопрос); и запрет на хакерскую деятельность вкупе с хакерским инструментарием, и ряд положений, игнорирующих презумпцию невиновности, а также побуждающих граждан к «самообвинению». Достаточно подробный разбор весьма спорных юридических новшеств, предложенных в проекте и противоречащих европейской Конвенции о правах человека, был сделан в коллективном письме GILC (**www.gilc.org**), международной коалиции нескольких десятков правозащитных групп, на имя генерального секретаря Евросовета. По оценкам, сделанным в заявлении GILC, этот проект «противоречит прочно утвердившимся нормам защиты личности, подрывает разработку эффективных технологий сетевой безопасности и снижает подотчетность правительств в их правоохранительной деятельности».[32]

В контексте нашей истории наибольший интерес представляют те положения проекта Договора, что посвящены непосредственно хакерам и их инструментам. В компактном представлении выглядят эти положения проекта следующим образом.

Каждая сторона, подписывающая договор, должна принять такое законодательство и прочие меры, которые окажутся необходимы для преследования как уголовных преступлений следующих деяний: (1) доступ к компьютерной системе в целом или любой ее части без надлежащего на то права; (2) осуществляемый с помощью технических средств перехват компьютерных данных, идущих внутри компьютерной системы, от нее или к ней, а также перехват

[31] [DE03]

[32] [GI00]

электромагнитных излучений системы, несущих такие компьютерные данные; (3) внесение, уничтожение, подмена, повреждение или удаление компьютерных данных без надлежащего на то права; (4) создание, продажа и прочее распространение устройств и компьютерных программ, разработанных или приспособленных для целей, перечисленных в предыдущих пунктах; (5) распространение информации, способствующей доступу к компьютерным системам без надлежащего на то права.

На проходившей в ту пору в Амстердаме конференции DEF CON, где собираются хакеры, занимающихся вопросами компьютерной безопасности, новость о подготовке драконовского договора взбудоражила всех. Как прокомментировал ситуацию один из участников форума, «они просто боятся тех вещей, которых не понимают, того, что не могут контролировать… это действительно может превратиться в охоту на ведьм». По заключению американского эксперта по киберправу Дженифер Грэник, из положений документа следует, что вне закона оказываются и все публикации об уязвимостях и слабостях компьютерных систем. В частности, и столь популярные среди профессионалов рассылочные листы как BugTraq и NTBugTraq, имеющие десятки тысяч подписчиков и служащие ценным источником для поддержания компьютерных систем «в форме». А то, что под запретом окажутся такие программы, как сетевые сканеры, тестирующие уязвимость портов системы, очевидно и без заключения экспертов. Более того, логика документа может со временем наложить запрет и на самые обычные программы-отладчики (дебаггеры), поскольку и этот инструмент широко используется для «хакинга». Конечно, всем ясно, что это абсурд и глупость, поскольку для программиста дебаггер – что отвертка для слесаря. (Талантливый слесарь, как известно, и отверткой может открыть замок, но никому не приходит в голову запретить отвертки).[33]

[33] [SU00]

Конец ознакомительного фрагмента.